Oberlandesgericht Köln, 15 U 40/23

Datum:	03.04.2025
Gericht:	Oberlandesgericht Köln
Spruchkörper:	15. Zivilsenat
Entscheidungsart:	Urteil
Aktenzeichen:	15 U 40/23
ECLI:	ECLI:DE:OLGK:2025:0403.15U40.23.00

Tenor:

Auf die Berufung des Klägers wird das Urteil des Landgerichts Aachen vom 10.2.2023 (8 O 92/22) unter Zurückweisung des weitergehenden Rechtsmittels teilweise abgeändert und insgesamt wie folgt neu gefasst:

Die Beklagte wird verurteilt, an den Kläger 100 Euro nebst Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz seit dem 7.6.2022 zu zahlen.

Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger künftige materielle und künftige derzeit noch nicht vorhersehbare immaterielle Schäden zu ersetzen, die dem Kläger durch den unbefugten Zugriff auf das Datenarchiv der Beklagten, der im Zeitraum ab dem 25.5.2018 bis September 2019 erfolgt ist, entstehen.

Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000 Euro, ersatzweise an ihrem gesetzlichen Vertreter (I.) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (I.) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, die Telefonnummer des Klägers für andere Zwecke als für die Zwei-Faktor-Authentifizierung bzw. für die Accountsicherung zu verarbeiten.

Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 159,94 Euro zuzüglich Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz seit dem 7.6.2022 zu zahlen.

Die weitergehende Klage wird abgewiesen.

Die Kosten des Rechtsstreits erster Instanz tragen der Kläger zu 61 % und die Beklagte zu 39 %. Die Kosten des Berufungsverfahrens tragen der Kläger zu 64 % und die Beklagte zu 36 %.

Das Urteil ist für den Kläger hinsichtlich des Unterlassungsanspruchs gegen Sicherheitsleistung in Höhe von 1.000 Euro vorläufig vollstreckbar. Im Übrigen ist das Urteil für beide Parteien ohne Sicherheitsleistung vorläufig vollstreckbar.

Die Revision wird nicht zugelassen.

Der Berufungsstreitwert wird auf 3.500 Euro bis zum 16.12.2024 und danach auf 3.000 Euro festgesetzt. Der Streitwert des erstinstanzlichen Verfahrens wird unter Abänderung der im angefochtenen Urteil enthaltenen Streitwertfestsetzung gemäß § 63 Abs. 3 Nr. 2 GKG auf 3.500 Euro festgesetzt.

Gründe: 1

I. 2

Von einer Bezugnahme auf die tatsächlichen Feststellungen sowie der Darstellung von Änderungen oder Ergänzungen wird nach §§ 540 Abs. 2, 313a Abs. 1 S. 1 ZPO abgesehen. 3

II. 4

Die Berufung des Klägers ist teilweise begründet, was zur Abänderung der angefochtenen Entscheidung im tenorierten Umfang führt. Im Übrigen bleibt sie ohne Erfolg. 5

1. Der Kläger hat gegen die Beklagte einen Anspruch auf Zahlung von Schadensersatz für immaterielle Schäden aus Art. 82 Abs. 1 DSGVO in Höhe von 100 Euro. 6

a. Die Regelung des Art. 82 Abs. 1 DSGVO ist vorliegend zeitlich anwendbar. Soweit die Beklagte erstmals im Berufungsrechtszug mit Nichtwissen bestritten hat, dass der konkret den Kläger betreffende Scrapingvorgang nach dem 24.5.2018 stattgefunden hat, ist sie mit diesem erstmaligen Bestreiten des in erster Instanz unbestrittenen Klägervortrags nach § 531 Abs. 2 ZPO ausgeschlossen. 7

aa. Der Kläger hat in der Klageschrift vorgetragen, die Anfang April 2021 im Internet veröffentlichten Daten seien „*im Jahr 2019*“ von der Plattform der Beklagten abgegriffen worden. Da er damit den Gesamtvorgang des Scrapings auf der Plattform der Beklagten vollständig in das Jahr 2019 verortet, hat er auch hinsichtlich des konkreten Zugriffs auf sein eigenes Nutzerkonto diesen zeitlichen Rahmen vorgetragen. Es handelt sich insoweit – anders als dies die Beklagte mit Schriftsatz vom 13.3.2025 geltend macht – nicht um einen prozessual unbeachtlichen Vortrag „ins Blaue hinein“. Eine Partei darf auch nur vermutete Tatsachen vortragen und unter Beweis stellen, wenn sie darüber keine genaueren Kenntnisse hat oder haben kann, sofern sie die Tatsachen nach Lage der Dinge für wahrscheinlich hält (BGH, Urt. v. 4.2.2021 – III ZR 7/20, NJW 2021, 1759 m.w.N.). 8

Unzulässig wird ein solches Vorgehen erst dort, wo die Partei ohne greifbare Anhaltspunkte für das Vorliegen eines bestimmten Sachverhalts willkürlich Behauptungen aufstellt. Bei der Annahme von Willkür in diesem Sinne ist Zurückhaltung geboten; in der Regel wird sie nur beim Fehlen jeglicher tatsächlichen Anhaltspunkte gerechtfertigt werden können (BGH, Beschl. v. 16.4.2015 – IX ZR 195/14, NJW-RR 2015, 829). Davon ist vorliegend aber nicht auszugehen, da die im Verfahren vorgelegten Pressemitteilungen der Beklagten, insbesondere die vom 6.4.2021 (Anlage B 10) und vom 15.4.2021 (Anlage B 12) sowie auch das vorgerichtliche Schreiben der Beklagten vom 11.11.2021 (Anlage B 16) ebenfalls von einem Vorfall „*bis September 2019*“ bzw. „*vor September 2019*“ sprechen.

