
Datum: 22.05.2025
Gericht: Oberlandesgericht Düsseldorf
Spruchkörper: 16. Zivilsenat
Entscheidungsart: Urteil
Aktenzeichen: 16 U 185/24
ECLI: ECLI:DE:OLGD:2025:0522.16U185.24.00

Vorinstanz: Landgericht Düsseldorf, 9a O 138/23
Schlagworte: Scraping
Normen: DSGVO Art. 82 Abs. 1

Tenor:

Auf die Berufung des Klägers wird das am 7. Juni 2024 verkündete Urteil der 9a. Zivilkammer des Landgerichts Düsseldorf (9a O 138/23) unter Zurückweisung des weitergehenden Rechtsmittels teilweise abgeändert und insgesamt wie folgt neu gefasst:

Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von 100 € zu zahlen nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 13. Juli 2023.

Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen materiellen Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, noch entstehen werden.

Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 €, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, die Telefonnummer des Klägers für andere Zwecke als die der Zwei-Faktor-Authentifizierung auf Grundlage einer

Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der A.-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.

Im Übrigen wird die Klage abgewiesen.

Von den Kosten des Rechtsstreits in beiden Instanzen haben der Kläger 60 % und die Beklagte 40 % zu tragen.

Das Urteil ist vorläufig vollstreckbar, wegen der Unterlassungsverpflichtung gegen Sicherheitsleistung in Höhe von 800 € und im Übrigen gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages.

Die Revision wird nicht zugelassen.

Gründe

I.

Der Kläger verfolgt in der Berufungsinstanz gegen die Beklagte zuletzt – nach teilweiser Klagerücknahme im Umfang seines Auskunftsantrags – noch Ansprüche gerichtet auf Schadensersatz, auf die Feststellung zukünftiger Ersatzpflicht und auf Unterlassung aufgrund angenommener Datenschutzverstöße der Beklagten im Zusammenhang mit einem sogenannten Datenabgriff („Scraping“) in dem von der Beklagten betriebenen sozialen Netzwerk A.

Der Kläger nutzt seit vielen Jahren einen A.-Account, der mit seiner E-Mail-Adresse „000000@000000.de“ verknüpft ist. Bei seiner Anmeldung bei A. machte er von der fakultativen Möglichkeit Gebrauch, dort auch seine Mobilfunknummer zu hinterlegen. Eine solchermaßen zum Profil hinzugefügte Mobilfunknummer ließ sich von allen auf A. registrierten Nutzern auch dann suchen, wenn sie von dem die Telefonnummer einstellenden A.-Nutzer in der für andere Nutzer eröffneten Zielgruppenauswahl nicht als „öffentlich“ und damit als für andere im Grundsatz nicht sichtbar eingestellt war. Die Standardeinstellungen auf der A.-Plattform der Beklagten sahen in der sogenannten Suchbarkeitseinstellung bis zu einer späteren Änderung durch die Beklagte eine Suchbarkeit durch „alle“ vor. Des Weiteren bestand für A.-Nutzer über die sogenannte Kontakt-Import-Funktion, mit der es möglich war, Telefonkontakte vom Smartphone in den sogenannten Messenger von A. hochzuladen, die Möglichkeit, diejenigen Kontakte zu finden und mit ihnen auf A. in Verbindung zu treten, die auf der A.-Plattform unter Angabe ihrer Rufnummer ebenfalls registriert waren. Um eine Suchbarkeit über die Suchfunktion auf der Plattform und über die Kontakt-Import-Funktion auszuschließen oder einzuschränken, war es ursprünglich erforderlich, die A.-Standardeinstellungen zu ändern.

Aus der Suchfunktion auf der Plattform sowie aus der Kontakt-Import-Funktion ergab sich die technische Möglichkeit, eine Vielzahl von Ziffernfolgen nach Art gängiger

1

2

3

4

5

Rufnummernformate zu nutzen, um auf der A.-Plattform nach dazu passenden Nutzern zu suchen. Stimmte eine generierte Nummer mit der hinterlegten Mobilfunknummer eines Nutzers überein, so wurden dessen öffentliche Nutzerinformationen der eingegebenen Nummer zugeordnet und abgerufen. Ab Januar 2018 kam es durch Unbekannte unter Nutzung dieser Möglichkeit zu einem massenhaften Abgriff von Daten von A.-Accounts, von dem auch der Kläger betroffen war. Im Jahr 2021 tauchten abgegriffene Daten im Internet auf. Die Beklagte bestätigte dem Kläger mit einem Schreiben vom 9. Januar 2023 (Anlage B16, Bl. 49-72 Anlagenband Beklagte), dass nach ihren Informationen durch das Scraping von den Einzeldaten des Klägers die „Nutzer ID“, der Vorname, der Nachname und das Geschlecht abgeschöpft worden seien.

Von einer weitergehenden Darstellung des Tatbestands wird gemäß § 540 Abs. 2, § 313a Abs. 1 Satz 1 ZPO abgesehen, weil ein Rechtsmittel gegen die Entscheidung gemäß § 543, § 544 Abs. 2 Nr. 1 ZPO nicht zulässig ist. 6

II. 7

Die Berufung des Klägers ist zulässig und hat in dem aus dem Tenor ersichtlichen Umfang teilweise Erfolg. 8

1. 9

Die auch in der Berufungsinstanz von Amts wegen zu prüfende internationale Zuständigkeit der deutschen Gerichte folgt aus Art. 82 Abs. 6 i.V.m. Art. 79 Abs. 2 Satz 1 DSGVO, weil der Kläger als betroffene Person seinen gewöhnlichen Aufenthalt in Deutschland hat und die Datenschutz-Grundverordnung nach dem Vorbringen der Parteien in zeitlicher, sachlicher und räumlicher Hinsicht anwendbar ist. 10

Der zeitliche Anwendungsbereich der gemäß Art. 99 Abs. 2 DSGVO am 25. Mai 2018 in Geltung getretenen Datenschutz-Grundverordnung ist eröffnet. Zwischen den Parteien war erstinstanzlich gemäß § 138 Abs. 3 ZPO unstreitig, dass der Kläger erst im Jahr 2019 und damit zur Zeit der Geltung der Datenschutz-Grundverordnung von möglichen Datenschutzverstößen der Beklagten durch das Abschöpfen seiner eigenen personenbezogenen Daten betroffen war. Dem entsprechenden Vorbringen des Klägers ist die Beklagte nicht entgegengetreten. Soweit sie den Zeitpunkt der Betroffenheit des Klägers erstmals zum Ende der Berufungsinstanz in Abrede stellt, kann sie hiermit gemäß § 531 Abs. 2 Satz 1 Nr. 3 ZPO nicht mehr gehört werden, weil sie nicht dargelegt hat, warum sie diesen Vortrag nicht schon in erster Instanz hätte halten können. 11

Der sachliche Anwendungsbereich der Datenschutz-Grundverordnung ist ebenfalls eröffnet. Gemäß Art. 2 Abs. 1 DSGVO gilt die Datenschutz-Grundverordnung unter anderem für die automatisierte Verarbeitung personenbezogener Daten. Bei den hier im Fokus stehenden Daten des Klägers, die sich in dem sogenannten Leak-Datensatz („000000,000000, B.,male,,,,,7/3/2018 12,00,00 AM“) wiederfinden, den der Kläger im Laufe des Verfahrens vorgelegt hat, handelt es sich um solche personenbezogenen Daten, weil sie sich gemäß der Definition in Art. 4 Nr. 1 DSGVO auf eine identifizierte – betroffene – Person beziehen. Diese Daten wurden, jedenfalls soweit es um die Angaben der Mobilfunknummer, der A.-ID, des Namens und des Geschlechts („male“) ging, von der Beklagten im Rahmen des von ihr betriebenen sozialen Netzwerks A. automatisiert verarbeitet. 12

Schließlich ist auch der räumliche Anwendungsbereich der Datenschutz-Grundverordnung eröffnet. Gemäß Art. 3 Abs. 1 DSGVO findet die Datenschutz-Grundverordnung auf die 13

Verarbeitung personenbezogener Daten Anwendung, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen in der Europäischen Union erfolgt. Bei der Beklagten handelt es sich um ein Unternehmen nach dem Recht der irischen Republik mit Sitz in Irland, mithin mit einer Niederlassung innerhalb der Europäischen Union. Da die Beklagte das soziale Netzwerk A. für Nutzer in der Europäischen Union betreibt, ist sie auch Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO.

