OLG München, Endurteil v. 06.06.2025 – 36 U 4233/23 e

Titel:

Ansprüche nach Scraping-Vorfall

Normenketten:

DSGVO Art. 5, Art. 6 Abs. 1, Art. 25, Art. 82

ZPO § Abs. 2 Nr. 2

Leitsätze:

1. Ist der Zeitpunkt eines Scraping-Vorfalls streitig, trifft denjenigen, der die Daten gespeichert hat, eine sekundäre Darlegungslast. (Rn. 57 – 58) (redaktioneller Leitsatz)

2. Die Voreinstellung der Suchbarkeit anhand einer Telefonnummer auf "Alle" verstößt gegen den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. b) und c), Art. 25 Abs. 2 S. 1, S. 3 DS-GVO. (Rn. 67 – 81) (redaktioneller Leitsatz)

3. Der – selbst kurzzeitige – bloße Verlust der Kontrolle über personenbezogene Daten kann einen immateriellen Schaden darstellen, ohne dass dieser Begriff den Nachweis zusätzlicher spürbarer negativer Folgen erfordert, etwa eine missbräuchliche Verwendung der betreffenden Daten zum Nachteil der betroffenen Person. (Rn. 93) (redaktioneller Leitsatz)

4. Ein Unterlassungsantrag, der Begriffe wie „unbefugte Dritte“, „nach dem Stand der Technik mögliche Sicherheitsmaßnahmen“ und „Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme“ enthält, ist nicht hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO. (Rn. 112 – 117) (redaktioneller Leitsatz)

Schlagworte:

Datenscraping, Kontrollverlust, Immaterieller Schadensersatz, Datenschutzverletzung, Voreinstellungen, Unterlassungsanspruch, Beweislast

Vorinstanz:

LG München II, Urteil vom 29.09.2023 – 11 O 1884/22

Fundstelle:

GRUR-RS 2025, 15491

Tenor

I. Auf die Berufung des Klägers wird das Urteil des Landgerichts München II vom 29.09.2023, Az. 11 O 1884/22, abgeändert:

1. Die Beklagte wird verurteilt, an den Kläger 200,00 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit 13.07.2022 zu bezahlen.

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

3. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 159,94 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit 13.07.2022 zu zahlen.

4. Im Übrigen wird die Klage abgewiesen.

II. Die weitergehende Berufung des Klägers wird zurückgewiesen.

III. Von den Kosten des Rechtsstreits beider Instanzen tragen der Kläger 83% und die Beklagte 17%.

IV. Das Urteil ist vorläufig vollstreckbar.

Beschluss

Der Streitwert wird für das Verfahren erster Instanz und für das Berufungsverfahren auf 4.000,00 € festgesetzt.

Entscheidungsgründe

I.

1
Der Kläger macht gegen die Beklagte Ansprüche auf Schadensersatz, Feststellung und Unterlassung wegen behaupteter Verstöße gegen die Verordnung (EU) 2016/679 (Datenschutzgrundverordnung; im Folgenden: DS-GVO) geltend.

2
1. Die Beklagte, die ihren Sitz in Irland hat, betreibt auf dem Gebiet der Europäischen Union das soziale Netzwerk F. .

3
Im Zuge des Registrierungsprozesses müssen die Nutzer Informationen angeben, darunter Name und Geschlecht, die neben der Nutzer-ID immer öffentlich einsehbar sind. Daneben können die Nutzer in ihrem Profil weitere Daten zu ihrer Person (Mobilfunknummer, E-MailAdresse, Wohnort, Geburtsdatum, Stadt, Beziehungsstatus) hinterlegen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern („Freunde“, [auch] „Freunde von Freunden“, „öffentlich“) auf diese Daten zugreifen können („Zielgruppenauswahl“). Soweit keine individuellen Einstellungen gewählt wurden, war im relevanten Zeitraum die Auswahl auf „Freunde“ voreingestellt.

4
Die „Suchbarkeits-Einstellungen“ legen fest, wer das Profil eines Nutzers unter anderem anhand der Telefonnummer finden kann. Standardmäßig war die Suchbarkeit auf „Alle“ eingestellt. Dieser Kreis konnte stattdessen auf „Freunde“, „Freunde von Freunden“ oder ab Mai 2019 zusätzlich auf „Nur ich“ begrenzt werden.

5
Die Beklagte ermöglichte es Nutzern bis September 2019, ihre auf dem Mobilgerät gespeicherten Kontakte mit den bei F. hinterlegten Telefonnummern abzugleichen, um die dahinterstehenden Personen als Freunde hinzuzufügen (Kontakt-Import-Funktion, auch CIT). Diese Möglichkeit bestand auch, wenn die Zielgruppenauswahl des jeweiligen Nutzers im Hinblick auf die Telefonnummer nicht auf „öffentlich“ gestellt und damit nicht für Dritte einsehbar war.

6
Unabhängig davon besteht für die Nutzer die Möglichkeit, ihren Account durch eine sogenannte „Zwei-Faktor-Authentifizierung“ mittels Übermittlung der eigenen Mobilfunknummer an die Beklagte zu sichern.

7
Über Funktion und Bedeutung der Privatsphäre-Einstellungen informierte die Beklagte ihre Nutzer unter anderem im Hilfebereich des Nutzerkontos. Daneben stellte sie eine Datenrichtlinie bereit, die sie im April 2018 anpasste.

8
In einem zwischen den Parteien streitigen Zeitraum ordneten unbekannte Dritte durch die automatisierte und massenhafte Eingabe randomisierter Ziffernfolgen über die Kontakt-Import-Funktion des Netzwerks Telefonnummern Nutzerkonten zu und griffen jedenfalls die zu diesen Nutzern vorhandenen – immer öffentlich einsehbaren und/oder aufgrund der individuellen Zielgruppenauswahl öffentlich gestellten – Daten ab (sog. Scraping). Das Scraping verstieß gegen die Nutzungsbedingungen von F. .

9
Die auf diese Weise erlangten und nunmehr mit einer Telefonnummer verknüpften Daten von ca. 533 Millionen Nutzern aus 106 Ländern wurden im April 2021 im Internet öffentlich verbreitet. Die Beklagte stellte am 06.04.2021 im Artikel „Die Fakten zu Medienberichten über F. -Daten“ klar, dass es sich um öffentlich einsehbare Informationen handelte (Anlage B10). Die Beklagte informierte die zuständige Datenschutzbehörde nicht über den Vorfall. Mittlerweile hat die Beklagte die „Menschen, die du kennen

könntest“-Funktion implementiert, die nicht mehr die direkten Kontaktübereinstimmungen anzeigt, sondern neben dem Telefonnummernabgleich weitere Indikatoren für eine soziale Verbindung der Nutzer heranzieht.

10
Der Kläger unterhielt seit 31.05.2010 ein Nutzerkonto bei F. . Er hatte sich mit der EMail-Adresse … angemeldet und auf dem Netzwerk persönliche Daten eingestellt, seiner Erinnerung nach von Anfang an auch die Telefonnummer. Die Suchbarkeitseinstellung hatte der Kläger bis mindestens September 2019 auf dem Standard „Alle“/„Everyone“ belassen, so dass er mithilfe der Kontakt-Import-Funktion von Dritten über seine Telefonnummer gefunden werden konnte. Durch das Scraping wurden jedenfalls die Nutzer-ID, der Vor- und Nachname und das Geschlecht des Klägers abgerufen. Der Kläger wurde von der Beklagten von dem Datenvorfall nicht in Kenntnis gesetzt.

11
Die Beklagte übermittelte dem Kläger mit Schreiben vom 23.08.2021 eine Anleitung zur Einsichtnahme in die bei der Beklagten hinterlegten Informationen und deren Verwendung (Anlage K2). Die Klägervertreter forderten die Beklagte mit E-Mail vom 14.09.2021 zur Zahlung von Schadensersatz in Höhe von 500,00 €, Unterlassung zukünftiger Zugänglichmachung der Daten des Klägers an unbefugte Dritte und zur Auskunft über die abgegriffenen und veröffentlichten Daten auf (Anlage K1).