Diesen klägerischen Vortrag hat die Beklagte in erster Instanz nicht bestritten. In der Klageerwiderung hat sie zwar allgemein vorgetragen, dass das Scraping im Zeitraum von Januar 2018 bis September 2019 – dem von ihr so bezeichneten „*Relevanten Zeitraum*“ – stattgefunden habe. Sie hat jedoch, obwohl der Kläger seinen mit der Klage unter anderem geltend gemachten Anspruch auf Schadensersatz wegen immaterieller Schäden ausdrücklich auf Vorschriften der DSGVO gestützt hat, nicht geltend gemacht, dass der Zugriff auf das Nutzerkonto des Klägers vor dem 25.5.2018 stattgefunden habe und der Kläger sich daher mangels zeitlicher Anwendbarkeit der DSGVO nicht auf diese stützen könne. Sie hat ebensowenig geltend gemacht, dass sie zum Zeitpunkt des Zugriffs auf das Nutzerkonto des Klägers mangels vorhandener Daten über keinerlei eigene Kenntnisse verfüge. Vielmehr hat sie in der Klageerwiderung und auch in den weiteren erstinstanzlichen Schriftsätzen ausführlich dargelegt, dass ihr kein Verstoß gegen die Vorschriften der DSGVO vorzuwerfen sei. Gerade im Rahmen ihrer rechtlichen Ausführungen zum Antrag zu 1) hat sich die Beklagte nicht mit der Frage des zeitlichen Anwendungsbereichs von Art. 82 Abs. 1 DSGVO befasst, sondern vielmehr darauf abgestellt, dass die vom Kläger angeführten Verstöße gegen Art. 13, 14, 24, 25, 34 und 15 DSGVO nicht vom sachlichen Anwendungsbereich des Art. 82 DSGVO erfasst seien, dass weiter kein Verstoß ihrerseits gegen diese Normen vorliege und dass dem Kläger schließlich kein immaterieller Schaden entstanden sei. Im Hinblick darauf hat die Beklagte mit dem von ihr vorgetragenen Gesamtzeitraum für das Scraping (Januar 2018 bis September 2019) eben nicht gleichzeitig ausdrücklich oder konkludent bestritten, dass speziell die Daten des Klägers, wie dieser es geltend gemacht hat, erst im Jahre 2019 abgegriffen wurden. Da damit die Absicht der Beklagten, den Vortrag des Klägers zu einem ihn betreffenden Datenabgriff im Jahr 2019 bestreiten zu wollen, weder ausdrücklich erklärt wurde noch aus den übrigen Erklärungen hervorging, hat sie den Vortrag des Klägers nach § 138 Abs. 3 ZPO unstreitig gestellt. Der Kläger hatte daher im erstinstanzlichen Verfahren keine Veranlassung, zum Zugriffszeitpunkt/-zeitraum auf sein Nutzerkonto konkreter vorzutragen. 9

bb. Das im Berufungsverfahren erstmals erfolgte Bestreiten der Beklagten, bei dem es sich nicht um eine bloße Präzisierung ihres erstinstanzlichen Vortrags handelt, ist nicht zuzulassen, weil die insoweit darlegungspflichtige Beklagte nicht – auch nicht im nachgelassenen Schriftsatz vom 13.3.2025 – konkret dargetan hat, dass und warum ein Ausnahmefall des § 531 Abs. 2 Nr. 1 und/oder Nr. 3 ZPO vorliegt. 10

(1) Die Frage des Zugriffs der Scraper konkret auf das Konto des Klägers ist kein Gesichtspunkt, der vom Gericht des ersten Rechtszugs erkennbar übersehen oder für unerheblich gehalten wurde (§ 531 Abs. 2 Nr. 1 ZPO). Von einem solchen Fall ist auszugehen, wenn das Erstgericht, hätte es die vom Berufungsgericht für zutreffend erachtete Rechtsauffassung geteilt, zu einem Hinweis nach § 139 Abs. 2 ZPO verpflichtet gewesen wäre (BGH, Beschl. v. 29.5.2018 – VI ZR 370/17, NJW 2018, 3652; MüKoZPO/Rimmelspacher, 6. Aufl. 2020, ZPO § 531 Rn. 20). Zu einem solchen Hinweis 11

hätte das Landgericht jedoch keine Veranlassung gehabt. Da der Kläger seine Ansprüche ausdrücklich auf eine Verletzung der DSGVO gestützt und bereits in der Klageschrift geltend gemacht hat, es sei „*im Jahr 2019*“ zu einem Datenabgriff von seinem Konto auf dem sozialen Netzwerk der Beklagten gekommen, bestand für die Kammer kein Anlass zu der Annahme, dass die Beklagte bei ihrem Vortrag, wann der Gesamtvorgang des Scrapings stattgefunden habe, die Frage der zeitlichen Anwendbarkeit der DSGVO speziell für die Ansprüche des hiesigen Klägers „*erkennbar übersehen oder für unerheblich gehalten hat*“ (§ 139 Abs. 2 ZPO). Vielmehr war davon auszugehen, dass die Beklagte – die in der Sache umfassend und rechtlich vertieft zu ihren angeblichen Verstößen gegen die DSGVO vorgetragen hat – diesen Punkt im Vortrag des Klägers gerade nicht bestreiten wollte.

(2) Die Beklagte hat nicht dargelegt, dass die fehlende Geltendmachung dieses Verteidigungsmittels in erster Instanz nicht auf Nachlässigkeit beruht (§ 531 Abs. 2 Nr. 3 ZPO). Angesichts des in der Klageschrift auf Art. 82 Abs. 1 DSGVO gestützten Schadensersatzanspruchs sowie des Umstands, dass Ersatzansprüche wegen immaterieller Schäden nach den bislang geltenden sonstigen Normen nicht in Betracht kamen, war auch für die Beklagte ersichtlich, dass es auf die (zeitliche) Anwendbarkeit dieser Regelung ankam. Die Beklagte hat insbesondere nicht dargetan, dass sie erst aufgrund von nach Schluss der mündlichen Verhandlung vor dem Landgericht erlangten Erkenntnissen in der Lage war, das Klägervorbringen zu dem Zeitpunkt des ihn betreffenden Vorfalls mit Nichtwissen zu bestreiten, dass sie erst danach Kenntnis davon erlangt hat, dass sie nicht im Besitz von Rohdaten und Logdateien ist und ihr nicht bekannt ist, wer die Scraper waren. Das neue Vorbringen der Beklagten ist auch nicht unstreitig. 12

b. Die Beklagte hat als Verantwortliche gemäß Art. 4 Nr. 7 DSGVO durch ihre Verarbeitung der personenbezogenen Daten des Klägers schuldhaft gegen Art. 5 Abs. 1 lit. b) und lit. c), Art. 25 Abs. 2 S. 1 und 3 DSGVO verstoßen, weil die von ihr vorgenommene Voreinstellung der Suchbarkeit über die Mobilfunknummer auf „*C.*“ nicht dem Grundsatz der Datenminimierung entsprochen hat. 13

aa. Der Senat nimmt zunächst Bezug auf die Ausführungen des Bundesgerichtshofs in seiner Entscheidung vom 18.11.2024 (VI ZR 10/24, juris Rn. 86 ff.), die aufgrund der identischen standardmäßigen Suchbarkeitseinstellungen auch auf den hiesigen Kläger vollständig übertragbar sind und schließt sich ihnen an. 14

bb. Die insoweit als Verantwortliche darlegungs- und beweispflichtige Beklagte hat auch nicht dargetan, dass für die Verarbeitung der Daten des Klägers eine der in Art. 6 Abs. 1 S. 1 DSGVO genannten Rechtsgrundlagen vorlag. 15