Neben der DSGVO ist auf das Rechtsverhältnis der Parteien gemäß Art. 3 Abs. 1, Art. 6 Abs. 2 Rom I-VO deutsches Recht anwendbar, weil die Parteien dies mit den Nutzungsbedingungen der Beklagten so vereinbart haben. 14

2. 15

Der auf Ersatz eines immateriellen Schadens gerichtete Klageantrag zu 1. ist zulässig und auch teilweise begründet. Dem Kläger steht gegen die Beklagte ein Anspruch auf Schadensersatz nach Art. 82 Abs. 1 DSGVO in Höhe von 100 € nebst Zinsen ab Rechtshängigkeit zu. 16

a) 17

Entgegen der Ansicht der Beklagten begegnet der Antrag nicht schon Bestimmtheitsbedenken. Wie der Kläger klargestellt hat, stützt er sein Klagebegehren nicht auf eine unzulässige Häufung alternativer Klagegründe oder Streitgegenstände. Vielmehr geht es ihm um den Ersatz eines immateriellen Schadens, der sich aus mehreren Datenschutzverstößen der Beklagten ergeben haben soll. Insoweit nimmt der Kläger auf den einen von ihm beschriebenen Scraping-Vorfall Bezug, von dem er im Jahr 2019 betroffen war. Damit liegt dem geltend gemachten Schadensersatzanspruch aber ein eindeutig abgrenzbarer, einheitlicher Lebenssachverhalt und damit ein einheitlicher Streitgegenstand zugrunde (siehe BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 18). 18

Da es bei Klagen, die auf Ersatz immaterieller Schäden gerichtet sind, keiner Bezifferung des Anspruchs bedarf, sondern vielmehr ausreicht, wenn vom Kläger eine Mindestvorstellung mitgeteilt wird, auf die sich der Ersatzbetrag belaufen soll, konnte der Kläger seinen Antrag auch wie geschehen unter Nennung eines Mindestbetrags formulieren. 19

b) 20

Der zulässige Antrag ist in der Hauptsache auch teilweise begründet. Gemäß Art. 82 Abs. 1 DSGVO setzt ein Schadensersatzanspruch nach dieser Vorschrift einen Verstoß des Verantwortlichen gegen die Datenschutz-Grundverordnung, den Eintritt eines Schadens sowie einen Kausalzusammenhang zwischen dem Verstoß und dem Schaden voraus (vgl. auch EuGH, Urteile vom 4. Mai 2023 – C-300/21, ZIP 2023, 1244, 1246, Rn. 32, und vom 25. Januar 2024 – C-687/21, DB 2024, 519, 523, Rn. 58). Die Beklagte hat nicht nur gegen die Datenschutz-Grundverordnung verstoßen, sondern der Kläger hat dadurch auch einen ersatzfähigen immateriellen Schaden erlitten. Einen ihm durch Datenschutzverstöße der Beklagten entstandenen materiellen Schaden macht der Kläger nicht geltend. 21

aa) 22

Der von Art. 82 Abs. 1 DSGVO für einen Schadensersatzanspruch verlangte Verstoß gegen die Datenschutz-Grundverordnung liegt vor. Dabei kann hier dahinstehen, ob jeder Verstoß gegen materielle oder formelle Bestimmungen der Datenschutz-Grundverordnung oder erst 23

eine verordnungswidrige Datenverarbeitung im Sinne von Art. 82 Abs. 2 Satz 1 DSGVO einen Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO begründen kann (siehe zum Meinungsstreit OLG Stuttgart, Urteil vom 22. November 2023 – 4 U 20/23, juris, Rn. 381 ff.). Da die Beklagte – wie noch auszuführen ist – personenbezogene Daten des Klägers ohne die nach Art. 6 Abs. 1 DSGVO erforderliche Rechtsgrundlage verarbeitet hat, liegt nicht nur ein Verstoß gegen die Datenschutz-Grundverordnung, sondern auch eine verordnungswidrige Datenverarbeitung vor.

(1) 24

Gemäß Art. 4 Nr. 2 DSGVO fällt unter den Begriff der Datenverarbeitung neben der Offenlegung durch Übermittlung und Verbreitung auch jede andere Form der Bereitstellung personenbezogener Daten. Die auf der A.-Plattform der Beklagten vormals technisch mögliche Suche des Nutzerprofils des Klägers anhand seiner Mobilfunknummer – die ungeachtet der Ungewissheiten über den exakten Ablauf des Scraping-Vorfalles zwischen den Parteien unstreitig ist – stellte eine von der Beklagten ermöglichte Form der Bereitstellung von personenbezogenen Daten des Klägers dar. Die Suchfunktionalität oder Suchbarkeit ermöglichte es anderen Nutzern, das Nutzerprofil des Klägers mit dessen öffentlichen Profildaten mittels Such- oder Kontakt-Import-Funktion anhand seiner Mobilfunknummer zu finden. Den unbekannten „Scrapern“ ermöglichte diese Funktionalität, das Nutzerprofil des Klägers anhand von Nummernfolgen nach Art von Telefonnummern, bei denen es sich mangels Kenntnis von der Telefonnummerneigenschaft einer bestimmten Person zunächst noch nicht um personenbezogene Daten handelte, zu finden und die den Suchtreffer auslösende Ziffernfolge als Mobilfunknummer zu identifizieren und dem Kläger zuzuordnen sowie mit seinen weiteren öffentlichen Nutzerprofildaten nach Art des Leak-Datensatzes zu verknüpfen. 25

(2) 26

Gemäß Art. 6 Abs. 1 Unterabs. 1 DSGVO ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn eine der dort genannten Voraussetzungen beziehungsweise Rechtsgrundlagen für die Verarbeitung vorliegt. Die Darlegungs- und Beweislast für eine rechtmäßige Datenverarbeitung trägt nach Art. 5 DSGVO der Verantwortliche (EuGH, Urteil vom 4. Juli 2023 – C-252/21, juris, Rn. 95), hier also die Beklagte. Danach war die Datenverarbeitung rechtswidrig. Für die Funktionalität, welche die Suchbarkeit des Nutzerprofils des Klägers anhand der Mobilfunknummer ermöglichte, hat die Beklagte keine der Rechtmäßigkeitsbedingungen nach Art. 6 Abs. 1 Unterabs. 1 DSGVO dargelegt. 27

(a) 28

Die Beklagte beruft sich als Rechtsgrundlage für die Suchbarkeit des Nutzerprofils des Klägers anhand seiner Mobilfunknummer auf Art. 6 Abs. 1 Unterabs. 1 Buchst. b DSGVO. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Erfüllung eines Vertrags erforderlich ist. Die Beklagte vertritt insofern die Auffassung, dass die Suchbarkeit des Nutzerprofils des Klägers anhand seiner Mobilfunknummer für die Erfüllung des Hauptzwecks des mit dem Kläger geschlossenen Nutzungsvertrags, die gegenseitige Auffindbarkeit der Nutzer untereinander zwecks Vernetzung miteinander zu ermöglichen, erforderlich gewesen sei. Wörtlich führt sie hierzu in der Berufungserwiderung aus (Bl. 294 GA OLG): 29

„Der zwischen den Parteien geschlossene Nutzervertrag bezieht sich auf die Bereitstellung der A.-Plattform als soziales Netzwerk. Einem solchen sozialen Netzwerk ist es immanent, 30

dass die einzelnen Nutzer (so auch die Klagepartei) Freunde und generell ihnen bekannte Personen finden und sich miteinander vernetzen können. Solche Verknüpfungen werden durch die Verwendung von Funktionen, wie der Kontakt-Importer-Funktion, hergestellt, die, wie im Hilfebereich und in der Datenrichtlinie erläutert, die Telefonnummern von Nutzern erfordern. Die Kontakt-Importer-Funktion ist deswegen ein für Nutzer der A.-Plattform wesentliches Tool. Die Daten werden mithin für die Erfüllung des Nutzervertrags auf Grundlage von Art. 6 Abs. 1 S. 1 lit. b) DSGVO erhoben. Eine Einwilligung i.S.v. Art. 6 Abs. 1 S. 1 lit. a) DSGVO ist in diesem Fall weder relevant noch eine Voraussetzung für die rechtmäßige Datenverarbeitung.“