12
2. Der Kläger hat erstinstanzlich beantragt, die Beklagte zur Zahlung immateriellen Schadensersatzes in Höhe von mindestens 1.000,00 € nebst Zinsen zu verurteilen und die Ersatzpflicht der Beklagten für alle künftigen Schäden, die aus dem unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten im Jahr 2019 entstanden sind und/oder noch entstehen werden, festzustellen. Des Weiteren hat der Kläger beantragt, die Beklagte strafbewehrt zu verurteilen, es zu unterlassen, personenbezogene Daten des Klägers, namentlich Telefonnummer, F. ID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt und Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern. Außerdem sollte die Beklagte zur Unterlassung verurteilt werden, die Telefonnummer des Klägers 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 bzw. für die F. -Messenger App die Berechtigung verweigert wird. Schließlich begehrte der Kläger Auskunft über die den Kläger betreffenden personenbezogenen Daten, die die Beklagte verarbeitet, und Zahlung der vorgerichtlichen Rechtsanwaltskosten in Höhe von 887,03 € nebst Zinsen.

13
Der Kläger hat erstinstanzlich unter anderem vorgetragen, der Datenschutzvorfall habe sich im Jahr 2019 ereignet. Der ihn betreffende, vom Scraping betroffene Datensatz, habe gelautet:

…, … (Anm.: Telefonnummer, F. -ID, Name, Geschlecht, Wohnort, Beziehungsstatus, Arbeitgeber).

14
Seit April 2021 erhalte er vermehrt dubiose Nachrichten und E-Mails.

15
Die Beklagte hat in erster Instanz unter anderem eingewandt, das Datenscraping habe im Zeitraum von Januar 2018 bis September 2019 stattgefunden. Es sei nur möglich gewesen, Nutzer anhand einer Telefonnummer zu finden, wenn die Suchbarkeitseinstellung auf „Alle“ gestellt gewesen sei. Im April 2018 habe sie die Suche von Nutzern anhand der Telefonnummer in der F. -Suchfunktion deaktiviert die Kontakt-Import-Funktion habe fortbestanden. Die vom Kläger behaupteten unerwünschten Kontaktaufnahmen Dritter und den Zusammenhang mit dem Scraping hat die Beklagte bestritten.

16
3. Das Landgericht München II hat mit Endurteil vom 29.09.2023 die Klage abgewiesen.

17
Das Landgericht hat sämtliche Anträge für hinreichend bestimmt i. S. d. § 253 Abs. 2 Nr. 2 ZPO gehalten, sie in der Sache jedoch abgelehnt. Ein Schadensersatz aus Art. 82 DS-GVO und der korrelierende

Feststellungsantrag stehe dem Kläger nicht zu, da die behaupteten Verstöße gegen Art. 13, 14, 34, 15, 25 DS-GVO schon nicht vom Anwendungsbereich des Art. 82 DS-GVO erfasst seien. Die Vorschrift erfasse von vornherein nur Pflichtverstöße im Rahmen einer „Verarbeitung“. Art. 13, 14, 34, 15 DS-GVO begründeten demgegenüber nur Informationspflichten gegenüber betroffenen Personen. Art. 25 DS-GVO stelle in erster Linie eine organisatorische Verpflichtung für den Verantwortlichen dar. Überdies habe der darlegungs- und beweisbelastete Kläger einen Verstoß gegen die DS-GVO nicht dargelegt und bewiesen. Auch die Transparenzpflichten nach Art. 5 Abs. 1, 13, 14 DS-GVO seien nicht verletzt. Die von der Beklagten verwendete Mehrebenen-Datenschutzerklärung sei im relevanten Zeitraum durch weitergehende Informationen im Hilfebereich ergänzt worden. Informationen zu (hypothetischen) Verarbeitungstätigkeiten Dritter habe die Beklagte nicht erteilen müssen. Es liege auch keine Verletzung der Pflicht zur Implementierung angemessener technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO vor. Die Beklagte sei nicht verpflichtet gewesen, der Erhebung öffentlich zugänglicher Informationen des klägerischen Profils aufgrund seiner selbst gewählten Einstellung durch Schutzmaßnahmen entgegenzuwirken. Weiter treffe die Beklagte kein Verstoß gegen Art. 25 DS-GVO. Die Standard-Suchbarkeitseinstellung „Alle“ während des streitgegenständlichen Zeitraums habe dem Zweck der F. -Plattform entsprochen. Benachrichtigungs- und Meldepflichten aus Art. 34, 33 DS-GVO seien ebenso nicht verletzt. Eine unrechtmäßige Verarbeitung personenbezogener Daten ohne Rechtsgrundlage nach Art. 6 DS-GVO sei nicht erfolgt, da die Daten im Einklang mit der Zielgruppenauswahl des Klägers öffentlich zugänglich gewesen seien.

18
Letztlich liege mangels haftungsausfüllender Kausalität kein ersatzfähiger immaterieller Schaden vor. Aufgrund der Anhörung des Klägers lasse sich nicht nachweisen, dass die unberechtigten Anrufe und SMS im Kausalzusammenhang mit dem Scraping-Vorfall bei der Beklagten erfolgt seien. Der Kläger gebe im Internet auf verschiedenen Plattformen und Shops seine personenbezogenen Daten an, auch E-Mail und Telefonnummer.

19
Der Unterlassungsanspruch sei unbegründet, da schon zweifelhaft sei, ob die DS-GVO einen solchen vorsehe. Jedenfalls fehle es an einem Verstoß gegen die DS-GVO. Eine Wiederholungsgefahr sei nicht zu befürchten, da es jedem Nutzer obliege, jederzeit seine Suchbarkeitseinstellungen anzupassen. Den Auskunftsanspruch habe die Beklagte mit Schreiben vom 04.11.2021 erfüllt.

20
Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die tatsächlichen Feststellungen des angefochtenen Urteils (§ 540 Abs. 1 Nr. 1 ZPO), wegen der Anträge erster Instanz wird auf den dortigen Tatbestand Bezug genommen.

21
4. Gegen diese Entscheidung wendet sich der Kläger mit der form- und fristgerecht eingelegten Berufung.

22
Der Kläger datiert den Datenvorfall maßgeblich auf September 2019. Er habe keine Kenntnis von den zwei Einstellungsmöglichkeiten zur Sichtbarkeit und zur Suchbarkeit gehabt. Er bestreitet, dass das Auffinden des Nutzer-Profils mittels Eingabe der Telefonnummer im CIT nur möglich gewesen sei, wenn die Suchbarkeitseinstellung auf „Everyone“ eingestellt war.

23
Der Kontrollverlust habe beim Kläger ein Gefühl des Unbehagens und der Sorge vor einem möglichen Missbrauch seiner persönlichen Informationen hinterlassen. Er erhalte seit dem Vorfall unregelmäßig Kontaktversuche über sein Telefon in Form von SMS und/oder Anrufen, die Betrugsversuche und potentielle Virenlinks enthielten. Häufig würden dabei bekannte Plattformen und Zahlungsdienstleister wie Amazon oder PayPal oder Anbieter wie DHL, Netflix etc. imitiert, um mit den gestohlenen Daten Vertrauen zu erwecken und um an weitere Daten zu gelangen. Der Kläger hege verstärktes Misstrauen gegenüber diesen Kontaktversuchen von unbekannten Nummern und Adressen, da er bei jedem Kontakt einen Betrug oder Ähnliches befürchte. Der Kläger gebe seine Telefonnummer stets bewusst und zielgerichtet weiter und mache diese nicht wahl- und grundlos der Öffentlichkeit zugänglich.

24

Der Kläger ist der Ansicht, der Anwendungsbereich des Art. 82 DS-GVO sei eröffnet. Die Beklagte habe gegen Art. 5 Abs. 1, 13, 14, 15 DS-GVO verstoßen, da ihre Informationen nicht transparent und leicht verständlich gewesen seien, sondern umfangreich und verschachtelt mit Links und Unterlinks. Insbesondere sei kein Hinweis auf die Verwendung der Mobilfunknummer für das CIT erfolgt. Des Weiteren sei Art. 6 DS-GVO verletzt, da der Kläger in die Nutzung seiner nicht öffentlich geteilten Mobilfunknummer nicht wirksam eingewilligt habe. Die Suchbarkeit des Profils durch Dritte anhand der Mobilfunknummer sei für die Erfüllung des zwischen den Parteien geschlossenen Vertrags nicht erforderlich gewesen, ebenso wenig wie für die Wahrung der berechtigten Interessen der Beklagten oder Dritter. Die Beklagte habe außerdem gegen Art. 32 DS-GVO und das Gebot des Datenschutzes durch Technikgestaltung verstoßen; ihre technischen und organisatorischen Maßnahmen seien nicht ausreichend gewesen. Die Beklagte habe das Gegenteil zu beweisen. Sie hätte die Tätigkeiten des External-Data-Misuse-Teams (Maßnahmen, Kontrolle etc.) substantiieren müssen, da der Kläger ein konkretes Informationsbedürfnis formuliert habe.