(1) Eine Einwilligung des Klägers nach Art. 6 Abs. 1 S. 1 lit. a) DSGVO – auf die sich die Beklagte selbst nicht beruft – liegt nicht hier nicht vor. Nach Art. 4 Nr. 11 DSGVO ist eine Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Nach Art. 7 Abs. 1 DSGVO trägt der Verantwortliche die Darlegungs- und Beweislast für das Vorliegen einer Einwilligung. Vorliegend hat die Beklagte nicht dargelegt, dass der Kläger in die Suchbarkeit seines Kontos anhand seiner Mobilfunknummer i.S.v. Art. 4 Nr. 11 DSGVO eingewilligt hat. 16

Aus der fehlenden Abänderung der standardmäßigen Voreinstellung der Suchbarkeitsfunktion („*C.*“) im Zeitpunkt der Hinzufügung der Mobilfunknummer zu seinem 17

Account folgt keine Einwilligung des Klägers. Eine in unmissverständlicher Weise abgegebene Einwilligung setzt ein aktives Verhalten des Einwilligenden voraus. Daher begründen Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person – wie auch aus Erwägungsgrund 32 Satz 3 DSGVO folgt – keine Einwilligung (EuGH, Urt. v. 1.10.2019 - C-637/17, NJW 2019, 3433 Rn. 61 f.; EuGH, Urt. v. 11.11.2020 - C-61/19, NJW 2021, 841 Rn. 35 f.).

Die aktualisierten Nutzungsbedingungen der Beklagten vom 19.4.2018 (Anlage B19) sowie die aktualisierte Datenrichtlinie (Anlage B20) können ebenfalls keine Einwilligung des Klägers herbeiführen. Eine Einwilligung „in informierter Weise“ (Art. 4 Nr. 11 DSGVO) hätte vorausgesetzt, dass die Beklagte den Kläger in diesen Dokumenten transparent über die Suchbarkeit seines Nutzerprofils anhand der Telefonnummer informiert hätte. Dies ist jedoch mit den von der Beklagten vorgelegten Screenshots, die – unstreitig – den von ihr erfolgten Hinweis des Nutzers auf die aktualisierten Nutzungsbedingungen sowie die Einwilligung des Nutzers mittels Anklicken einer entsprechenden Schaltfläche darstellen, nicht erfolgt. Dabei hätte sich eine ausreichende Information über die weiterhin voreingestellte Suchbarkeit des Profils auf Basis der Telefonnummer nur in dem Link zu den Nutzungsbedingungen verbergen können, da es in der Anmerkung zum Zustimmungsfeld ("*F.*") heißt: "*R. "F." klickst, akzeptierst du die aktualisierten Nutzungsbedingungen*". Die Zustimmung "*F.*" bezieht sich damit ausdrücklich nicht auch auf die Datenrichtlinie, die Cookie-Richtlinie oder die bisherigen Einstellungen hinsichtlich der Daten, der Privatsphäre und der Sicherheit. 18

Selbst wenn man die vom Nutzer durch Anklicken der entsprechenden Schaltfläche erteilte Zustimmung im Sinne der Beklagten umfassender verstehen würde, ändert dies an der fehlenden Einwilligung des Klägers nichts. Denn auch die Datenrichtlinie enthält – ebensowenig wie die Nutzungsbedingungen – keine Informationen über die Suchbarkeit des Kontos anhand der Telefonnummer. Unter der Überschrift „*E.?*“ wird lediglich die Zielgruppenauswahl erläutert, nicht jedoch die Suchbarkeitsauswahl (Anlage B20, S. 6). 19

Soweit die Beklagte schließlich auf Ausführungen im Hilfebereich hinweist, hat sie schon nicht dargelegt, dass der Kläger im Vorfeld seiner Einwilligung zu den Nutzungsbedingungen auf diese Ausführungen hingewiesen wurde oder auf diese überhaupt Zugriff hatte. Davon abgesehen ist der vermeintlich maßgeblichen Passage „„*Zitat wurde entfernt*““ auch kein Hinweis auf eine Suchbarkeit des eigenen Profils anhand der eigenen Mobilfunknummer zu entnehmen. Vielmehr wird der Nutzer nur darauf hingewiesen, dass die Beklagte seine Mobilfunknummer möglicherweise für eine Kontaktaufnahme mit ihm nutzt und ihm „Freunde“ vorschlägt, nicht aber, dass Dritte diese Nummer nutzen können, um sein Profil zu finden (so auch OLG Oldenburg, Urt. v. 21.5.2024 – 13 U 100/23, juris). 20

(2) Die Beklagte kann sich auch nicht darauf berufen, dass die Verarbeitung der Mobilfunknummer des Klägers im Rahmen der Suchbarkeit des Nutzerkontos zur Erfüllung des Vertrages erforderlich war (Art. 6 Abs. 1 S. 1 lit. b) DSGVO). 21

„*Erforderlich*“ im Sinne von Art. 6 Abs. 1 S. 1 lit. b) DSGVO ist eine Verarbeitung, wenn sie objektiv unerlässlich ist, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist. Der Verantwortliche muss also nachweisen, dass ohne sie der Hauptgegenstand des Vertrags nicht erfüllt werden könnte (EuGH, Urt. v. 4.7.2023 – C-252/21, GRUR-RS 2023, 15772). Dies ist hier hinsichtlich der Mobilfunknummer des Klägers nicht der Fall. Die Beklagte benötigt die Mobilfunknummer des Klägers für die Durchführung des mit ihm geschlossenen Vertrages über die Nutzung des sozialen Netzwerkes nicht, was sich schon daraus ergibt, dass es dem Nutzer unstreitig möglich ist, seine Telefonnummer nach der Registrierung wieder zu entfernen. Soweit die 22

Beklagte sich darauf beruft, eine Teilnahme auf der sozialen Plattform sei sinnlos, wenn sich Nutzer nicht gegenseitig über ihre Mobilfunknummer finden könnten, greift auch dies nicht durch. Denn zum einen können sich die Nutzer gegenseitig auch über ihre Namen finden und ist gerade zu diesem Zweck der Name der Nutzer nach dem Vortrag der Beklagten in Form einer unabänderlichen Einstellung stets öffentlich einsehbar. Zum anderen führt allein eine von der Beklagten als sinnvoll erachtete Form der Nutzung des sozialen Netzwerkes nicht dazu, dass die Datenverarbeitung im Sinne von Art. 6 Abs. 1 S. 1 lit. b) DSGVO „*erforderlich*“ ist.