Entgegen der Ansicht der Beklagten lagen die Voraussetzungen von Art. 6 Abs. 1 Unterabs. 1 Buchst. b DSGVO jedoch nicht vor (siehe OLG Hamm, Urteil vom 15. August 2023 – I-7 U 19/23, juris, Rn. 94 ff.). Die in Art. 6 Abs. 1 Unterabs. 1 Buchst. a bis f DSGVO vorgesehenen Rechtfertigungsgründe sind eng auszulegen (EuGH, Urteil vom 4. Juli 2023 – C-252/21, juris, Rn. 93). Die Verarbeitung personenbezogener Daten ist zur Erfüllung eines Vertrags im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. b DSGVO erforderlich, wenn die Datenverarbeitung objektiv unerlässlich ist, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der Vertragsleistung ist, so dass der Hauptgegenstand des Vertrags ohne die Datenverarbeitung nicht erfüllt werden könnte. Der Umstand, dass die Datenverarbeitung im Vertrag erwähnt wird oder für dessen Erfüllung lediglich von Nutzen ist, genügt nicht. Entscheidend ist, dass die Datenverarbeitung des Verantwortlichen für die ordnungsgemäße Erfüllung des mit dem Betroffenen geschlossenen Vertrags wesentlich ist und dass daher keine praktikablen und weniger einschneidenden Alternativen bestehen (EuGH, Urteil vom 4. Juli 2023 – C-252/21, juris, Rn. 98 f. und 125).

31

Nach diesen Maßgaben war die Suchbarkeit des Nutzerprofils des Klägers anhand seiner Mobilfunknummer nicht erforderlich im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. b DSGVO (so auch OLG Hamm, Urteil vom 15. August 2023 – I-7 U 19/23, juris, Rn. 94 ff., OLG Stuttgart, Urteil vom 22. November 2023 – 4 U 20/23, juris, Rn. 502 ff.). Die Suchbarkeit der Nutzerprofile anhand der Mobilfunknummer war zur Erfüllung des von der Beklagten angeführten Hauptzwecks des Nutzervertrags – die gegenseitige Auffindbarkeit zwecks Vernetzung – nicht unerlässlich. Vielmehr konnten sich die Nutzer gegenseitig zum Beispiel auch über ihre Namen finden (siehe OLG Dresden, Urteil vom 5. Dezember 2023 – 4 U 1094/23, juris, Rn. 34; OLG Oldenburg, Urteil vom 21. Mai 2024 – 13 U 100/23, juris, Rn. 29). Gerade um der entsprechenden Suchmöglichkeit willen ist der Nutzernamen auf der Plattform A. stets öffentlich einsehbar. Dass die Suchbarkeit über die Mobilfunknummer nach der eigenen Bewertung der Beklagten daneben nicht erforderlich war, zeigt sich daran, dass eine Telefonnummer nicht zu den Pflichtangaben zählte, die im Rahmen der Erstanmeldung bei A. anzugeben waren. Vielmehr war die Angabe einer Telefonnummer durch die A.-Nutzer fakultativ. Darüber hinaus konnte die standardmäßige Voreinstellung der Suchbarkeit auch nach der Telefonnummer der Nutzer von diesen abgewählt werden. Die Beklagte hat jene die Telefonnummern betreffende Suchfunktionalität später auch eingeschränkt.

32

(b) 33

Das Vorliegen anderer Rechtsgrundlagen für die Suchbarkeit des Nutzerprofils des Klägers anhand seiner Mobilfunknummer führt die Beklagte nicht an. Sie sind hier auch nicht ersichtlich (siehe OLG Hamm, Urteil vom 15. August 2023 – I-7 U 19/23, juris, Rn. 104 ff.). Insbesondere hat der Kläger nicht in informierter Weise und unmissverständlich gemäß Art. 6 Abs. 1 Unterabs. 1 Buchst. a DSGVO seine Einwilligung in die betreffende Datenverarbeitung erteilt. Das hätte vorausgesetzt, dass die Beklagte den Kläger transparent über die

34

Suchbarkeit des Nutzerprofils anhand der Mobilfunknummer informiert hätte. Das ist jedoch weder dargelegt noch ersichtlich. Die geänderten Nutzungsbedingungen der Beklagten vom 19. April 2018, denen der Kläger zustimmen musste, enthielten ebenso wenig Informationen über die Suchbarkeit des Nutzerprofils anhand der Mobilfunknummer wie die Datenrichtlinie, auf welche die Nutzungsbedingungen Bezug nahmen. Schließlich folgte auch aus der Verlinkung der Privatsphäre-Einstellungen in den Nutzungsbedingungen sowie den Privatsphäre-Tools und Hilfebereichsseiten der Plattform keine transparente Information über die Suchbarkeit anhand der Mobilfunknummer. Der Kläger musste sich mit diesen Informationsmöglichkeiten nicht befassen, sondern durfte wegen Art. 25 Abs. 2 Satz 1 und 3 DSGVO darauf vertrauen, dass die Beklagte die jeweils datenschutzfreundlichsten Voreinstellungen gewählt hatte, die gewährleisteten, dass seine Telefonnummer ohne sein Zutun nur dem kleinstmöglichen Empfängerkreis zugänglich gemacht werden würde (siehe OLG Oldenburg, Urteil vom 14. Mai 2024 – 13 U 114/23, juris, Rn. 22 ff.).

Den Vortrag der Beklagten, er habe die Suchbarkeit seiner Telefonnummer im Jahr 2018 für jedermann bewusst eröffnet, indem er die Suchbarkeitseinstellung von „Friends“ (Freunde) zu „Everyone“ (alle) geändert habe, hat der Kläger in beiden Instanzen bestritten. Zwar hat das Landgericht im unstreitigen Teil des Tatbestands des angefochtenen Urteils für die erste Instanz eine hiervon abweichende Feststellung getroffen. Diese entfaltet jedoch keine Beweiskraft gemäß § 314 Satz 1 ZPO, weil das Urteil insoweit in sich und durch seinen Verweis auf das landgerichtliche Sitzungsprotokoll vom 19. April 2024 widersprüchlich ist (vgl. zum Entfallen der Beweiskraft in solchen Fällen z.B. Seiler, in: Thomas/Putzo, ZPO, 46. Aufl., § 314 Rn. 2). In den Entscheidungsgründen des angefochtenen Urteils (Seite 12 des amtlichen Umdrucks) hat das Landgericht ausgeführt, dass der Kläger im Rahmen seiner persönlichen Anhörung angegeben habe, „bis heute keinerlei Änderungen in seinen Profileinstellungen oder sonstige Schutzmaßnahmen ergriffen zu haben“. Das findet sich in etwas anderer Form auch in dem vom Urteil in Bezug genommenen Protokoll der informatorischen Anhörung des Klägers wieder, wonach dieser auf den Vorhalt der von der Beklagten behaupteten Änderung der Suchbarkeitseinstellung unter anderem bekundet hat: „[...] das habe ich nicht gemacht. Ich hatte keinen Grund, das umzustellen.“ Dass der Kläger mit alledem bestreiten wollte, jene die Suchbarkeit der Telefonnummer betreffende Standardeinstellung überhaupt jemals geändert zu haben, hat er mit den Ausführungen in seinem zweitinstanzlichen Schriftsatz vom 15. Januar 2025 nochmals bekräftigt. Die Beklagte hat ihr Vorbringen dessen ungeachtet zu keiner Zeit weiter substantiiert und insbesondere zur Aussagekraft der von ihr dazu vorgelegten Anlage B17 keinen weiteren Vortrag mehr gehalten. Eine vom Kläger vorgenommene Änderung der die Suchbarkeit der Telefonnummer betreffenden Standardeinstellung steht damit nicht fest. Die Beklagte ist für ihre gegenteilige Behauptung beweisfällig geblieben.

bb) 36

Es kommt in diesem Zusammenhang für einen Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO auch nicht darauf an, ob der Beklagten wegen des die Mobilfunknummer erfassenden Datenverarbeitungsvorgangs über den einen festgestellten Datenschutzverstoß hinaus noch weitere Datenschutzverstöße anzulasten sind. Das Vorliegen mehrerer Datenschutzverstöße durch ein und denselben Verarbeitungsvorgang bleibt auf die Höhe eines etwaigen Schadensersatzanspruchs ohne Auswirkungen (siehe EuGH, Urteil vom 11. April 2024 – C-741/21, juris, Rn. 64 f.).

cc) 38

39

Dem Kläger ist infolge des Datenschutzverstoßes der Beklagten auch ein immaterieller Schaden im Sinne von Art. 82 Abs. 1 DSGVO entstanden.