25
Außerdem habe er schlüssig vorgetragen, dass die Hilfestellung und Datenschutzhinweise der Beklagten gegen Art. 12 DS-GVO verstießen, und er habe Widersprüche und Unzulänglichkeiten aufgezeigt. Eine Zustimmung zu den Datenschutzhinweisen als Allgemeine Geschäftsbedingungen gereiche dem Kläger wegen §§ 309 Nr. 12 Buchst. b), 308 Nr. 6 BGB nicht zum Nachteil. Ferner liege ein Verstoß gegen die Grundsätze der datenschutzfreundlichen Voreinstellungen „Privacy bei Design“ und „Privacy bei Default“ i. S. d. Art. 24, 25 DSGVO vor. Dem Nutzer werde im Registrierungsprozess suggeriert, dass er seine Mobilfunknummer zum Zwecke der die Sicherheit erhöhenden „Zwei-Faktor-Authentifizierung“ hinterlege. Schließlich habe die Beklagte ihre Meldepflicht gegenüber der zuständigen Aufsichtsbehörde nach Art. 33 DS-GVO und ihre Benachrichtigungspflicht gegenüber dem Kläger nach Art. 34 DS-GVO verletzt. Letztlich habe sie keine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO vorgenommen. Die Beklagte müsse beweisen, keinen Verstoß gegen die DS-GVO verübt zu haben.

26
Die Beklagte sei wegen des Auskunftsrechts nach Art. 15 DS-GVO verpflichtet, weitere Informationen zum Empfänger der Daten mittels Logfiles zur Verfügung zu stellen.

27
Art. 82 DS-GVO erfasse materielle und immaterielle Schäden. Eine Erheblichkeitsschwelle müsse nicht erreicht werden. Allein der Kontrollverlust des Klägers sei bereits ein Schaden, der sich seit dem Datenleck durch Kontaktversuche unbekannter Dritter mit dem Ziel der Erlangung weiterer Daten manifestiert habe. Ängste, Stress, Komfort- und Zeiteinbußen stellten einen immateriellen Schaden dar und würden durch die Verbreitung der Daten im Darknet vergrößert. Telekommunikationsdaten gehörten zu den hoch sensiblen Daten. Die Kausalität des Datenlecks bei der Beklagten für die Spams habe der Kläger bestätigt. Es liege an der Beklagten, den Beweis zu führen, dass der Verstoß nicht zu einem Schaden beim Kläger geführt habe.

28
Für die Höhe des Schadensersatzes müsse die Vielzahl der Verstöße gegen die DS-GVO Berücksichtigung finden und der Umstand, dass dies die Geschäftsgrundlage der Beklagten darstelle. Sie lebe aus Gewinnstreben das Gegenteil des Grundsatzes Privacy by Default und ergreife nur Schein- bzw. Minimalmaßnahmen bezüglich Information, Mitteilung, Auskunft, Technik und Organisation. Die Kriterien des Art. 83 DS-GVO wie Art, Schwere und Dauer des Verstoßes, Grad des Verschuldens und Maßnahmen zur Minderung des Schadens seien entsprechend anwendbar. Den Kläger treffe kein Mitverschulden wegen fehlender Änderung der Einstellungen. Ein Abgreifen der Daten wäre trotzdem möglich gewesen.

29
Aus Art. 82 DS-GVO könne auch der Feststellungsanspruch für zukünftige materielle und immaterielle Schäden abgeleitet werden. Es sei derzeit noch nicht absehbar, welche unbekannten Dritten Zugriff auf die Daten des Klägers erhalten haben und für welche kriminellen Zwecke sie missbraucht werden. Die Möglichkeit eines Schadenseintritts genüge. Gegebenenfalls müsse sich der Kläger eine neue Mobilfunknummer zulegen. Die Beklagte habe nicht substantiiert behauptet, die Maßnahmen zum CIT ausreichend korrigiert zu haben.

30

Der Unterlassungsanspruch sei zulässig, da ausreichend bestimmt. Eine gewisse Verallgemeinerung von Antrag und Titel sei gestattet, solange das Charakteristische der konkreten Verletzungstatbestände zum Ausdruck komme. Mit Blick auf den Effektivitätsgedanken könne der Unterlassungsanspruch zu einer aktiven Beseitigungspflicht führen. Der Leistungsanteil stelle eine bloß unselbständige Nebenpflicht zum Unterlassen dar. Die Anspruchsgrundlage bildeten §§ 280 Abs. 1, 241 Abs. 2 BGB, Art. 17 DS-GVO und §§ 1004 Abs. 1 S. 2, 823 Abs. 2 BGB analog. Eine Sperrwirkung des Art. 79 DS-GVO bestehe nicht. Die Wiederholungsgefahr sei durch die Rechtsverletzung indiziert. Die Beklagte habe diese nicht widerlegt. Die Suchbarkeitseinstellung sei bereits im Zeitraum von 2018 bis vor September 2019 von „Everyone“ auf „Friends of Friends“ umgestellt worden.

31
Der Kläger hat zunächst die erstinstanzlich gestellten Ansprüche geltend gemacht, darunter in Ziffer 4. den Antrag auf Verurteilung der Beklagten zur Erteilung der Auskunft über die den Kläger betreffenden personenbezogenen Daten, welche die Beklagte verarbeitet, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.

32
Der Kläger beantragt unter Rücknahme des Auskunftsantrags zuletzt:

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

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

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

a) personenbezogenen Daten der Klägerseite, namentlich/welche da sind Telefonnummer, F. ID, Familiennamen, Vornamen, Geschlecht,

Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

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

5. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

33
Der Kläger beantragt weiter,

dem EuGH näher formulierte Fragen vorzulegen, das Verfahren gemäß § 148 ZPO in Bezug auf diese und analog zur Entscheidung des EuGH in den Verfahren C-189/22, C-741/21, C-687/21, C-667/21, C-340/21, C-307/2 auszusetzen.

34
Die Beklagte beantragt,

die Berufung zurückzuweisen.

35
Die Beklagte verteidigt die Entscheidung des Landgerichts. Der Kläger habe schon nicht dargelegt, dass seine Daten im zeitlichen Anwendungsbereich der DS-GVO abgerufen worden seien. Der Scraping-Sachverhalt habe im Zeitraum von Januar 2018 bis September 2019 stattgefunden. Da die Beklagte nicht über die gescrapten Rohdaten verfüge und keine Logdateien vorhalte, könne sie den Zeitpunkt des Scrapings der Daten des Klägers nicht bestimmen.

36
Die (angebliche) Verletzung der Aufklärungspflichten nach Art. 5 Abs. 1 Buchst. a), 13, 14 DS-GVO sei nicht vom Anwendungsbereich des Art. 82 DS-GVO erfasst. Überdies habe die Beklagte dem Kläger alle erforderlichen Informationen mit ausreichender Detailtiefe und Transparenz bereitgestellt, insbesondere zur Verwendung der Mobilfunknummer für die Kontakt-Import-Funktion. Eine Einwilligung nach Art. 6 Abs. 1 S. 1 Buchst. a) DS-GVO sei nicht erforderlich. Da sich die Verarbeitung personenbezogener Daten auf die Durchführung des jeweiligen Nutzervertrages stütze, finde Art. 6 Abs. 1 S. 1 Buchst. b) DS-GVO Anwendung. Einem sozialen Netzwerk sei es immanent, dass Nutzer Freunde und Bekannte finden und sich mit ihnen vernetzen können. Solche Verknüpfungen werden durch die Kontakt-Import-Funktion als wesentliches Tool, das die Telefonnummern der Nutzer erfordere, ermöglicht.

37
Ebenso scheide Art. 24 DS-GVO als Anknüpfungspunkt für einen Schadensersatzanspruch aus, da er keine konkreten Verpflichtungen begründe. Die Beklagte habe ihre Pflichten zur Implementierung angemessener technischer und organisatorischer Maßnahmen gemäß Art. 32, 24, 5 Abs. 1 Buchst. f) DS-GVO im Zusammenhang mit der KontaktImport-Funktion nicht verletzt. Sie habe die Anti-Scraping-Maßnahmen im relevanten Zeitraum regelmäßig überprüft und gegebenenfalls angepasst. Im Zuge des Scraping-Sachverhalt sei keine unbefugte Offenlegung von Daten erfolgt; diese habe im Einklang mit den Privatsphäre-Einstellungen des Klägers gestanden. Jedenfalls seien die Risiken und die Wahrscheinlichkeit des Schadenseintritts gering gewesen.