cc. Das nach Art. 82 Abs. 3 DSGVO zu vermutende Verschulden der Beklagten ist nicht ausgeräumt worden, weil die Beklagte nicht nachgewiesen hat, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. 23

c. Der Kläger hat durch diesen Datenschutzverstoß einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DSGVO erlitten. 24

aa. Nach Anhörung des Klägers steht zur Überzeugung des Senats fest, dass dieser einen Kontrollverlust dergestalt erlitten hat, dass seine bei der Beklagten gespeicherte Mobilfunknummer zusammen mit seinem Pseudonym im Internet veröffentlicht wurde. 25

Der Kläger hat überzeugend dargelegt, dass er seine private Mobilfunknummer – die er bei „A.“ hinterlegt hat – weder bei Bestellungen oder Buchungen im Internet noch auf sonstigen sozialen Netzwerken oder auf anderen bzw. einer eigenen Internetseite in einer Art und Weise veröffentlicht hat, die mit der hier streitgegenständlichen Veröffentlichung seiner Daten vergleichbar ist. Der Datensatz enthält zwar nicht den bürgerlichen Nachnamen des Klägers, sondern vielmehr ein Pseudonym. Die Beklagte hat aber die Angaben des Klägers während seiner persönlichen Anhörung, wonach dieser – unter anderem aufgrund seiner Tätigkeit als DJ – unter diesem Namen seit Jahren bekannt ist, nicht bestritten und der ihr gewährte Schriftsatznachlass bezog sich nicht auf diesen Aspekt. Insofern ist der vom Kläger erlittene Kontrollverlust mit demjenigen vergleichbar, den er erlitten hätte, wenn der Datensatz seinen bürgerlichen Nachnamen enthalten würde. 26

Nach den glaubhaften Angaben des Klägers ist der Senat weiter davon überzeugt, dass dieser nicht bereits vor dem hier streitgegenständlichen Vorfall Opfer eines sog. Datenlecks geworden ist und bereits bei diesem die Kontrolle über seine Mobilfunknummer verloren hat. Insofern kann nicht festgestellt werden, dass sich das Risiko, auch Dritte könnten seine Telefonnummer nicht datenschutzkonform verarbeitet haben, schon vor dem Scraping auf der Plattform der Beklagten verwirklicht hat. Mag die vom Kläger in seiner Anhörung bestätigte Angabe der Mobilfunknummer beispielsweise bei Bestellungen auf Verkaufsplattformen oder an Internetdienste „*zur Sicherheitserhöhung*“ auch ein gewisses Risiko beinhalten, so ist dies nicht mit dem Kontrollverlust durch das streitgegenständliche Scraping und der dauerhaften Preisgabe der mit dem Namen des Klägers verknüpften Mobilfunknummer im Internet vergleichbar. 27

Dagegen fehlt es an einem Kontrollverlust des Klägers hinsichtlich der weiteren im streitgegenständlichen Datensatz veröffentlichten Daten (A.-ID, Name, Geschlecht, Beziehungsstatus und Arbeitgeber). Denn diese Daten hat der Kläger nach dem unstreitigen Vorbringen der Beklagten öffentlich einsehbar auf seiner Profilseite hinterlegt und damit öffentlich zugänglich gemacht bzw. er hat sie im Rahmen der Registrierung bei der Beklagten angegeben, wobei in der dabei verlinkten Datenrichtlinie darauf hingewiesen wird, dass diese Daten immer – auch von Personen, die nicht auf der Plattform der Beklagten registriert sind – gesehen werden können. Hat der Kläger damit aber bewusst auf eine Kontrolle dieser Daten 28

verzichtet, da sein Profil mit den darauf veröffentlichten Daten nicht nur von jedem anderen Nutzer der Beklagten, sondern – so der schon in erster Instanz unstreitige Vortrag der Beklagten – auch von Dritten, die keine Nutzer des sozialen Netzwerkes sind, wahrgenommen werden konnte, so kommt hinsichtlich dieser ein Kontrollverlust nicht in Betracht.

bb. Der Kontrollverlust über die Mobilfunknummer stellt einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DSGVO dar. Der Senat nimmt insofern Bezug auf die Ausführungen des Bundesgerichtshofs in seiner Entscheidung vom 18.11.2024 (VI ZR 10/24, juris Rn. 27 ff.) unter Bezugnahme auf Entscheidungen des Europäischen Gerichtshofs und schließt sich diesen an. 29

cc. Die mit der Klageschrift behaupteten weitergehenden Folgen, die darin bestehen sollen, dass sich der Kläger wegen des Scraping-Vorfalls und des damit verbundenen Kontrollverlustes in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch der ihn betreffenden Daten befinde, bei jeder digitalen Nachricht einen Betrug fürchte und sich mit dem Datenleck habe auseinandersetzen müssen, haben sich in der persönlichen Anhörung des Klägers allerdings nicht bestätigt 30

Der Kläger, der auf den Senat den Eindruck eines erfahrenen Nutzers digitaler Medien machte, hat entsprechende Ängste und Sorgen verneint. Er hat zwar angegeben, über die ab 2019/2020 bei ihm eingegangenen Spams – häufig SMS, weniger Anrufe – „*total verärgert*“ gewesen zu sein. Weiter hat er angegeben, er sei unter anderem auch nach seinem Schichtdienst von Spam-Anrufen gestört worden, wenn er eigentlich habe schlafen wollen. Unabhängig von der Frage, ob es sich bei den vom Kläger mit insgesamt drei bis vier störenden Anrufen angegebenen Belästigungen schon um solche handelt, die über das hinausgehen, was üblicherweise mit einem Kontrollverlust verbunden ist, können sie eine weitergehende Folge des hier streitgegenständlichen Scrapings nicht begründen. Denn der Kläger hat angegeben, dass die störenden Spam-Anrufe bereits im Jahre 2019 begonnen hätten und hat – auf entsprechende Nachfrage des Senats – erklärt, dass er „*schon vor Corona*“ Spams erhalten habe. Insofern kann schon nach seinen eigenen Angaben nicht festgestellt werden, dass diese Form der Belästigung auf den Datenschutzvorfall bei der Beklagten zurückzuführen ist, hinsichtlich dessen der Kläger selbst vorgetragen und das Landgericht in der angefochtenen Entscheidung insoweit unangegriffen festgestellt hat, dass die dabei abgegriffenen Daten erst im April 2021 im Internet veröffentlicht worden sind. Der im Hinblick auf den Datenschutzvorfall insgesamt gelassenen Einstellung des Klägers entsprechen auch seine weiteren Angaben, wonach er aufgrund des streitgegenständlichen Datenschutzvorfalls weder beabsichtigt, seine Mobilfunknummer zu wechseln („*Das habe ich überlegt, aber das ist mir zu viel Aufwand*“) noch die Plattform der Beklagten zu verlassen. Der Kläger hat auch nicht bekundet, dass er neben der Beauftragung eines Anwalts und neben der von ihm nach eigenen Angaben im Herbst 2024 vorgenommenen Änderung der Suchbarkeitseinstellung weitere Maßnahmen ergriffen hat, um sich mit dem Datenleck auseinanderzusetzen. Vielmehr hat er angegeben, auf der Internetseite seines früheren Prozessbevollmächtigten einen Test hinsichtlich der Betroffenheit seiner Telefonnummer durchgeführt zu haben „*und dann war ich dabei*“. 31