(1) 40

Der Begriff des „immateriellen Schadens“ in Art. 82 Abs. 1 DSGVO ist in Ermangelung eines in der Vorschrift enthaltenen Verweises auf das innerstaatliche Recht der Mitgliedstaaten autonom unionsrechtlich zu bestimmen. Maßgeblich ist danach das Begriffsverständnis, wie es in der Rechtsprechung des Gerichtshofs der Europäischen Union ausgeformt worden ist. Zwar soll nach Erwägungsgrund 146 Satz 3 DSGVO der Begriff des Schadens weit ausgelegt werden, in einer Art und Weise, die den Zielen der Verordnung in vollem Umfang entspricht. Der bloße Verstoß gegen die Bestimmungen der Datenschutz-Grundverordnung reicht nach der Rechtsprechung des Gerichtshofs jedoch nicht aus, um einen Schadensersatzanspruch zu begründen. Vielmehr ist darüber hinaus der Eintritt eines Schadens durch diesen Verstoß erforderlich. 41

Ein haftungsbegründender immaterieller Schaden im Sinne von Art. 82 Abs. 1 DSGVO kann jedoch nach der Rechtsprechung des Gerichtshofs schon in dem – selbst kurzzeitigen – Verlust der Kontrolle über personenbezogene Daten liegen, ohne dass der Begriff des „immateriellen Schadens“ den Nachweis zusätzlicher spürbarer negativer Folgen erfordert. Insofern schließt sich der Senat nach nochmaliger eigener Prüfung der Rechtsprechung des Gerichtshofs dem vom Bundesgerichtshof hierzu vertretenen Verständnis an (vgl. BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 30). Unter einem Verlust der Kontrolle versteht der Senat dabei eine Situation, in der der Betroffene seine personenbezogenen Daten nicht mehr beherrschen kann, weil sie etwa an ihm unbekannte Dritte gelangt oder ohne nennenswerte Eingrenzung preisgegeben sind. Das ist der Fall bei einem Scraping und bei einer Veröffentlichung der Daten im Internet, aber noch nicht – beispielsweise – bei einer Weitergabe der Telefonnummer an bestimmte Empfänger oder ihre Verwendung zur Zwei-Faktor-Authentifizierung bei Nutzung von Benutzerkonten (Accounts). In einem solchen Fall sind die Daten noch nicht allgemein veröffentlicht (vgl. BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 41). 42

(2) 43

Eine Situation des Kontrollverlusts hat der Kläger im Hinblick auf seine Mobilfunknummer und ihre Verknüpfung mit seiner A.-ID, seinem Vor- und Nachnamen und seinem Geschlecht dargelegt. Insofern reicht es aus, wenn ein Betroffener eine Veröffentlichung seiner Daten im Internet vorträgt und angibt, diese Daten nicht zuvor in einer vergleichbaren Weise allgemein veröffentlicht zu haben (siehe BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 39 ff.). Einen solchen Vortrag hat der Kläger gehalten. Ein bereits zuvor eingetretener Kontrollverlust ergibt sich nicht daraus, dass der Kläger im Rahmen seiner informatorischen Anhörung vor dem Landgericht angegeben hat, seine Mobilfunknummer bei Amazon, Otto, WhatsApp und PayPal sowie für das Online-Banking zu nutzen. Das steht einer allgemeinen Veröffentlichung nicht gleich. Der Abgriff der Daten war in erster Instanz zudem ebenso unstreitig wie eine Veröffentlichung im Internet im Jahr 2021. 44

Zwar hat der Kläger seinen Vor- und Nachnamen und sein Geschlecht auf seinem für jedermann sichtbaren A.-Profil eingestellt. Auch war auf der betreffenden Profilseite die A.-ID des Klägers zu finden. Für die Mobilfunknummer galt dies nach seinem Vortrag jedoch nicht. Auch war diese nach seinem Vorbringen nicht schon zuvor im Internet für jedermann sichtbar mit den übrigen genannten Daten verknüpft. Daraus folgt, dass nur für die erstgenannten Daten ein Kontrollverlust durch den Datenabgriff und die Veröffentlichung sowohl singulär als 45

auch in ihrer Verknüpfung ausscheidet. Denn diese Daten waren schon zuvor – bei A. – allgemein zugänglich im Internet veröffentlicht. Das war dem Kläger bei lebensnaher Betrachtung nicht nur klar, sondern damit war er im Sinne einer Einwilligung gemäß Art. 6 Abs. 1 Unterabs. 1 Buchst. a DSGVO auch ersichtlich einverstanden, weil er – so ist sein Verhalten zu verstehen – eine Veröffentlichung in Form des von ihm gestalteten A.-Profils gerade wollte.

Die Beklagte hat zwar bestritten, dass der Kläger die Kontrolle über seine Mobilfunknummer und ihre Verknüpfung mit den weiteren von ihr als abgegriffen eingeräumten Daten erst mit dem Datenabgriff verloren hat. Dieser Vortrag genügte jedoch nicht den Anforderungen an ein in diesem Fall zu forderndes qualifiziertes Bestreiten. Die vom Kläger behauptete negative Tatsache, die Kontrolle über die Daten nicht schon zuvor verloren zu haben, sie insbesondere nicht bereits allgemein veröffentlicht zu haben, hätte die Beklagte mit der konkreten Angabe bestreiten müssen, wodurch ein Kontrollverlust schon zuvor eingetreten sein soll (vgl. zu dieser sekundären Darlegungslast BGH, Urteile vom 11. Oktober 2007 – IX ZR 105/06, juris, Rn. 12, und vom 8. Januar 2019 – II ZR 139/17, juris, Rn. 31; auch BAG, Urteil vom 16. Dezember 2021 – 2 AZR 356/21, juris, Rn. 31 ff.). Einen solchen Vortrag hat sie nicht gehalten.

Soweit die Beklagte erstmals zum Ende der Berufungsinstanz eine Kausalität zwischen dem Datenabgriff und dem Kontrollverlust bestreitet, kann sie hiermit nicht mehr gehört werden. Das Vorbringen ist nach § 138 Abs. 1 ZPO unbeachtlich. Es steht in einem von der Beklagten nicht aufgelösten Widerspruch zu ihrem erstinstanzlichen Vorbringen und dem Inhalt des von ihr in erster Instanz vorgelegten Schreibens vom 9. Januar 2023. Dessen ungeachtet ist das Vorbringen auch nach § 531 Abs. 2 Satz 1 Nr. 3 ZPO nicht mehr zuzulassen, weil erstinstanzlich zwischen den Parteien unstreitig gewesen ist, dass – jedenfalls – die im Schreiben der Beklagten vom 9. Januar 2023 mitgeteilten Daten des Klägers vom Datenabgriff betroffen waren, und die Beklagte nicht dargelegt hat, warum sie Gegenteiliges nicht schon in erster Instanz vorgetragen hat.

dd) 48

Die Höhe des dem Kläger gemäß Art. 82 Abs. 1 DSGVO für den ihm entstandenen immateriellen Schaden zustehenden Schadensersatzes bemisst sich nach den schadensersatzrechtlichen Grundsätzen des deutschen Rechts. 49