38
Aus der (angeblichen) Verletzung von Benachrichtigungs- und Informationspflichten nach Art. 33, 34 DS-GVO könne ebenfalls kein Anspruch nach Art. 82 DS-GVO resultieren. Die Beklagte sei nicht verpflichtet gewesen, den Scraping-Sachverhalt einer Aufsichtsbehörde zu melden, da keine Verletzung der Sicherheit und des Schutzes personenbezogener Daten vorgelegen habe, zumindest kein Risiko für die Rechte und Freiheiten natürlicher Personen bestanden habe. Aus denselben Gründen mussten die Betroffenen nicht informiert werden.

39
Eine Verletzung der Pflicht zum Datenschutz durch Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen nach Art. 25 DS-GVO liege nicht vor. Es seien ohnehin nur die Datenpunkte Nutzer-ID, Vor- und Nachname und Geschlecht durch das Scraping abgerufen worden, d. h. die immer öffentlichen Nutzerinformationen. Die Standardeinstellung für die Suchbarkeit der Telefonnummer sei nicht zu beanstanden, da auch die Nutzung der Telefonnummer im Rahmen der Suchfunktion dem Unternehmenszweck der Beklagten, Menschen miteinander zu verbinden, und damit der Durchführung des Nutzungsvertrages diene. Eine Suchbarkeit allein anhand des Namens reiche wegen der enormen Zahl der F. -Nutzer von ca. 2,8 Milliarden weltweit zur Identifizierung nicht aus. Der Kläger hätte jederzeit Änderungen seiner Suchbarkeitseinstellungen vornehmen können. Die „Möglichkeit zum Eingreifen“ mit der Erläuterung, wie man dies tun könne, mache die Standardeinstellung mit Art. 25 Abs. 2 DS-GVO vereinbar. Außerdem werde durch die Voreinstellung der Suchbarkeit des Nutzerprofils die Telefonnummer nicht einer unbestimmten Zahl anderer natürlicher Personen „zugänglich“ gemacht, weil eine Benutzung des CIT deren Kenntnis durch die suchende Person gerade voraussetzte.

40
Der Anspruch nach Art. 82 DS-GVO könne nicht aus einer Verletzung der DatenschutzFolgenabschätzung nach Art. 35 DS-GVO abgeleitet werden. Ein solcher würde schon nicht in den zeitlichen Anwendungsbereich der DS-GVO fallen.

41
Die Beklagte treffe kein Verschulden i. S. d. Art. 82 Abs. 3 DS-GVO. Sie habe Maßnahmen gegen Scraping implementiert, die im Gleichgewicht zur beabsichtigen Nutzerfunktionalität stünden.

42
Der Kläger habe keinen materiellen oder immateriellen Schaden erlitten. Dafür sei eine tatsächliche Beeinträchtigung persönlichkeitsbezogener Belange von einigem Gewicht im Sinne von erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen erforderlich. Ein Verlust der Kontrolle über personenbezogene Daten genüge nicht; er sei für sich genommen nicht einem Schaden gleichzusetzen. Ein Verstoß gegen das Recht auf informationelle Selbstbestimmung als nationale Vorschrift werde von Art. 82 DS-GVO nicht erfasst. Der Kläger habe einen Kontrollverlust auch nicht nachgewiesen und weder konkrete weitere Folgen noch bestimmte negative Auswirkungen bei sich vorgetragen. Er beschränke sich auf formelhafte Behauptungen. Insbesondere werde bestritten, dass der Kläger vor dem Scraping-Sachverhalt eine Kontrolle über die abgerufenen Daten innegehabt habe.

43
Die Verbreitung von Spam sei mittlerweile weit verbreitet. Überdies könne eine erneute Veröffentlichung ohnehin öffentlich sichtbarer Nutzerinformationen zu keinem Kontrollverlust führen.

44
Es fehle des Weiteren am Kausalzusammenhang zwischen der angeblichen Pflichtverletzung und dem behaupteten Kontrollverlust oder sonstiger angeblicher negativer Folgen. Der Kläger sei seiner Darlegungs- und Beweislast nicht nachgekommen. In Bezug auf die angeblichen Spam-Nachrichten und -Anrufe habe er weder substantiiert dargelegt noch bewiesen, dass sie auf den Scraping-Sachverhalt zurückgehen. Es handele sich um Alltagserscheinungen, für die eine Vielzahl möglicher Gründe in Betracht komme.

45
Die beanspruchte Schadenshöhe sei überzogen. Art. 82 DS-GVO komme ausschließlich eine Ausgleichsfunktion und gerade keine Abschreckungs- oder Straffunktion zu. Der Schadensersatz könne allenfalls im symbolischen Bereich liegen. Die Beklagte habe Maßnahmen zur Eindämmung von Scraping ergriffen, der Scraping-Sachverhalt sei durch Dritte verursacht worden und der Kontrollverlust beziehe sich nur auf öffentlich einsehbare Daten. Den Kläger treffe ein Mitverschulden, weil er es trotz ausreichender Information unterlassen habe, seine Privatsphäre-Einstellungen anzupassen und seine Telefonnummer zu ändern.

46
Der Feststellungsantrag sei bereits unzulässig, da ein künftiger Schadenseintritt nicht hinreichend wahrscheinlich sei. Das Missbrauchspotenzial der streitgegenständlichen Daten sei gering. Der Kläger habe ein besondere Gefahrenbewusstsein, weshalb das Risiko, dass er Opfer eines künftigen Missbrauchs werde, nicht nennenswert sei. Da er seine Telefonnummer nicht ändere, scheiterten künftige Schadensersatzansprüche an einem überwiegenden Mitverschulden des Klägers bzw. der Verletzung von Schadensminderungspflichten.

47
Die Unterlassungsanträge seien unzulässig, da auf aktives Tun gerichtet und nicht hinreichend bestimmt. Es bestehe keine gesetzliche Grundlage. Art. 17 DS-GVO scheide aus. §§ 1004, 823 Abs. 1 BGB seien durch Art. 79 Abs. 1 DS-GVO gesperrt. Jedenfalls fehle es an einer Rechtsverletzung und einer Wiederholungsgefahr. Der Kläger könne die Privatsphäre-Einstellungen jederzeit ändern und seine Telefonnummer aus dem Nutzerkonto löschen. Die Telefonnummer könne zudem ausschließlich zur Zwei-Faktor-Authentifizierung hinterlegt werden. Darüber hinaus habe die Beklagte die Suchbarkeit über die Telefonnummer mittels CIT zwischenzeitlich entfernt.

48
Die Beklagte beantragt weiter, das Verfahren bis zur Vorabentscheidung des EuGH zum Az. C-273/25 auszusetzen Zur Ergänzung des Sach- und Streitstandes wird auf die gewechselten Schriftsätze nebst Anlagen, auf die gerichtlichen Hinweise sowie auf das Protokoll der mündlichen Verhandlung Bezug genommen.

II.

49
Das Oberlandesgericht München ist zur Entscheidung berufen und hat dieser die DS-GVO zugrunde zu legen.

50
1. Das Oberlandesgericht München ist international zuständig nach Art. 82 Abs. 6, 79 Abs. 2 S. 2 DS-GVO.

51
Art. 82 Abs. 6 DS-GVO sieht für die Inanspruchnahme des Rechts auf Schadensersatz die Zuständigkeit der Gerichte vor, die nach den in Art. 79 Abs. 2 DS-GVO genannten Rechtsvorschriften des Mitgliedstaats zuständig sind. Art. 79 Abs. 2 S. 2 DS-GVO wiederum gibt der betroffenen Person das Recht, eine Klage gegen einen nicht hoheitlich tätig gewordenen Verantwortlichen oder Auftragsverarbeiter bei den Gerichten des Mitgliedstaats zu erheben, in dem die betroffene Person ihren Aufenthaltsort hat. Der Kläger als betroffene Person hat seinen gewöhnlichen Aufenthalt in Deutschland.

52
2. Der sachliche, räumliche und zeitliche Anwendungsbereich der DS-GVO ist eröffnet.

53
a) Nach Art. 2 Abs. 1 DS-GVO gilt die Verordnung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Es ist unstreitig, dass die bei der Beklagten gespeicherten Informationen personenbezogene Daten des Klägers enthalten, die gesammelt und gespeichert werden.

54
b) Art. 3 Abs. 1 DS-GVO erklärt die Verordnung in Bezug auf die Verarbeitung personenbezogener Daten für anwendbar, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet. Die Beklagte hat ihren Sitz in Irland.