d. Der nach Anhörung des Klägers festgestellte Kontrollverlust in Form der Preisgabe seines Pseudonyms mit der Mobilfunknummer im Internet ist kausal auf den Datenschutzverstoß der Beklagten zurückzuführen. Die Beklagte selbst nennt keine alternative Ursache dafür, dass die Mobilfunknummer des Klägers in Kombination mit seinem Namen auf den genannten Internetseiten – dies in Kombination mit der sog. A.-ID und damit 32

einer Nutzungskennung gerade der Plattform der Beklagten – veröffentlicht worden ist. Es kommt im Hinblick auf diesen Kontrollverlust nicht darauf an, ob und welche Spam-SMS/-Anrufe gerade auf dem Scrapingvorfall bei der Beklagten und der Veröffentlichung dieser Daten im Internet beruhen.

e. Für den vom Kläger erlittenen Kontrollverlust über seine Mobilfunknummer hält der Senat einen Schadensersatzanspruch in Höhe von 100 Euro für angemessen. 33

Nach den Ausführungen des Bundesgerichtshofs im Urteil vom 18.11.2024 (VI ZR 10/24, juris Rn. 93) richtet sich die Bemessung des immateriellen Schadensersatzes gemäß Art. 82 Abs. 1 DSGVO nach den innerstaatlichen Vorschriften und somit vorliegend nach § 287 ZPO unter Berücksichtigung des Äquivalenz- und des Effektivitätsgrundsatzes. Der Senat hat bei Ausübung seines ihm im Rahmen von § 287 ZPO zustehenden Schätzungsermessens hier zunächst berücksichtigt, dass die vom Datenschutzverstoß der Beklagten betroffenen personenbezogenen Daten des Klägers nicht besonders sensibel wie beispielsweise diejenigen des Art. 9 Abs. 1 DSGVO sind, sondern vielmehr im Rahmen des täglichen (Geschäfts-) Lebens üblicherweise einer Vielzahl von Personen mitgeteilt werden. Die Mobilfunknummer bezweckt typischerweise die Kontaktaufnahme mit anderen Menschen und wird gerade zu diesem Zweck verwendet. Auf der anderen Seite ist in den Blick zu nehmen, dass Name und Mobilfunknummer des Klägers infolge des Scrapingvorfalls einem unbegrenzten Empfängerkreis für einen (bisher) mehrjährigen Zeitraum zugänglich gemacht wurden und dass es – anderes macht die Beklagte nicht geltend – nicht möglich sein wird, den entsprechenden Datensatz des Klägers wieder dauerhaft und vollständig aus dem Internet zu entfernen. Insofern kann als effektiver Ausgleich für den vom Kläger erlittenen immateriellen Schaden in Form eines Kontrollverlustes und den damit für ihn – wie für jedermann – unmittelbar zusammenhängenden Unannehmlichkeiten ein Betrag in Höhe von 100 Euro angesetzt werden, um den Schaden vollständig und wirksam auszugleichen. Hiermit ist jedenfalls der hypothetische Aufwand für die Wiedererlangung der Kontrolle im Wege eines Rufnummernwechsels abgegolten. Dass hierzu ein höherer Betrag erforderlich wäre, ist weder dargetan noch sonst ersichtlich. 34

Soweit der Kläger geltend gemacht hat, der Europäische Gerichtshof habe in seiner Entscheidung vom 8.1.2025 (T-354/22, juris) für den Kontrollverlust über eine IP-Adresse einen Schadensersatzanspruch gegen die Kommission wegen Verstoß gegen Art. 46 der Verordnung 2018/1725 in Höhe von 400 Euro zuerkannt, zwingt dies im vorliegenden Fall nicht zu einer höheren Schätzung desjenigen Betrages, der für einen effektiven Ausgleich des vom Kläger erlittenen immateriellen Schadens erforderlich ist. Die vorliegende Schätzung richtet sich – wie oben dargelegt – zum einen nach innerstaatlichem Recht und wird daher durch eine Entscheidung zu einem Verstoß gegen sonstige europarechtliche Regelungen nicht unmittelbar beeinflusst. Zum anderen ist den Gründen des EuGH-Urteils auch nicht zu entnehmen, welche konkreten Umstände für die Bemessung des Ersatzanspruchs ausschlaggebend waren. Vielmehr beschränken sich die Gründe insofern auf den Satz „*Unter den Umständen des vorliegenden Falles hält das Gericht wegen des immateriellen Schadens, den die Kommission verursacht hat, eine Entschädigung in Höhe von 400 Euro für angemessen.*“ 35

f. Ein Mitverschulden des Klägers am Kontrollverlust hinsichtlich seiner Mobilfunknummer kann nicht festgestellt werden. Soweit die Beklagte darauf abstellt, der Kläger habe seine Suchbarkeitseinstellungen nach dem Vorfall zunächst nicht geändert und auch seine Mobilfunknummer beibehalten, ändert dies nichts. Denn dieses Verhalten des Klägers hat unstreitig erst nach dem streitgegenständlichen Scraping stattgefunden und 36

konnte damit auf den Kontrollverlust als solchen keine Auswirkung haben.