(1) 50

Die Datenschutz-Grundverordnung enthält keine Bestimmung über die Bemessung des aus Art. 82 Abs. 1 DSGVO geschuldeten Schadensersatzes. Insbesondere können aufgrund des unterschiedlichen Zwecks der Vorschriften nicht die in Art. 83 DSGVO genannten Kriterien herangezogen werden. Die Bemessung richtet sich vielmehr entsprechend dem Grundsatz der Verfahrensautonomie nach den innerstaatlichen Vorschriften über den Umfang der finanziellen Entschädigung (BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 93). In Deutschland ist damit insbesondere die Verfahrensvorschrift des § 287 ZPO anzuwenden. 51

Bei der Ermittlung des nach Art. 82 Abs. 1 DSGVO zu ersetzenden Schadens unterliegt die innerstaatliche Verfahrensausautonomie allerdings den sich aus dem unionsrechtlichen Äquivalenz- und Effektivitätsgrundsatz ergebenden Einschränkungen (BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 94). Eine auf Art. 82 Abs. 1 DSGVO gestützte Entschädigung in Geld ist in Anbetracht der Ausgleichsfunktion des in dieser Vorschrift 52

vorgesehenen Schadensersatzanspruchs als „vollständig und wirksam“ im Sinne von Erwägungsgrund 146 Satz 6 DSGVO anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen die Datenschutz-Grundverordnung konkret erlittenen Schaden in vollem Umfang auszugleichen. Eine Abschreckungs- oder Straffunktion soll der Anspruch aus Art. 82 Abs. 1 DSGVO nicht erfüllen. Infolgedessen darf bei der Bemessung einer Geldentschädigung weder die Schwere des Verstoßes gegen die Datenschutz-Grundverordnung, durch den der betreffende Schaden entstanden ist, berücksichtigt werden, noch – wie bereits ausgeführt – der Umstand, ob ein Verantwortlicher mehrere Verstöße gegenüber derselben Person begangen hat oder ob er vorsätzlich oder fahrlässig gehandelt hat (BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 96).

Im Ergebnis soll die zuzusprechende Entschädigung zwar nicht hinter dem vollständigen Ausgleich des Schadens zurückbleiben, sie darf aber auch nicht in einer Höhe bemessen werden, die über den vollständigen Ersatz des Schadens hinausgeht. Ist der Schaden gering, ist daher auch ein Schadensersatz in nur geringer Höhe zuzusprechen (BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 97). Dies gilt auch unter Berücksichtigung des Umstands, dass der durch eine Verletzung des Schutzes personenbezogener Daten verursachte immaterielle Schaden seiner Natur nach nicht weniger gewichtig ist als eine Körperverletzung (BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 97). 53

(2) 54

Bei der auf § 287 ZPO gestützten Bemessung des Entschädigungsbetrags sind dann, wenn ein Schaden nur in Form eines Kontrollverlusts an personenbezogenen Daten eingetreten ist, weil weitere Schäden nicht nachgewiesen sind, bei der Schätzung des Schadens insbesondere die etwaige Sensibilität der konkret betroffenen personenbezogenen Daten und deren typischerweise zweckmäßige Verwendung zu berücksichtigen. Zudem sind die Art des Kontrollverlusts, die Dauer des Kontrollverlusts und die Möglichkeit der Wiedererlangung der Kontrolle etwa durch Entfernung einer Veröffentlichung aus dem Internet oder Änderung des personenbezogenen Datums in den Blick zu nehmen. In Fällen, in denen die Wiedererlangung der Kontrolle mit verhältnismäßigem Aufwand möglich ist, kann auch der hypothetische – insbesondere finanzielle – Aufwand für die Wiedererlangung der Kontrolle als Anhalt für einen effektiven Schadensausgleich dienen (siehe zum Ganzen BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 99). 55

(3) 56

Nach diesen Maßgaben wird der dem Kläger mit dem Kontrollverlust entstandene Schaden mit einem Betrag von 100 € effektiv ausgeglichen. Das ergibt eine Gesamtwürdigung der im Fall des Klägers maßgeblichen Umstände. 57

Ein Kontrollverlust steht nur hinsichtlich der Mobilfunknummer und ihrer Verknüpfung mit der A.-ID, dem Vor- und Nachnamen und dem Geschlecht des Klägers fest. Dieser Kontrollverlust dauert zwar seit 2019 an, eine Vertiefung desselben ist jedoch seit der Veröffentlichung der Daten im Internet im Jahr 2021 nicht erkennbar. Zwar erscheint es wenig wahrscheinlich, dass der Kläger die Kontrolle über die Daten durch ihre Entfernung aus dem Internet zurückerlangen wird. Es spricht jedoch manches dafür, dass ein an den Daten gegebenenfalls bestehendes Interesse Dritter mit fortschreitender Zeit abnimmt, so dass der durch den Datenschutzverstoß der Beklagten herbeigeführte Kontrollverlust an Bedeutung verlieren könnte. Mithilfe der Daten ist im Übrigen lediglich eine Kontaktaufnahme mit dem Kläger möglich. Zwar kann die Mobilfunknummer auch zur Übersendung von Spam-SMS und für werbende, belästigende oder sogar betrügerische Anrufe genutzt werden. Zu einem 58

etwaigen materiellen Schaden führen SMS-Nachrichten und Anrufe jedoch nicht ohne weitere Zwischenschritte. Gegen diese kann sich der für die Gefahr sensibilisierte Kläger durch Achtsamkeit wappnen. Bei den vom Kontrollverlust betroffenen Daten handelt es sich zudem nicht um höchst sensible Daten des Klägers, etwa Gesundheits- oder vergleichbar intime Daten, deren Verbreitung in der Öffentlichkeit dem Ansehen oder dem Fortkommen des Klägers schaden könnte (vgl. auch BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 42). Die Mobilfunknummer dient vielmehr regelmäßig der Kontaktaufnahme mit Dritten und wird zu diesem Zweck anderen zugänglich gemacht. Allein dadurch besteht immer die Gefahr, dass eine bis zu einem bestimmten Zeitpunkt kontrollierte Weitergabe der Telefonnummer irgendwann nicht mehr kontrollierbar ist, weil schlechterdings niemand vollumfänglichen Einfluss darauf haben kann, wie Dritte mit der Nummer umgehen. Es kommt hinzu, dass der Kläger einen Rufnummernwechsel, mit dem er die Kontrolle über seine Mobilfunknummer sofort wiedererlangen könnte, zwar bislang nicht vorgenommen hat, dies aber auf der Grundlage seines Vortrags durchaus könnte.

(4) 59

Bei Bemessung der Schadenshöhe nicht zu berücksichtigen sind weitere vom Kläger auf den Kontrollverlust zurückgeführte Unannehmlichkeiten. 60

Zwar stellen mit dem Kontrollverlust verbundene negative Gefühle wie Ängste und Befürchtungen sowie in der Auseinandersetzung mit dem Scraping-Vorfall und dem Schutz vor künftigem Datenmissbrauch aufgewandte Zeit und Mühe Umstände dar, die einen bereits mit dem reinen Kontrollverlust eingetretenen immateriellen Schaden im Sinne des Art. 82 Abs. 1 DSGVO vertiefen oder vergrößern können (vgl. BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 31, 35 und 45). Das gilt jedenfalls dann, wenn sie über die mit dem eingetretenen Kontrollverlust für jedermann unmittelbar zusammenhängenden Unannehmlichkeiten hinausgehen (BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 101). Auch eine etwaige psychische Belastung durch Spam-Anrufe und Spam-SMS, die auf den Kontrollverlust zurückzuführen sind, kann den immateriellen Schaden vergrößern. 61