55
c) Gemäß Art. 99 Abs. 2 DS-GVO gilt die Verordnung ab dem 25.05.2018. Dabei ist hinsichtlich der zeitlichen Anwendbarkeit nicht der Zeitpunkt der Registrierung eines Nutzerkontos im sozialen Netzwerk der Beklagten maßgeblich, sondern der Zeitpunkt des Scraping-Vorfalls (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 19).

56
Der Kläger hat den Datenschutzvorfall maßgeblich auf September 2019 datiert, die Beklagte hat als „relevanten Zeitraum“ Januar 2018 bis September 2019 benannt.

57
Grundsätzlich muss der Anspruchsteller alle Tatsachen behaupten und beweisen, aus denen sich sein Anspruch herleitet. Damit trifft den Kläger die Darlegungs- und Beweislast dafür, dass der zeitliche Anwendungsbereich der DS-GVO eröffnet ist. Der Grundsatz von Treu und Glauben gebietet jedoch eine sekundäre Darlegungslast des Gegners, wenn die darlegungs- und beweisbelastete Partei außerhalb des von ihr darzulegenden Geschehensablaufs steht und keine Kenntnisse von den maßgeblichen Tatsachen besitzt, während der Prozessgegner angesichts des unterschiedlichen Informationsstands beider Parteien zumutbar nähere Angaben machen kann (BGH, Urteil vom 05.10.2023, III ZR 216/22, NJW 2023, 3794, juris Rdnr. 31). Dabei obliegt es dem Prozessgegner im Rahmen der sekundären Darlegungslast auch, zumutbare Nachforschungen zu unternehmen. Genügt der Gegner seiner sekundären Darlegungslast nicht, gilt die Behauptung des Anspruchstellers nach § 138 Abs. 3 ZPO als zugestanden (BGH, Versäumnisurteil vom 04.02.2021, III ZR 7/20, NJW 2021, 1759, juris Rdnr. 19; BGH, Urteil vom 28.06.2016, VI ZR 559/14, NJW 2016, 3244, juris Rdnr. 18).

58
Der Senat geht in Anwendung dieser Grundsätze davon aus, dass das Scraping der den Kläger betreffenden Daten jedenfalls nach dem 25.05.2018 erfolgte, da die Beklagte im Rahmen ihrer sekundären Darlegungslast nicht ausreichend vorgetragen hat, dass sich der Vorfall vor dem Inkrafttreten der DS-GVO ereignet hat. Das von der Rechtsprechung beschriebene, das Prinzip der Darlegungs- und Beweislast aufweichende Wissengefälle besteht hier. Die Beklagte als Betreiberin der Plattform und alleinige „Herrin“ über die Technik stand dem Scraping-Vorfall weitaus näher als der Kläger, der lediglich Nutzer des Angebots war und keinerlei Einblick in die technischen Vorgänge bei der Beklagten hatte. Der Kläger hat mit seiner Bezugnahme auf September 2019 Angaben der Beklagten aus der Vergangenheit aufgegriffen, die

um 2019 kreisten. So führte die Beklagte in ihrer Pressemitteilung vom 06.04.2021 aus, „böswillige Akteure“ hätten die Daten von F. -Nutzern nicht durch das Hacken der Systeme erlangt, sondern indem sie sie vor September 2019 von der F. -Plattform gescrapt hätten. Aufgrund der ergriffenen Maßnahmen zeigte sich die Beklagte zuversichtlich, dass das spezifische Problem, das den Betrügern das Scrapen der Daten im Jahr 2019 ermöglicht habe, nicht mehr bestehe. Im Weiteren wies die Beklagte darauf hin, Änderungen am Kontakt-Importer vorgenommen zu haben, als ihr bewusst geworden sei, dass „böswillige Akteure“ diese Funktion im Jahr 2019 genutzt haben (Anlage B10). Der Kläger ist damit seiner Darlegungslast nachgekommen. Mehr war von ihm als Außenstehendem nicht zu verlangen. Es war an der Beklagten, die das Kommunikationssystem entwickelt hat und nach eigenen Angaben fortlaufend überwacht, ihre Einwendungen zu spezifizieren. Dies hat sie nicht getan. Welche Erkenntnisse die Beklagte dazu veranlasst haben, im Verfahren den Zeitraum des Scrapings auf Januar 2018 bis September 2019 und damit zum Teil auf die Zeit vor Inkrafttreten der DS-GVO auszuweiten, ist nicht ersichtlich. Dies gilt umso mehr, als sich die Beklagte in ihrem Schreiben vom 23.08.2021 (Anlage K2) und vor allem in ihrer Auskunft vom 07.10.2021 gegenüber dem Kläger eingehend mit den Vorgaben der DS-GVO befasste, ohne deren Anwendbarkeit in Frage zu stellen (Anlage B16). Mit einem bloßen Hinweis darauf, dass sie die Rohdaten der abgegriffenen Daten und die Logdaten nicht vorhalte, vermag die Beklagte dem Erfordernis der sekundären Darlegungslast nicht zu genügen.

III.

59
Dem Kläger steht ein Anspruch auf immateriellen Schadensersatz aus Art. 82 Abs. 1 DS-GVO in Höhe von 200,00 € zu.

60
Nach dieser Vorschrift hat jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

61
1. Ein Schadensersatzanspruch im Sinne des Art. 82 Abs. 1 DS-GVO erfordert einen Verstoß gegen die Datenschutz-Grundverordnung, das Vorliegen eines materiellen oder immateriellen Schadens sowie einen Kausalzusammenhang zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind. Die Darlegungs- und Beweislast für diese Voraussetzungen trifft die Person, die auf der Grundlage von Art. 82 Abs. 1 DS-GVO den Ersatz eines (immateriellen) Schadens verlangt (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 21; EuGH, Urteil vom 04.10.2024, C-507/23, NJW 2025, 141, juris Rdnr. 24; EuGH, Urteil vom 11.04.2024, C-741/21, NJW 2024, 1561, juris Rdnr. 34 f.; EuGH, Urteil vom 25.01.2024, C-687/21, NJW 2024, 2009, juris Rdnr. 58; EuGH, Urteil vom 21.12.2023, C-667/21, K & R 2024, 114, juris Rdnr. 82; EuGH, Urteil vom 04.05.2023, C-300/21, NJW 2023, 1930, juris Rdnr. 32; EuGH, Urteil vom 14.12.2023, C-340/21, NJW 2024, 1091, juris Rdnr. 77). Ein Schaden wird daher nicht bereits aufgrund des Verstoßes gegen die DS-GVO vermutet (EuGH, Urteil vom 20.06.2024, NJW 2024, 2599, C-182/22, juris Rdnr. 42).

62
Die DS-GVO verweist für den Sinn und die Tragweite der in ihrem Art. 82 enthaltenen Begriffe, insbesondere in Bezug auf die Begriffe „materieller oder immaterieller Schaden“ und „Schadenersatz“, nicht auf das Recht der Mitgliedstaaten. Daraus folgt, dass diese Begriffe für die Anwendung der DS-GVO als autonome Begriffe des Unionsrechts anzusehen sind, die in allen Mitgliedstaaten einheitlich auszulegen sind (EuGH, Urteil vom 04.05.2023, C300/21, NJW 2023, 1930, juris Rdnr. 30; EuGH, Urteil vom 14.12.2023, C-456/22, K & R 2024, 112, juris Rdnr. 15). Dabei soll nach Erwägungsgrund 146 S. 3 DS-GVO der Begriff des Schadens weit ausgelegt werden, in einer Art und Weise, die den Zielen der DS-GVO in vollem Umfang entspricht, namentlich dem Ziel, innerhalb der Union ein gleichmäßiges und hohes Niveau des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten (BGH, Urteil vom 28.01.2025, VI ZR 183/22, NJW 2025, 1059, juris Rdnr. 9; EuGH, Urteil vom 14.12.2023, C-456/22, K & R 2024, 112, juris Rdnr. 19 f.).

63

2. Die Beklagte ist Verantwortliche i. S. d. Art. 4 Nr. 7 DS-GVO. Sie ist die juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

64
Die Angaben zu den Personalien des Klägers sind als Informationen über bestimmte oder bestimmbare natürliche Personen „personenbezogene Daten“ im Sinne von Art. 4 Nr. 1 DSGVO (EuGH, Urteil vom 04.10.2024, C-200/23, juris Rdnr. 67).

65
Der Verarbeitungsbegriff des Art. 4 Nr. 2 DS-GVO ist umfassend und inkludiert jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Diese Aufzählung ist nicht abschließend (EuGH, Urteil vom 24.02.2022, C-175/20, K & R 2022, 260, juris Rdnr. 35).