2. Der Kläger hat einen Anspruch auf Feststellung, dass die Beklagte verpflichtet ist, ihm künftige materielle und künftige derzeit noch nicht vorhersehbare immaterielle Schäden zu ersetzen, die ihm durch den unbefugten Zugriff auf das Datenarchiv der Beklagten im Zeitraum ab dem 25.5.2018 bis September 2019 entstehen. 37

a. Der Antrag ist zulässig, weil die Möglichkeit des Eintritts künftiger Schäden zu bejahen ist. Der Kläger wurde durch den von der Beklagten begangenen Verstoß gegen die DSGVO in seinem Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG bzw. in seinem Recht auf Schutz der personenbezogenen Daten gemäß Art. 8 GRCh verletzt. Aufgrund der unstreitig fortdauernden Veröffentlichung der personenbezogenen Daten des Klägers besteht das Risiko einer missbräuchlichen, insbesondere betrügerischen Verwendung fort. 38

b. Der Feststellungsantrag ist auch begründet, weil die Beklagte – wie oben dargelegt – zu Lasten des Klägers schuldhaft gegen die DSGVO verstoßen hat und ihm damit dem Grunde nach ein Anspruch auf Ersatz der künftigen materiellen Schäden aus Art. 82 Abs. 1 DSGVO zusteht. 39

3. Der Kläger hat gegen die Beklagte einen Anspruch auf Unterlassung der Verarbeitung seiner Telefonnummer, soweit die Verarbeitung über die Zwei-Faktor-Authentifizierung und die Accountsicherung hinausgeht (Antrag zu 3b). Der Unterlassungsantrag zu 3a) ist dagegen unzulässig. 40

a. Der im Schriftsatz vom 16.12.2024 in einer geänderten Form gestellte Antrag zu 3a) ist unzulässig, so dass es auf die Frage, ob eine Zustimmung der Beklagten erforderlich war, im Ergebnis nicht ankommt. Dem Antrag fehlt es an der notwendigen Bestimmtheit (§ 253 Abs. 2 Nr. 2 ZPO). 41

Der Kläger verlangt mit seinem geänderten Antrag die Unterlassung der Verarbeitung bestimmter Daten über das CIT, ohne dass die Beklagte „*Sicherheitsmaßnahmen*“ vorhält. Diese Sicherheitsmaßnahmen werden im Antrag zwar teilweise dahingehend konkretisiert, dass der Kläger Maßnahmen in Form von „*Sicherheits-Captchas*“ bzw. die „*Überprüfung massenhafter IP-Abfragen*“ aufführt. Dabei handelt es sich jedoch nur um beispielhafte Angaben, die zum einen ebenfalls nicht inhaltlich konkretisiert sind und die zum anderen im Folgenden durch die Formulierung „*vergleichbare*“ Sicherheitsmaßnahmen wieder inhaltlich relativiert werden. Wann genau aus Sicht des Klägers eine „*massenhafte*“ IP-Abfrage vorliegt bzw. was „*vergleichbare*“ Sicherheitsmaßnahmen sein sollen, wird weder im Antrag noch im entsprechenden Schriftsatz näher erläutert. Der Kläger trägt in diesem Zusammenhang nur vor, dass er die vom Bundesgerichtshof als zu unbestimmt gerügten Begriffe präzisiert habe. Auch die nunmehr verwendeten Formulierungen lassen für die Beklagte aber nicht sicher erkennen, wie die Verarbeitung über das CIT künftig gestaltet werden soll. 42

Selbst wenn man den Antrag zu 3a) als zulässig ansehen würde, würde es ihm jedenfalls am Rechtsschutzbedürfnis fehlen. Der Unterlassungsanspruch richtet sich allein gegen die Verarbeitung der personenbezogenen Daten des Klägers im Rahmen des sog. CIT, wobei der Kläger darauf abstellt, dass dieses Programm bei Eingabe seiner Telefonnummer den Zugriff auf weitere Daten und deren Verknüpfung mit der Telefonnummer ermöglicht. Genau diese Verarbeitung seiner Telefonnummer kann der Kläger aber ohne weiteres durch Änderung der Suchbarkeitseinstellungen, über die er bereits außergerichtlich, spätestens aber seit der ersten Instanz hinreichend informiert ist und die er nach eigenem Vorbringen 43

auch vorgenommen hat, selbst beschränken bzw. ausschließen.

b. Der Antrag zu 3b) ist dagegen zulässig und begründet. 44

aa. Auf Basis der Ausführungen des Bundesgerichtshofs im Urteil vom 18.11.2024 (VI ZR 10/24, juris) ist der – vorliegend in identischer Form wie im vom Bundesgerichtshof entschiedenen Verfahren gestellte – Antrag zu 3b) dahingehend auszulegen, dass der Kläger über seine Einwendungen gegen das CIT hinaus die Unterlassung einer Verarbeitung seiner Telefonnummer verlangt, die über die Zwei-Faktor-Authentifizierung und die Accountsicherung hinausgeht. Zwar hat er in Reaktion auf die oben genannte Entscheidung des Bundesgerichtshofs seinen Antrag nicht entsprechend umgestellt. Dies steht einer Auslegung durch den Senat im Hinblick auf das erkennbare Klageziel aber nicht entgegen. Auch vorliegend hatte der Kläger bereits in erster Instanz vorgetragen und dies im Rahmen seiner persönlichen Anhörung auch bestätigt, er sei davon ausgegangen, dass seine Telefonnummer ausschließlich zum Zwecke der Accountsicherung bzw. der Wiederherstellung seines Passwortes hinterlegt wird, so dass das Klageziel, welches der Bundesgerichtshof im Parallelverfahren im Wege der Auslegung des Antrags angenommen hat, auch im vorliegenden Verfahren gegeben ist. 45

Dieser Antrag ist zulässig; insbesondere ist das erforderliche Rechtsschutzbedürfnis gegeben. Die Beklagte hat auch im nachgelassenen Schriftsatz vom 13.3.2025 nicht vorgetragen, dass und wie der Kläger eine Verarbeitung seiner Mobilfunknummer für Werbung und Vorschläge – wie in der Information Anlage B6 aufgeführt – „ausschalten“ könnte und ihm damit ein einfacherer Weg als ein Klageverfahren zur Verfügung stünde. Soweit sie in diesem Schriftsatz vorträgt, es gebe „*mehrere einfacherer Möglichkeiten, mit denen die Klagepartei die Verwendung der Telefonnummer einschränken*“ könne, fehlt es an Angaben zu konkreten Möglichkeiten des Klägers, die Einstellungen für die Verarbeitung seiner Telefonnummer so zu ändern, dass sie von Seiten der Beklagten nur noch für die Zwei-Faktor-Authentifizierung und für die Accountsicherung verwendet wird. 46