Entsprechende Beeinträchtigungen des Klägers hat das Landgericht jedoch nicht festgestellt, obwohl es den Kläger informatorisch angehört hat. Zwar hat der Kläger nach dem Inhalt des landgerichtlichen Sitzungsprotokolls vom 19. April 2024 den Erhalt von Spam-Anrufen bekundet und nach den Ausführungen in den Entscheidungsgründen des landgerichtlichen Urteils darüber hinaus auch den Erhalt von Spam-SMS und Spam-Mails. Von der Kausalität zwischen den vom Kläger geschilderten Spam-Anrufen beziehungsweise Spam-SMS und dem Scraping-Vorfall konnte sich das Landgericht aber keine hinreichende Überzeugung bilden. Es hat zwar nicht dargelegt, von welchem Beweismaßstab es insoweit ausgegangen ist. Steht der geltend gemachte Schadensersatzanspruch dem Grunde nach fest, reicht für die richterliche Entscheidung über die Schadenshöhe gemäß § 287 ZPO eine erhebliche, auf gesicherter Grundlage beruhende Wahrscheinlichkeit für die richterliche Überzeugungsbildung aus (BGH, Urteil vom 11. März 2022 – V ZR 35/21, juris, Rn. 30). So verhält es sich hier, weil der Senat – abweichend von dem Landgericht – schon den reinen Kontrollverlust als den haftungsbegründenden Schaden ansieht. Doch auch unter Anlegung des abgesenkten Beweismaßstabs des § 287 ZPO kann der Senat im Rahmen einer eigenen Würdigung keine Beeinträchtigung des Klägers durch den Kontrollverlust feststellen, die über die Unannehmlichkeiten hinausgeht, die jedermann durch einen solchen Kontrollverlust erleidet. Insbesondere Anhaltspunkte, die für eine besondere psychische Beeinträchtigung sprechen könnten, hat die Anhörung des Klägers vor dem Landgericht nicht ergeben. Zwar hat er geschildert, seit einem Jahr arbeitsunfähig an einer Depression erkrankt zu sein. Einen 62

Bezug zu dem Scraping-Vorfall hat er jedoch selbst nicht hergestellt, sondern verneint. Angesichts der denkbar vielfältigen Ursachen für Spam-Anrufe und Spam-SMS ist auch nicht zu beanstanden, dass das Landgericht keine Kausalität zwischen dem Scraping-Vorfall und der von dem Kläger geschilderten Spam-Belästigung hat feststellen können. Aus eigener Erfahrung ist dem Senat bekannt, dass es zu Spam-Anrufen und Spam-SMS auf Mobiltelefonen auch kommen kann, wenn A. nicht genutzt wird. Dass ihn die Spam-Anrufe „verrückt machten“, wie er bekundet hat, kann der Kläger daher nicht mit Erfolg der Beklagten anlasten.

Da sich eine Ursächlichkeit des Scraping-Vorfalles nicht feststellen lässt, kann dahinstehen, ob schon der Erhalt von Spam-Anrufen und Spam-SMS ohne weitere Folgen einen immateriellen Schaden darstellen oder diesen vertiefen kann (ablehnend OLG Hamm, Urteil vom 18. Dezember 2024 – I-11 U 168/23, juris, Rn. 33). 63

Was die vom Kläger vorgetragene Belastung mit Spam-Mails betrifft, kommt deren Berücksichtigung bei der Bemessung des Schadensersatzbetrags schon deshalb nicht in Betracht, weil der Kläger einen seine E-Mail-Adresse betreffenden Kontrollverlust durch den Datenabgriff bei der Beklagten nicht nachgewiesen hat. 64

(5) 65

Der Schadensersatzanspruch des Klägers ist auch nicht aufgrund eines im bislang unterbliebenen Rufnummernwechsel zu sehenden Mitverschuldens zu kürzen. Dass der Kläger seine Mobilfunknummer bislang nicht gewechselt hat, dies aber könnte, ist bei der Bemessung des Schadensersatzbetrags vom Senat bereits berücksichtigt worden. 66

c) 67

Der vom Kläger mit dem Klageantrag zu 1. ebenfalls verfolgte Anspruch auf Zinsen aus dem Betrag der Hauptforderung ab dem Zeitpunkt der Rechtshängigkeit ergibt sich dem Grunde und der Höhe nach aus § 291 i.V.m. § 288 Abs. 1 Satz 2 BGB. Mangels eines anderen feststellbaren Zustellzeitpunkts ist anzunehmen, dass die Klage spätestens an dem Tag zugestellt worden ist, an dem die Beklagte ihre Verteidigungsbereitschaft angezeigt hat. Der Zinsanspruch besteht damit ab dem darauf folgenden Tag, dem 13. Juli 2023. 68

3. 69

Der Klageantrag zu 2. ist in der vom Kläger zuletzt verfolgten Fassung nur teilweise – in dem aus dem Tenor ersichtlichen Umfang – zulässig und begründet. Unter Berücksichtigung der klarstellenden Ausführungen des Klägers im erstinstanzlichen Schriftsatz vom 18. Oktober 2023 ist der Antrag zum einen, was der Senat bei der Formulierung des Tenors berücksichtigt hat, auf die Feststellung der Ersatzpflicht für zukünftige materielle Schäden gerichtet. Zum anderen richtet er sich auf die Feststellung der Ersatzpflicht für derzeit noch nicht vorhersehbare immaterielle Schäden. 70

a) 71

Wie der Senat bereits in der Vergangenheit entschieden hat, ist die bloße Möglichkeit des künftigen Eintritts der geltend gemachten Schäden zum Maßstab für die Annahme des gemäß § 256 Abs. 1 ZPO erforderlichen Feststellungsinteresses zu nehmen. Eine darüber hinausgehende Schadenswahrscheinlichkeit ist nicht erforderlich. Die Möglichkeit zukünftiger Schäden reicht im vorliegenden Fall aus, weil es nicht um reine Vermögensschäden geht, 72

sondern um Schäden, die aus der vom Kläger behaupteten Verletzung seines Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, mithin seines allgemeinen Persönlichkeitsrechts als einem sonstigen absolut geschützten Rechtsgut im Sinne von § 823 Abs. 1 BGB, resultieren. Auch die hier primär herangezogene Vorschrift des Art. 82 Abs. 1 DSGVO hat, soweit – wie hier – auch eine unrechtmäßige Datenverarbeitung gerügt wird, eine Verletzung des Rechts auf Schutz der personenbezogenen Daten gemäß Art. 8 GRCh zum Inhalt. Dabei kann die Möglichkeit ersatzpflichtiger zukünftiger Schäden ohne Weiteres zu bejahen sein, wenn ein deliktsrechtlich geschütztes absolutes Rechtsgut verletzt wurde und dadurch bereits ein Schaden eingetreten ist (BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 48).

Wie der Bundesgerichtshof nach Erlass des landgerichtlichen Urteils entschieden hat, ist danach die Möglichkeit des Eintritts künftiger Schäden in einem Fall wie dem vorliegenden ohne Weiteres zu bejahen. Durch den Verstoß der Beklagten gegen die Datenschutz-Grundverordnung ist der Kläger jedenfalls in seinem Recht auf Schutz der personenbezogenen Daten gemäß Art. 8 GRCh verletzt worden. Mit dem fortdauernden Kontrollverlust infolge der Veröffentlichung der Daten im Internet besteht auch das Risiko einer missbräuchlichen, insbesondere betrügerischen Nutzung dieser Daten mit der Folge eines materiellen Schadens bis heute fort. 73