66
Selbst bei einem engeren Verständnis des Art. 82 Abs. 1 DS-GVO wäre in Bezug auf den hier inmitten stehenden Scraping-Vorfall ohne Weiteres von einer Datenverarbeitung der Beklagten in Form der Speicherung, des Abfragens, der Offenlegung durch Übermittlung, der Bereitstellung und Verknüpfung auszugehen (vgl. BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 23).

67
3. Die Beklagte hat mit der Voreinstellung der Suchbarkeit anhand einer Telefonnummer auf „Alle“ gegen den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. b) und c), Art. 25 Abs. 2 S. 1, S. 3 DS-GVO verstoßen.

68
a) Gemäß Art. 5 Abs. 1 Buchst. b) Halbs. 1 DS-GVO müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“). Der Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c) DS-GVO verlangt, dass die Datenverarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt ist. Die Ausnahmen und Einschränkungen des Grundsatzes des Schutzes solcher Daten müssen sich auf das absolut Notwendige beschränken (EuGH, Urteil vom 24.02.2022, C-175/20, K & R 2022, 260, juris Rdnr. 72 f.; BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 87).

69
Die Grundsätze des Art. 5 DS-GVO werden durch konkrete Vorgaben zur technischen Ausgestaltung und insbesondere durch Vorgaben in Bezug auf datenschutzfreundliche Voreinstellungen in Art. 25 DS-GVO konkretisiert. Gemäß Art. 25 Abs. 2 S. 1 DSGVO hat der Verantwortliche demnach geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Die Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Damit beinhaltet Art. 25 Abs. 2 S. 3 DS-GVO die ausdrückliche Verpflichtung zu Voreinstellungen, die verhindern, dass die Daten ohne Weiteres, also ohne bewusste persönliche Änderung der Voreinstellung, der Öffentlichkeit oder sonst einem unbestimmten Adressatenkreis zugänglich gemacht werden (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 88 m. w. N.).

70
Die Vorgabe, die Daten nicht „einer unbestimmten Zahl natürlicher Personen“ zugänglich zu machen, ist nach ihrem Zweck darauf ausgelegt, dass der Personenkreis derjenigen, die Zugriff auf die Daten des Betroffenen haben können, für diesen überschaubar sein soll. Die Regelung des Art. 25 Abs. 2 DS-GVO hat dabei gerade die Voreinstellungen von sozialen Netzwerken im Blick. Dahinter steht die Erkenntnis, dass

werksseitig vorgegebene Voreinstellungen durch die Nutzer nur selten verändert werden. Es soll daher verhindert werden, dass Nutzer durch Voreinstellungen, die eine über die erforderliche Verarbeitung hinausgehende extensive Datennutzung vorsehen, dazu verleitet werden, ihre Datenschutzrechte abzuwählen, ohne dies zu realisieren (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 89 m. w. N.).

71
b) Diesen Anforderungen wurde das Vorgehen der Beklagten zum maßgeblichen Zeitpunkt des Scraping-Vorfalls nicht gerecht. Im relevanten Zeitraum war die Suchbarkeit anhand einer Telefonnummer für das Nutzerkonto des Klägers standardmäßig auf „Alle“ gestellt. Soweit der Kläger im Zusammenhang mit dem Unterlassungsantrag in der Berufungsinstanz behauptet, die Suchbarkeitseinstellung sei im Zeitraum 2018/2019 von „Alle“ auf „Friends of Friends“ umgestellt worden, fehlt es an einem Beleg und widerspricht er seinem eigenen Vorbringen erster Instanz. Außerdem hat die Beklagte die Standard-Einstellung „Alle“ nicht nur zugestanden, sondern einen Auszug aus dem Kundenkonto des Klägers vorgelegt, aus dem hervorgeht, dass auch bei ihm die Suchbarkeitseinstellung wie voreingestellt auf „Everyone“ lautete. Diesen Sachverhalt legt der Senat daher zugrunde.

72
Die Einstellung hatte zur Folge, dass alle anderen F. -Nutzer eine entsprechende Rufnummernsuche durchführen konnten. Gleichzeitig wurde über die Suchbarkeit der Rufnummer auch der Zugriff auf die weiteren Profilinformationen eröffnet, was sich konkret in der Vorgehensweise der Scraper niederschlug, die den Umstand ausnutzten, über die Verknüpfung der Telefonnummer sodann die öffentlichen personenbezogenen Daten des Nutzerprofils abzugreifen. Eine Einschränkung der Suchbarkeit konnte nur durch aktive Veränderung der Suchbarkeitseinstellungen durch den Nutzer selbst herbeigeführt werden. Datenschutzfreundlichere Einstellungsoptionen – insbesondere die erst 2019 eingeführte Suchbarkeitsoption „Nur ich“ – wurden demgegenüber nur als Optionen angeboten, obwohl die Nutzbarkeit des sozialen Netzwerks als solche hiervon nicht abhing, da eine Suche auch über die Eingabe des Namens möglich gewesen wäre. Die Beklagte ist damit ihrer in Art. 5 Abs. 2 DS-GVO festgeschriebenen Pflicht, die Einhaltung der Grundsätze des Art. 5 Abs. 1 DS-GVO nachzuweisen, nicht nachgekommen.

73
c) Die Voreinstellung war nicht durch Art. 6 Abs. 1 DS-GVO gedeckt.

74
aa) Art. 6 Abs. 1 S. 1 Buchst. a) DS-GVO sieht vor, dass die Verarbeitung rechtmäßig ist, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat.

75
Die Beklagte hat in der Berufungserwiderung gerade klargestellt, dass sich die Verarbeitung personenbezogener Daten zur Bereitstellung der F. -Plattform – und somit auch die damit verbundene Verarbeitung im Zusammenhang mit der Kontakt-Import-Funktion – gerade nicht auf eine Einwilligung des Nutzers stützt, sondern vielmehr auf die Durchführung des Nutzervertrages als solchen.

76
bb) Gemäß Art. 6 Abs. 1 S. 1 Buchst. b) DS-GVO ist eine Verarbeitung rechtmäßig, die für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen.

77
Es trifft zwar zu, wie von der Beklagten ausgeführt, dass sich der zwischen den Parteien geschlossene Nutzervertrag auf die Bereitstellung der F. Plattform als soziales Netzwerk bezieht und es einem solchen immanent ist, dass die einzelnen Nutzer Freunde und Bekannte finden und sich miteinander vernetzen können. Richtig ist auch, dass solche Verknüpfungen durch die Verwendung von Funktionen wie der Kontakt-Import-Funktion hergestellt werden, die dafür die Telefonnummern von Nutzern erfordern. Allerdings fehlt es insoweit am Tatbestandsmerkmal der Erforderlichkeit, das voraussetzt, dass die Verarbeitung personenbezogener Daten für die Vertragserfüllung objektiv unerlässlich ist, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist, so dass der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte

(EuGH, Urteil vom 04.07.2023, NJW 2023, 2997, C-252/21, juris Rdnr. 125; OLG Brandenburg, Urteil vom 24.03.2025, 1 U 18/23, juris Rdnr. 41).

78
Ein solcher Nachweis ist der Beklagten nicht gelungen. Die Nutzbarkeit von F. als Social-Media-Plattform hängt nicht allein von einer Suchbarkeit anhand der Telefonnummer ab. Ein Nutzer kann auch durch Eingabe seines Namens gefunden werden, wenngleich sich die Suche wegen der enormen Zahl an F. - Nutzern – die Beklagte spricht von ca. 2,8 Milliarden weltweit mühselig gestaltet und gegebenenfalls eine Reihe von Treffern durchforstet werden müssen. Eine Notwendigkeit, wie sie Art. 6 Abs. 1 S. 1 Buchst. b) DSGVO voraussetzt, bestand für das ehemals implementierte CIT jedenfalls nicht. Es handelte sich um ein reines Komfort-Tool, das den Nutzern ermöglichte, seine auf dem Mobiltelefon gespeicherten Kontakte rasch und ohne großen Aufwand auf F. zu spiegeln, sofern seine Kontakte dort Konten unterhielten. Im Übrigen zeigt bereits der Umstand, dass die Beklagte ihren Nutzern die Möglichkeit einräumt, im Rahmen der Suchbarkeitseinstellungen festzulegen, ob und wem die nicht immer öffentlichen Profildaten gezeigt werden und wer danach suchen kann, dass diese Informationen gerade nicht unabdingbar für eine hinreichende Verknüpfung der Nutzer untereinander sind.