Soweit die Beklagte in diesem Schriftsatz darauf verweist, dass der Kläger die Möglichkeit habe, seine Telefonnummer aus dem Nutzerkonto zu löschen und sodann „*weiterhin Zugang zu zwei anderen Methoden der Zwei-Faktor-Authentifizierung*“ habe, ist dieser Vortrag schon prozessual unzureichend, weil die Beklagte nicht konkret darlegt, welche Möglichkeiten dem Kläger insoweit zu Verfügung stehen, sondern nur auf das „A. S.“ verweist. Im Übrigen wäre auch mit solchen angeblichen alternativen Möglichkeiten das Rechtsschutzbedürfnis nicht zu verneinen: Der Kläger verfolgt vorliegend das Rechtsschutzziel, auf der Plattform der Beklagten seine Mobilfunknummer für die Zwei-Faktor-Authentifizierung zu nutzen, während die Beklagte eine darüber hinausgehende Nutzung der Nummer unterlassen soll. Dieses Rechtsschutzziel wird aber nicht dadurch erreicht, dass der Kläger – der sich für eine der von der Beklagten frei zur Verfügung gestellten Möglichkeiten der Zwei-Faktor-Authentifizierung entschlossen hat – nunmehr gezwungen wird, seine Telefonnummer vom Profil zu löschen und eine andere Möglichkeit der Zwei-Faktor-Authentifizierung zu nutzen. 47

Auch die von der Beklagten angeführte Möglichkeit, die Telefonnummer aus dem Nutzerkonto zu entfernen und sie anschließend „*für die Zwei-Faktor-Authentifizierung erneut zu registrieren*“, ist kein einfacherer Weg, das vom Kläger verfolgte Rechtsschutzziel zu erreichen. Denn insofern ergibt sich aus dem von der Beklagten vorgelegten Screenshot (Anlage B21), dass die Telefonnummer des Nutzers auch in diesem Fall wiederum zu weiteren Zwecken als die der Zwei-Faktor-Authentifizierung und Accountsicherung verarbeitet wird („*Diese Telefonnummer wird für die zweistufige Authentifizierung und die Anmeldung aktiviert. Möglicherweise verwenden wir sie außerdem, um unsere Community zu schützen,* 48

um die genaue Anzahl der Personen zu erfassen, die unsere Dienste nutzen, und um dich beim Zugriff auf A. und optionale Programme zu unterstützen … Falls die hier verwendete Nummer auch in anderen Produkten der A.-Unternehmen angegeben wurde, kann sie möglicherweise auch für andere Zwecke genutzt werden, etwa um die Freundschaftsvorschläge oder Werbung zu zeigen“). Eine Begrenzung der Verarbeitung, wie sie der Kläger mit der vorliegenden Klage verlangt, kann also auch über diesen Weg nicht erreicht werden.

bb. Der Antrag zu 3b) ist auch begründet, weil der Kläger verlangen kann, dass die Beklagte die Verarbeitung seiner Telefonnummer unterlässt, soweit diese über die Verarbeitung für die Zwei-Faktor-Authentifizierung bzw. für die Accountsicherung („Passwort vergessen“) hinausgeht. Ein solcher Anspruch ergibt sich aus § 280 Abs. 1 BGB, weil die Beklagte mit der konkreten Datenverarbeitung vertragliche Nebenpflichten zu Lasten des Klägers verletzt hat. 49

(1) Mit der Registrierung des Klägers auf der Plattform der Beklagten ist zwischen den Parteien ein vertragliches Nutzungsverhältnis sui generis zustande gekommen, in dessen Rahmen sich die Beklagte dazu verpflichtet hat, dem Kläger die Funktionen und Dienstleistungen, die sie über ihre Webseiten anbietet, unentgeltlich zur Nutzung zur Verfügung zu stellen, wofür sie im Gegenzug vom Kläger dessen Daten beanspruchen kann, um diese (wohl) für Werbezwecke verwenden zu können (vgl. BGH, Urt. v. 12.7.2018 – III ZR 183/17, NJW 2018, 3178; OLG München, Urt. v. 18.2.2020 – 18 U 3465/19, juris; OLG München, Beschl. v. 24.8.2018 – 18 W 1294/18, juris; OLG Stuttgart, Beschl. v. 6.9.2018 – 4 W 63/18, juris; OLG Oldenburg, Urt. v. 1.7.2019 – 13 W 16/19, juris). Dieser Nutzungsvertrag unterliegt deutschem Recht, was sich gemäß Art. 3 Abs. 1, Art. 6 Abs. 2 Rom I-VO aus der Rechtswahlklausel in Nummer 4.4 der Nutzungsbedingungen der Beklagten ergibt. Im Übrigen wäre gemäß Art. 6 Abs. 1 b) Rom I-VO auch ohne eine entsprechende Rechtswahl deutsches Recht anzuwenden, weil es sich bei dem Nutzungsvertrag um einen Verbrauchervertrag im Sinne dieser Vorschrift handelt (vgl. BGH, Urt. v. 27.1.2022 – III ZR 3/21, juris Rn. 15). 50

(2) In der Rechtsprechung ist anerkannt, dass sich aus § 280 Abs. 1 BGB im Fall der Verletzung vertraglicher (Neben-)Pflichten nicht nur ein Schadensersatzanspruch, sondern grundsätzlich auch ein Anspruch auf Unterlassung jedenfalls dann ergeben kann, wenn die Verletzungshandlung noch andauert bzw. der daraus resultierende Schaden noch nicht irreparabel ist (vgl. BGH, Urt. v. 2.5.2024 – I ZR 12/23, NJW 2024, 3375). Ein solcher Unterlassungsanspruch setzt eine Erstbegehungs- oder Wiederholungsgefahr voraus. Nichts anderes gilt bei der Verletzung von – nicht ausdrücklich vereinbarten und gesetzlich nicht ausdrücklich normierten – Rücksichtnahmepflichten im Sinne von § 241 Abs. 2 BGB, durch die die Erreichung des Vertragszwecks bedroht wird. Ob nach dem Inhalt des Schuldverhältnisses entsprechende Rücksichtnahmepflichten bestehen, ist durch Auslegung der vertraglichen Vereinbarung zu ermitteln (BGH, Urt. v. 2.5.2024 – I ZR 12/23, NJW 2024, 3375). 51

Unter Berücksichtigung dieser Grundsätze besteht die vertragliche (Neben-) Pflicht der Beklagten, die vom Kläger zur Verfügung gestellten personenbezogenen Daten nach Maßgabe der gesetzlichen Vorschriften (DSGVO) zu verarbeiten bzw. für ihren hinreichenden Schutz zu sorgen. Denn der Kläger überlässt der Beklagten im Rahmen des vertraglichen Verhältnisses seine Daten zum Zwecke der Erfüllung der vertraglichen Zwecke und darf damit darauf vertrauen, dass sie auf den Servern der Beklagten entsprechend den gesetzlichen Vorschriften behandelt werden bzw. dass der von ihm erklärte Umfang der 52

Datenüberlassung beachtet wird.