Mangels Feststellungsinteresses unzulässig ist der Antrag hingegen, soweit dieser auf die Feststellung etwaiger immaterieller Spätschäden gerichtet ist. Der Kläger hat die Möglichkeit immaterieller Spätfolgen nicht schlüssig dargetan. Im erstinstanzlichen Schriftsatz vom 18. Oktober 2023 hat er ausgeführt, dass „eine immaterielle Schadensvertiefung schwer vorstellbar ist“. Diesen Vortrag hat er nachfolgend nicht mehr geändert. 74

b) 75

Der Feststellungsanspruch in Bezug auf künftige materielle Schäden besteht auch in der Sache. Entstünden dem Kläger aufgrund des feststehenden Datenschutzverstoßes der Beklagten zukünftig materielle Schäden, so wären nach den vorangegangenen Ausführungen insoweit die Voraussetzungen einer Haftung der Beklagten aus Art. 82 Abs. 1 DSGVO gegeben. 76

c) 77

Der Feststellungsanspruch ist auch nicht unter dem Gesichtspunkt eines Mitverschuldens ausgeschlossen, weil der Kläger bislang seine Mobilfunknummer nicht gewechselt hat. Ein Mitverschulden nach § 254 BGB an der Schadensentstehung setzt voraus, dass der Geschädigte die Sorgfalt außer Acht gelassen hat, die nach Lage der Sache erforderlich erscheint, um sich selbst vor Schaden zu bewahren (BGH, Urteil vom 28. September 1978 – VII ZR 116/77, juris, Rn. 19). Das Unterlassen eines Wechsels der Mobilfunknummer in einem Fall wie dem vorliegenden erfüllt diese Voraussetzung nicht. Zum einen ist die Gefahr, dass durch den Missbrauch der vom Kontrollverlust betroffenen Daten materielle Schäden entstehen, gering. Zum anderen kann der Kläger legitime Interessen an der Weiternutzung seiner Mobilfunknummer geltend machen. Die damit verbundene geringe Schadensgefahr tritt dahinter zurück. 78

Über ein etwaiges Mitverschulden im Rahmen der haftungsausfüllenden Kausalität ist vom Senat nicht zu entscheiden. Darüber lässt sich nicht abstrakt, sondern nur in Bezug auf einen konkret eingetretenen Schaden befinden. Hiervon abgesehen spielt die Weiternutzung der Mobilfunknummer im Rahmen der haftungsausfüllenden Kausalität auch keine Rolle. 79

4.	80
Die vom Kläger mit der Berufung weiterverfolgten Unterlassungsanträge – Klageanträge zu 3.a. und 3.b. – sind in der vom Kläger zuletzt zur Entscheidung gestellten Form nur zum Teil zulässig und begründet.	81
a)	82
Der Klageantrag zu 3.a. ist auch nach der dem § 264 Nr. 2 ZPO unterfallenden Umformulierung weiterhin unzulässig. Der Antrag genügt nicht den Bestimmtheitsanforderungen des § 253 Abs. 2 Nr. 2 ZPO.	83
aa)	84
Ein Klageantrag ist hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO, wenn er den erhobenen Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis absteckt, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung erkennen lässt, das Risiko eines Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeiten auf den Beklagten abwälzt und eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt. Ein Unterlassungsantrag darf nicht derart undeutlich gefasst sein, dass die Entscheidung darüber, was dem Beklagten verboten ist, letztlich dem Vollstreckungsverfahren überlassen bleibt (BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 52).	85
Eine hinreichende Bestimmtheit ist bei einem Unterlassungsantrag für gewöhnlich gegeben, wenn eine Bezugnahme auf die konkrete Verletzungsform erfolgt oder die konkret angegriffene Verletzungsform antragsgegenständlich ist und der Klageantrag zumindest unter Heranziehung des Klagevortrags unzweideutig erkennen lässt, in welchen Merkmalen des angegriffenen Verhaltens die Grundlage und der Anknüpfungspunkt für den Rechtsverstoß und damit das Unterlassungsgebot liegen soll (BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 53).	86
bb)	87
Gemessen hieran ist der umformulierte Antrag zu Ziffer 3.a., mit dem der Kläger begehrt, dass die Beklagte es unterlasse, eine bestimmte Verarbeitung seiner personenbezogenen Daten mithilfe der Telefonnummereingabe und des Kontakt-Import-Tools zu ermöglichen, ohne dass die Beklagte zum Zeitpunkt der Verwendung des Kontakt-Import-Tools unter Eingabe der Telefonnummer Sicherheitsmaßnahmen in Form einer Implementierung von Sicherheits-CAPTCHAs und der Überprüfung massenhafter IP-Abfragen oder vergleichbaren Sicherheitsmaßnahmen vorgehalten hat, nicht hinreichend bestimmt. Er lässt sich auch unter Heranziehung des Klagevorbringens und der Erläuterung der Umformulierung im Schriftsatz vom 15. Januar 2025 nicht in einer Weise auslegen, dass der Kläger ein hinreichend bestimmtes Unterlassen begehrt. Die erläuternden Ausführungen beschreiben die im Klageantrag selbst nicht in Bezug genommene konkrete Verletzungsform von ihrer sicherheitstechnischen Seite, um die es dem Kläger mit dem Antrag geht, nicht weiter. Auch ändern sie nichts daran, dass der im Antrag verwendete Begriff der „vergleichbaren Sicherheitsmaßnahmen“ unbestimmt ist. Es ist nicht hinreichend klar, was damit gemeint ist. Eine weitere Konkretisierung dieses Begriffs lässt sich auch dem Vorbringen des Klägers nicht entnehmen.	88

b)	
Erfolg hat die Berufung demgegenüber, soweit sie sich gegen die Abweisung des Unterlassungsantrags zu Ziffer 3.b. wendet.	90
aa)	91
Dieser Unterlassungsantrag ist zulässig.	92
(1)	93
Der Antrag ist trotz seiner weiten Formulierung hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO.	94
Er lässt sich unter Heranziehung des Klagevorbringens dahingehend auslegen, dass der Kläger ein Unterlassen jeglicher Verarbeitung seiner Telefonnummer durch die Beklagte begehrt, die über die notwendige Verarbeitung für die Zwei-Faktor-Authentifizierung hinausgeht (siehe auch BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 62). Er verlangt, dass die Beklagte die Telefonnummer des Klägers im Übrigen nicht auf Basis einer vom Kläger erteilten Einwilligung weiterverarbeitet, da diese Einwilligung nach dem Verständnis des Klägers unwirksam ist, weil ihm das Ausmaß der Datenverarbeitung betreffend seine Telefonnummer bei Erteilung der Einwilligung nicht verständlich war.	95
Der so verstandene Unterlassungsantrag ist hinreichend bestimmt, weil der Beklagten ohne Weiteres deutlich wird, für welche Zwecke sie die Telefonnummer des Klägers noch verarbeiten darf und für welche der Kläger die Unterlassung der Datenverarbeitung begehrt. Der Unterlassungsantrag konkretisiert darüber hinaus die inkriminierte Verletzungshandlung, nämlich die behauptete unrechtmäßige Verarbeitung auf Grundlage einer unwirksamen Einwilligung. Aus welchen Gründen die Einwilligung unwirksam sein soll, ergibt sich aus der weiteren Formulierung des Antrags. Nur zur Klarstellung für Fälle der Zwangsvollstreckung hat der Senat die zulässige Verarbeitung für Zwecke der Zwei-Faktor-Authentifizierung in den Unterlassungstenor aufgenommen.	96
(2)	97
Dem Kläger fehlt für den solchermaßen zu verstehenden Antrag auch nicht das Rechtsschutzbedürfnis.	98
(a)	99
Das Rechtsschutzbedürfnis fehlt, wenn eine Klage oder ein Antrag objektiv schlechthin sinnlos ist, wenn also der Kläger oder Antragsteller unter keinen Umständen mit seinem prozessualen Begehren irgendeinen schutzwürdigen Vorteil erlangen kann. Das ist etwa der Fall, wenn ein einfacherer oder billigerer Weg zur Erreichung des Rechtsschutzziels besteht oder der Antragsteller kein berechtigtes Interesse an der beantragten Entscheidung hat. Dafür gelten jedoch strenge Maßstäbe (vgl. BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 67).	100
(b)	101
Hiernach ist ein Rechtsschutzbedürfnis für den Unterlassungsantrag zu 3.b. nicht zu verneinen. Das Rechtsschutzbedürfnis entfällt nicht dadurch, dass der Kläger seine Telefonnummer aus dem Nutzerkonto selbst löschen könnte. Dadurch würde sich der Kläger	102