79
cc) Weitere Einwilligungsalternativen des Art. 6 Abs. 1 S. 1 DS-GVO, der eine erschöpfende und abschließende Aufzählung enthält (EuGH, Urteil vom 04.05.2023, CR 2023, 439, C-60/22, juris Rdnr. 56), kommen nicht in Betracht, auch nicht Art. 6 Abs. 1 S. 1 Buchst. c) DS-GVO, wonach die Verarbeitung rechtmäßig ist, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Nach Art. 6 Abs. 3 DS-GVO wird die Rechtsgrundlage für diese Verarbeitung entweder durch Unionsrecht oder das Recht der Mitgliedsstaaten festgelegt, dem der Verantwortliche unterliegt. Dabei muss die Rechtsgrundlage ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Ziel stehen und diese Verarbeitung innerhalb der Grenzen des unbedingt Notwendigen erfolgen (EuGH, Urteil vom 04.07.2023, NJW 2023, 2997, C-252/21, juris Rdnr. 138). Hierzu hat die Beklagte nichts vorgebracht.

80
Art. 6 Abs. 1 S. 1 Buchst. f) DS-GVO wiederum setzt die Erforderlichkeit der Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten voraus, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Dies ist nur dann der Fall, wenn der fragliche Betreiber den Nutzern, bei denen die Daten erhoben wurden, ein mit der Datenverarbeitung verfolgtes berechtigtes Interesse mitgeteilt hat, wenn diese Verarbeitung innerhalb der Grenzen dessen erfolgt, was zur Verwirklichung dieses berechtigten Interesses unbedingt notwendig ist und wenn sich aus einer Abwägung der einander gegenüberstehenden Interessen unter Würdigung aller relevanten Umstände ergibt, dass die Interessen oder Grundrechte und Grundfreiheiten dieser Nutzer gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen (EuGH, Urteil vom 04.07.2023, NJW 2023, 2997, C-252/21, juris Rdnr. 126). Auch insoweit fehlt es an schlüssigem Vorbringen der Beklagten.

81
Ein Verstoß gegen die DS-GVO liegt somit vor.

82
4. Die Beklagte haftet nach Art. 82 Abs. 1 DS-GVO. Die Verschuldensvermutung des Art. 82 Abs. 3 DS-GVO hat sie nicht widerlegt.

83
a) Art. 5 Abs. 1 Buchst. b) und c), Art. 25 Abs. 2 S. 1, S. 3 DS-GVO sind vom Anwendungsbereich des Art. 82 Abs. 1 DS-GVO erfasst (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 24).

84
b) Der Verstoß der Beklagten gegen Art. 5 Abs. 1 Buchst. b) und c), Art. 25 Abs. 2 S. 1, S. 3 DS-GVO hatte zur Folge, dass das Benutzerkonto des Klägers mit der Voreinstellung der Suchfunktion auf „Alle“ versehen war. Der Scraping-Vorfall bei der Beklagten als solcher steht ebenso fest wie die anschließende Veröffentlichung abgegriffener Daten des Klägers im Internet.

85
Zumindest die Nutzer-ID, der Name, das Geschlecht und die Telefonnummer des Klägers waren von dem Datenvorfall betroffen. Name, Geschlecht und Nutzer-ID gehören zu den ohnehin immer öffentlich einsehbaren Informationen, die Telefonnummer war gerade der entscheidende Link, um diese Daten zusammenzuführen. Der Kläger hat sich im Hinblick auf seine Betroffenheit auf die „Leak-Liste“ berufen.

86
c) Art. 82 DS-GVO sieht eine Haftung für vermutetes Verschulden vor. Damit hat nicht die betroffene Person im Rahmen eines Schadensersatzanspruches nach Art. 82 Abs. 1 DS-GVO ein Verschulden des Verantwortlichen nachzuweisen, sondern die Exkulpation obliegt nach Art. 82 Abs. 3 DS-GVO dem Verantwortlichen (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 21; EuGH, Urteil vom 11.04.2024, C-741/21, NJW 2024, 1561, juris Rdnr. 46; EuGH, Urteil vom 21.12.2023, C-667/21, K & R 2024, 114, juris Rdnr. 103).

87
Nach Art. 82 Abs. 3 DS-GVO wird der Verantwortliche oder der Auftragsverarbeiter von der Haftung gemäß Art. 82 Abs. 2 DS-GVO befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

88
Diese Vorschrift ist eng auszulegen. Der Verantwortliche kann sich bei einer Verletzung des Schutzes personenbezogener Daten durch eine unbefugte Offenlegung bzw. einen unbefugten Zugang eines Dritten i. S. v. Art. 4 Nr. 10 DS-GVO nur dann von seiner Haftung befreien, wenn er nachweist, dass es keinen Kausalzusammenhang zwischen der etwaigen Verletzung der Verpflichtung zum Datenschutz durch ihn und dem der natürlichen Person entstandenen Schaden gibt (EuGH, Urteil vom 14.12.2023, C-340/21, NJW 2024, 1091, juris Rdnr. 70, 72, 74).

89
Der Scraping-Vorfall kann der Beklagten zwar nicht unmittelbar angelastet werden, weil er durch von ihr unabhängige Personen in unredlicher Absicht durchgeführt wurde. Jedoch hat die Beklagte mittels ihrer Voreinstellung zur Suchbarkeit anhand der Telefonnummer auf „Alle“ den automatisierten und massenhaften Einsatz der Kontakt-Import-Funktion und damit das Abgreifen der öffentlich einsehbaren Daten von betroffenen Nutzern ermöglicht. Für die Beklagte als weltweit agierendes Unternehmen mit langjähriger Erfahrung und spezifischer technischer Expertise im Betrieb von sozialen Netzwerken war es ohne weiteres erkennbar, dass die von ihr gewählte Voreinstellung zur Suchbarkeit mit Blick darauf, die viele Nutzer es sehr wahrscheinlich bei dieser Voreinstellung belassen werden, das Netzwert zu einem attraktiven Ziel für Scraping machen würde. Die Beklagte unterhielt gerade zu diesem Zwecke eine Abteilung, um die Gefahr solcher Datenabgriffe zu minimieren. Den effektivsten Schritt, das Kontakt-Import-Tool zu deaktivieren bzw. es zu modifizieren, unternahm sie jedoch erst nach dem streitgegenständlichen Vorfall.

90
5. Durch den Verstoß der Beklagten gegen die Datenschutzbestimmungen ist dem Kläger ein immaterieller Schaden entstanden, den der Senat mit 200,00 € bemisst.

91
a) Der bloße Verstoß gegen die Bestimmungen der Datenschutz-Grundverordnung reicht nicht aus, um einen Schadensersatzanspruch zu begründen. Der Eintritt eines Schadens im Rahmen einer rechtswidrigen Verarbeitung personenbezogener Daten ist nämlich eine nur potenzielle und keine automatische Folge einer solchen Verarbeitung. Außerdem führt ein Verstoß gegen die DS-GVO nicht zwangsläufig zu einem Schaden. Schließlich muss ein Kausalzusammenhang zwischen dem fraglichen Verstoß und dem der betroffenen Person entstandenen Schaden bestehen (EuGH, Urteil vom 04.10.2024, C-507/23, NJW 2025, 141, juris Rdnr. 27; EuGH, Urteil vom 04.05.2023, C-300/21, NJW 2023, 1930, juris Rdnr. 37).

92
Es ist daher über einen Verstoß gegen die DS-GVO hinaus – im Sinne einer eigenständigen Anspruchsvoraussetzung – der Eintritt eines tatsächlichen Schadens (durch diesen Verstoß) erforderlich, den die betroffene Person nachzuweisen hat. Andererseits darf der Ersatz eines immateriellen Schadens nicht davon abhängig gemacht werden, dass der der betroffenen Person entstandene Schaden einen

bestimmten Grad an Schwere oder Erheblichkeit erreicht hat (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 28 f.; EuGH, Urteil vom 25.01.2024, C-687/21, NJW 2024, 2009, juris Rdnr. 59 f.; EuGH, Urteil vom 11.04.2024, C-741/21, NJW 2024, 1561, juris Rdnr. 36; EuGH, Urteil vom 04.05.2023, C-300/21, NJW 2023, 1930, juris Rdnr. 46; EuGH, Urteil vom 20.06.2024, C-590/22, VersR 2024, 1302, juris Rdnr. 28).