(3) Diese Pflichten hat die Beklagte verletzt, weil es im Rahmen der Nutzung des CIT zumindest wegen datenschutzwidriger Voreinstellungen zu einem Zugriff Dritter kam und weil die Beklagte nicht dargelegt hat, dass der Kläger in die Verarbeitung seiner Telefonnummer zum Zwecke der Werbung und Unterbreitung von Vorschlägen eingewilligt hat. 53

Aus den Nutzungsbedingungen der Beklagten, die für den Umfang der zulässigen Datenverarbeitung maßgeblich sind, ergibt sich nicht mit hinreichender Deutlichkeit, dass die Beklagte die Telefonnummer des Klägers zu diesen Zwecken verwenden wird, so dass aus der Einwilligung mit den Nutzungsbedingungen keine Einwilligung des Klägers in die betreffende Datenverarbeitung folgt. Zwar hat der Kläger sich durch Zustimmung zu den Nutzungsbedingungen damit einverstanden erklärt, dass die Beklagte ihm Vorschläge hinsichtlich anderer Nutzer unterbreitet (vgl. Ziff. 1 der Nutzungsbedingungen „„*Zitat wurde entfernt*““). Ebenso hat der Kläger in die Übersendung von Werbeanzeigen eingewilligt (vgl. Ziff. 1 der Nutzungsbedingungen „„*Zitat wurde entfernt*““). Allerdings wird in den Nutzungsbedingungen nicht aufgeführt, welche konkreten Daten des Klägers gerade für diese Zwecke verwendet werden sollen; insbesondere ist nicht ausdrücklich aufgeführt, dass – auch – die Telefonnummer des Klägers in diesem Rahmen verarbeitet wird, so dass es sich seinerseits gerade nicht um eine „*informierte und freiwillige*“ Entscheidung im Sinne von Art. 4 Nr. 11 DSGVO handelt. Der Hinweis in Anlage B6, der ebenfalls nur pauschal gehalten ist, genügt in diesem Zusammenhang ebenfalls nicht. 54

(4) Hinsichtlich der Pflichtverletzung der Beklagten im Rahmen der CIT-Nutzung fehlt es zwar an einer Wiederholungsgefahr. Denn zum einen hat die Beklagte das CIT in einer Weise überarbeitet, dass Angriffe von Scrapern, wie streitgegenständlich geschehen, für die Zukunft ausgeschlossen werden können. Zum anderen kann der Kläger, wenn er trotz dieser Änderung des CIT noch weitere Angriffe von Scrapern in diesem Bereich befürchtet, seine Telefonnummer einer derartigen Verarbeitung ohne weiteres – durch eine Änderung der Suchbarkeitseinstellung – entziehen. Sein Vortrag, wonach auch die Deaktivierung der Suchbarkeitsfunktion durch die Beklage und das Vorhalten sog. „Anti-Scraping-Maßnahmen“ nichts daran ändere, dass die Gefahr eines Zugriffs von Dritten weiterhin bestehe, ist zum einen völlig pauschal und berücksichtigt zum anderen nicht den konkreten Streitgegenstand. Sollte es den Scrapern künftig gelingen, auf eine andere Art und Weise als über das CIT personenbezogene Daten der Nutzer von der Plattform der Beklagten abzugreifen, wäre das nicht die hier angegriffene Verletzungsform, sondern ein anderer (neuer) Vertragsverstoß. 55

Jedoch ist die Wiederholungsgefahr hinsichtlich der weiteren Pflichtverletzungen der Beklagten in Form der Verarbeitung der Telefonnummer des Klägers für Werbung bzw. Vorschläge ohne weiteres zu bejahen. Die Beklagte hat diese nicht widerlegt. Sie hat weder vorgetragen, dass die betreffenden Funktionen beim Kläger deaktiviert sind (die Telefonnummer wird also zu diesen Zwecken verarbeitet) noch, dass es eine Möglichkeit für den Kläger gibt, diese Verarbeitung selbst zu unterbinden. Entgegen dem Vortrag der Beklagten im Schriftsatz vom 13.3.2025 ist daher von einer andauernden Vertragsverletzung auszugehen. Die Beklagte trägt dort zum einen vor, dass der Kläger seine Kontoeinstellungen ändern könne, um zu kontrollieren, wem sein Nutzerprofil auf Grundlage der Telefonnummer vorgeschlagen wird. Die Änderung einer solchen Einstellung hätte aber – die Beklagte trägt dazu nichts Gegenteiliges vor – keine Auswirkung darauf, dass sie die Telefonnummer des Klägers verarbeitet, um ihm Werbung zu zeigen. Die Beklagte trägt zum anderen nur pauschal vor, der Kläger könne seine Telefonnummer aus dem Konto entfernen, und hätte dann „*weiterhin Zugang zu zwei anderen Methoden der Zwei-Faktor-* 56

Authentifizierung“. Um welche Methoden es sich dabei handelt, erläutert die Beklagte – wie vorstehend bereits ausgeführt – jedoch nicht, sondern verweist prozessual unzureichend lediglich auf Ausführungen im „A. S.“, die dem Schriftsatz nicht beigefügt sind.

4. Der Kläger hat weiter einen Anspruch auf Erstattung außergerichtlicher Anwaltskosten für die mit Schreiben vom 15.10.2021 (Anlage K1) erfolgte Geltendmachung seiner Ansprüche auf Schadensersatz und Unterlassung. Denn damit hat er die nach den obigen Ausführungen berechtigten Ansprüche aus dem Antrag zu 1) bzw. zu 3b) gegen die Beklagte mit – insoweit notwendiger – anwaltlicher Hilfe geltend gemacht. Dagegen ist das nach den obigen Ausführungen ebenfalls begründete Feststellungsbegehren hinsichtlich künftiger Schäden in diesem Schreiben nicht geltend gemacht worden und kann daher bei der Bestimmung des Gegenstandswertes für die Anwaltsgebühren nicht herangezogen werden. Bei einem damit anzusetzenden Gegenstandswert von 850 Euro (100 Euro für den Schadensersatzanspruch und 750 Euro für den Unterlassungsanspruch) ergibt sich bei Ansatz einer 1,3-Verfahrensgebühr nebst Auslagenpauschale und Umsatzsteuer ein Erstattungsanspruch in Höhe von 159,94 Euro. 57

5. Die prozessualen Nebenentscheidungen ergeben sich hinsichtlich der Kosten aus §§ 92 Abs. 1 S. 1, 269 Abs. 3 S. 2 ZPO und hinsichtlich der vorläufigen Vollstreckbarkeit aus §§ 708 Nr. 10, 713 ZPO bzw. § 709 S. 1 ZPO 58

6. Die Zulassung der Revision kam nicht in Betracht, da die Voraussetzungen des § 543 ZPO nicht vorliegen. 59