der Möglichkeit begeben, seine Telefonnummer zur Zwei-Faktor-Authentifizierung für die Anmeldung in seinem Nutzerkonto zu verwenden. Auch die Möglichkeit des Klägers, die Suchbarkeits-Einstellung bezüglich der Telefonnummer auf „nur ich“ zu stellen, lässt sein Rechtsschutzbedürfnis nicht entfallen. Aus zwei vom Kläger im Verfahren vorgelegten Online-Informationen der Beklagten ergibt sich, dass die Beklagte seine Telefonnummer „möglicherweise“ noch für weitere Zwecke verwendet. So heißt es in einer Information zu „Handy-Einstellungen“ wie folgt: „Mit einer aktuellen Handynummer kannst du dein Passwort ganz einfach zurücksetzen und SMS-Benachrichtigungen erhalten. Zudem können wir dir und anderen verbesserte Werbung zeigen.“ Weitere mögliche Verwendungen ergeben sich aus einer Online-Information der Beklagten mit der Überschrift „Möglicherweise verwenden wir deine Mobilnummer für diese Zwecke“. Darin findet sich etwa ein Hinweis auf die Möglichkeit der Verwendung für Zwecke der personalisierten Werbung. Zwar hat die Beklagte hierzu vorgetragen, dass die in der betreffenden Information angegebenen Verwendungszwecke nicht auf alle Nutzer zutreffen. Sie hat dies aber entgegen ihrer Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO für die Einhaltung der Prinzipien des Art. 5 Abs. 1 DSGVO nicht näher ausgeführt, insbesondere nicht im Hinblick auf die konkrete Situation des Klägers ausgeschlossen, dass er davon betroffen sein könnte. Sie hat auch nicht erläutert, wie der Kläger insoweit über seine Einstellungen gegebenenfalls selbst einfach Abhilfe schaffen könnte.

bb) 103

Der Unterlassungsantrag ist auch begründet. Dabei kann dahinstehen, ob sich ein 104
Unterlassungsanspruch aus Vorschriften der DSGVO ergibt. Jedenfalls ergibt er sich für den Kläger gemäß § 280 Abs. 1, § 241 Abs. 2 BGB aus dem mit der Beklagten geschlossenen Nutzungsvertrag selbst. Aus der Verletzung von Vertragspflichten nach § 280 Abs. 1 BGB kann sich ein vorbeugender Unterlassungsanspruch ergeben, wenn, ebenso wie bei einem gesetzlichen Unterlassungsanspruch nach § 823 Abs. 1 BGB i.V.m. § 1004 Abs. 1 Satz 2 BGB analog, eine Erstbegehungs- beziehungsweise Wiederholungsgefahr besteht (vgl. BGH, Urteil vom 18. November 2024 – VI ZR 10/24, juris, Rn. 83, mit Verweis auf BGH, Urteile vom 2. Mai 2024 – I ZR 12/23, juris, Rn. 14, vom 29. Juli 2021 – III ZR 179/20, juris, Rn. 102 f., und vom 8. November 2022 – II ZR 91/21, juris, Rn. 64). Hier hat die Beklagte mit der zum Datenabgriff führenden Datenverarbeitung Pflichten aus dem Nutzungsvertrag verletzt, weil eine rechtswirksame Einwilligung des Klägers in die mit der Suchfunktion verbundene Datenverarbeitung nicht vorgelegen hat. Die Verschuldensvermutung des § 280 Abs. 1 Satz 2 BGB hat die Beklagte nicht widerlegt.

Für die für den Unterlassungsanspruch notwendige Wiederholungsgefahr spricht nach der 105
von der Beklagten begangenen Pflichtverletzung eine tatsächliche Vermutung (vgl. BGH, Urteil vom 29. Juli 2021 – III ZR 179/20, juris, Rn. 103). Dabei begründet die Verletzung einer Vertragspflicht die Vermutung für eine Wiederholungsgefahr nicht nur für identische Verletzungsformen, sondern auch für andere Vertragspflichtverletzungen, soweit die Verletzungshandlungen im Kern gleichartig sind (BGH, Urteil vom 29. Juli 2021 – III ZR 192/20, juris, Rn. 116 m.w.N.). Für eine Widerlegung dieser Vermutung ausreichende Anhaltspunkte, an die strenge Anforderungen zu stellen sind, hat die Beklagte nicht vorgetragen. Es ist nach den Erklärungen der Beklagten nicht auszuschließen, dass der Kläger noch von Verwendungen beziehungsweise Verarbeitungen seiner Mobilfunknummer durch die Beklagte betroffen ist, die über die Verarbeitung zur Zwei-Faktor-Authentifizierung hinausgehen. Dass diese Verarbeitungen nach Art. 6 DSGVO rechtmäßig wären, lässt sich nicht feststellen, weil die Beklagte – wie schon ausgeführt – der ihr gemäß Art. 5 Abs. 1 Buchst. a, Abs. 2 DSGVO obliegenden Rechenschaftspflicht nicht genügt hat. Zu

Rechtfertigungsgründen für die nach ihren Online-Informationen möglichen anderweitigen Verwendungen hat sie nicht ansatzweise etwas vorgetragen. Vor diesem Hintergrund vermag der Senat eine die Wiederholungsgefahr ausschließende Sondersituation (vgl. dazu BGH, Urteil vom 27. April 2021 – VI ZR 166/19, juris, Rn. 23) nicht festzustellen.	
cc)	106
Nur klarstellend weist der Senat darauf hin, dass der bestehende Unterlassungsanspruch nicht geeignet ist, den zukünftigen Erhalt von Spam-Anrufen und Spam-SMS auf dem Mobiltelefon des Klägers zu verhindern. Für ein solches Klageziel war die Beklagte nicht die richtige Adressatin.	107
III.	108
Die Entscheidung über die Kosten des Rechtsstreits folgt aus § 92 Abs. 1 ZPO und entspricht dem Anteil der Parteien am Unterliegen und Obsiegen.	109
Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf § 709 ZPO.	110
Ein Grund zur Zulassung der Revision besteht nicht. Die Voraussetzungen des § 543 Abs. 2 ZPO liegen nicht vor. Weder hat die Rechtssache nach dem Urteil des Bundesgerichtshofs vom 18. November 2024 – VI ZR 10/24 – noch grundsätzliche Bedeutung noch erfordern die Fortbildung des Rechts oder die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Revisionsgerichts. Abweichungen von Entscheidungen der Oberlandesgerichte Dresden (z.B. Urteil vom 10. Dezember 2024 – 4 U 808/24, juris), Hamm (z.B. Urteil vom 18. Dezember 2024 – I-11 U 168/23, juris) und Koblenz (Urteil vom 11. Februar 2025 – 3 U 145/24, juris) beruhen nach Auffassung des Senats auf unterschiedlichen tatrichterlichen Würdigungen.	111
Das Verfahren ist auf den Antrag der Beklagten im nicht nachgelassenen Schriftsatz vom 6. Mai 2025 auch nicht in entsprechender Anwendung von § 148 ZPO auszusetzen. Anders als das Landgericht Erfurt in seinem von der Beklagten in Bezug genommenen Aussetzungsbeschluss vom 3. April 2025 – 8 O 895/23 – sieht der Senat die Frage, ob der bloße Verlust der Kontrolle über personenbezogene Daten einen Schaden im Sinne von Art. 82 Abs. 1 DSGVO darstellen kann, im Einklang mit dem Bundesgerichtshof und dem Bundesarbeitsgericht (vgl. BAG, Urteil vom 20. Februar 2025 – 8 AZR 61/24, juris, Rn. 13) als durch die Rechtsprechung des Gerichtshofs der Europäischen Union (siehe EuGH, Urteile vom 20. Juni 2024 – C-590/22, juris, Rn. 33, und vom 4. Oktober 2024 – C-200/23, juris, Rn. 150) geklärt an. Im Übrigen geht der Senat von einem anderen Sachverhalt als das Landgericht Erfurt aus, weil nach den obigen Feststellungen des Senats die datenschutzrechtliche Verantwortung für die Verknüpfung der Telefonnummer mit den Profildaten der A.-Nutzer bei der Beklagten liegt.	112
Der Streitwert wird – unter Rückgriff auch auf § 63 Abs. 3 Satz 1 Nr. 2 GKG – für beide Instanzen auf jeweils 3.500 € festgesetzt (vgl. BGH, Beschluss vom 10. Dezember 2024 – VI ZR 7/24, juris).	113
...	114