93
Dabei kann der – selbst kurzzeitige – bloße Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden darstellen, ohne dass dieser Begriff den Nachweis zusätzlicher spürbarer negativer Folgen erfordert, etwa eine missbräuchliche Verwendung der betreffenden Daten zum Nachteil der betroffenen Person. Es bedarf auch keiner sich aus dem Kontrollverlust entwickelnden besonderen Befürchtungen oder Ängste der betroffenen Person. Diese wären lediglich geeignet, den eingetretenen immateriellen Schaden noch zu vertiefen oder zu vergrößern. In diesen Fällen muss der Kontrollverlust aber feststehen, d. h. von der betroffenen Person nachgewiesen worden sein (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 30 f.; EuGH, Urteil vom 11.04.2024, C-741/21, NJW 2024, 1561, juris Rdnr. 42; EuGH, Urteil vom 25.01.2024, C-687/21, NJW 2024, 2009, juris Rdnr. 65 f.; EuGH, Urteil vom 14.12.2023, C-340/21, NJW 2024, 1091, juris Rdnr. 82, 84; EuGH, Urteil vom 14.12.2023, C-456/22, K & R 2024, 112, juris Rdnr. 22; EuGH, Urteil vom 04.10.2024, C-200/23, juris Rdnr. 156).

94
Kann der Betroffene den Kontrollverlust nicht nachweisen, reicht die begründete Befürchtung einer Person, dass ihre personenbezogenen Daten aufgrund eines Verstoßes gegen die DS-GVO von Dritten missbräuchlich verwendet werden, aus, um einen Schadensersatzanspruch zu begründen. Jedoch muss in diesem Fall die Befürchtung samt ihrer negativen Folgen ordnungsgemäß nachgewiesen sein. Die bloße Behauptung reicht ebenso wenig wie ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten aus (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 32; EuGH, Urteil vom 25.01.2024, C-687/21, NJW 2024, 2009, juris Rdnr. 67 f.; EuGH, Urteil vom 20.06.2024, C-590/22, VersR 2024, 1302, juris Rdnr. 36; EuGH, Urteil vom 14.12.2023, C-340/21, NJW 2024, 1091, juris Rdnr. 85).

95
b) Nach diesen Maßstäben ist der Kontrollverlust eingetreten, ein immaterieller Schaden steht damit fest. Es ist unstreitig, dass zumindest der Name und das Geschlecht des Klägers neben der zugeordneten Mobilfunknummer vom Scraping-Vorfall erfasst wurden. Diese Daten wurden von Dritten im Darknet verfügbar gemacht. Für den Kläger besteht keine realistische Möglichkeit, die Kontrolle über seine Daten zurückzuerlangen. Auf die Frage, ob damit Befürchtungen oder Ängste verbunden sind, kommt es daher allenfalls für die Bemessung der Höhe des notwendigen Ausgleichs an, nicht aber für die Feststellung des Schadens als solchem.

96
Dass der Kläger Daten wie seine Telefonnummer auch bei anderen Social MediaAnbietern oder Onlinehändlern hinterlegt hat, schließt den Kontrollverlust nicht aus. Der Kläger hat in seiner Anhörung klargestellt, grundsätzlich einen bewussten Umgang mit seinen Daten zu üben und seine Daten mit Bedacht und nicht wahllos weiterzugeben. Zeitlich hat er die fragwürdigen Vorgänge so verortet, dass sie selbst nach den Angaben der Beklagten mit dem Datenscraping in Zusammenhang gebracht werden können. Anhaltspunkte dafür, dass der Kläger unter anderem seine Telefonnummer, kombiniert mit Name und Geschlecht, aufgrund eines früheren sorglosen Umgangs verloren hätte, ergeben sich nicht. Die Beklagte hat auch keine anderen Gelegenheiten aufgezeigt, bei denen der Kläger einen Kontrollverlust erlitten haben könnte oder musste oder dass dies zeitlich vor dem Scraping-Vorfall gewesen sei, z. B. über Konten bei anderen Kommunikationsplattformen. Zwar hat der Kläger auch anderen Dritten seine Telefonnummer bekannt gegeben, für deren uneingeschränkte datenschutzkonforme Handhabung er nicht garantieren kann. Das durch die Abschöpfung der Daten aus dem Datenbestand der Beklagten und die anschließende Veröffentlichung im Internet mit Zugriffsmöglichkeit für jede Person eingetretene Risiko unterscheidet sich jedoch wesentlich von einer bewussten und zielgerichteten Weitergabe an bestimmte Empfänger (vgl. BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 42).

97
c) Den Schadensersatz bemisst der Senat mit 200,00 €.

98
aa) Bei der Bemessung des Betrags des auf die DS-GVO gestützten Schadensersatzanspruchs sind die in Art. 83 DS-GVO vorgesehenen Kriterien für die Festsetzung des Betrags von Geldbußen nicht entsprechend anzuwenden (EuGH, Urteil vom 20.06.2024, C-590/22, VersR 2024, 1302, juris Rdnr. 44).

99
Die DS-GVO enthält keine Bestimmung über die Bemessung des nach Art. 82 DS-GVO geschuldeten Schadenersatzes. Folglich haben die nationalen Gerichte zum Zweck dieser Bemessung nach dem Grundsatz der Verfahrensautonomie die innerstaatlichen Vorschriften der einzelnen Mitgliedstaaten über den Umfang der finanziellen Entschädigung anzuwenden, sofern die vom EuGH definierten unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität beachtet werden (EuGH, Urteil vom 11.04.2024, C-741/21, NJW 2024, 1561, juris Rdnr. 58; EuGH, Urteil vom 04.10.2024, C-507/23, NJW 2025, 141, juris Rdnr. 32; EuGH, Urteil vom 25.01.2024, C-687/21, NJW 2024, 2009, juris Rdnr. 53; EuGH, Urteil vom 21.12.2023, C-667/21, K & R 2024, 114, juris Rdnr. 83; EuGH, Urteil vom 04.05.2023, C-300/21, NJW 2023, 1930, juris Rdnr. 54; EuGH, Urteil vom 20.06.2024, NJW 2024, 2599, C-182/22, juris Rdnr. 27).

100
Dabei ist zu berücksichtigen, dass dem in Art. 82 Abs. 1 DS-GVO niedergelegten Schadensersatzanspruch ausschließlich eine Ausgleichsfunktion zukommt. Er erfüllt keine Abschreckungs- oder gar Straffunktion, weshalb auch das Vorliegen mehrerer auf denselben Verarbeitungsvorgang bezogener Verstöße nicht zu einer Erhöhung des Schadensersatzes führt (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 18; EuGH, Urteil vom 11.04.2024, C-741/21, NJW 2024, 1561, juris Rdnr. 59 f., 64 f.; EuGH, Urteil vom 25.01.2024, C-687/21, NJW 2024, 2009, juris Rdnr. 47; EuGH, Urteil vom 21.12.2023, C-667/21, K & R 2024, 114, juris Rdnr. 85; BGH, Urteil vom 28.01.2025, VI ZR 183/22, NJW 2025, 1059, juris Rdnr. 10; EuGH, Urteil vom 20.06.2024, NJW 2024, 2599, C-182/22, juris Rdnr. 23).

101
Dies hat unter anderem zur Folge, dass sich die Schwere eines solchen Verstoßes nicht auf die Höhe des gewährten Schadenersatzes auswirken darf und der Schadenersatz nicht in einer Höhe bemessen werden darf, die über den vollständigen Ausgleich des Schadens hinausgeht (EuGH, Urteil vom 04.10.2024, C-507/23, NJW 2025, 141, juris Rdnr. 43; EuGH, Urteil vom 11.04.2024, C-741/21, NJW 2024, 1561, juris Rdnr. 60; EuGH, Urteil vom 25.01.2024, C-687/21, NJW 2024, 2009, juris Rdnr. 48, 52; EuGH, Urteil vom 21.12.2023, C-667/21, K & R 2024, 114, juris Rdnr. 86; EuGH, Urteil vom 20.06.2024, C-590/22, VersR 2024, 1302, juris Rdnr. 41). Darüber hinaus verlangt Art. 82 DS-GVO nicht, dass der Grad des Verschuldens des Verantwortlichen bei der Höhe des Schadenersatzes berücksichtigt wird (EuGH, Urteil vom 21.12.2023, C-667/21, K & R 2024, 114, juris Rdnr. 103; BGH, Urteil vom 28.01.2025, VI ZR 183/22, NJW 2025, 1059, juris Rdnr. 11; EuGH, Urteil vom 20.06.2024, NJW 2024, 2599, C-182/22, juris Rdnr. 28). Nicht relevant ist des Weiteren, dass der Verstoß gegen die DS-GVO zugleich einen Verstoß gegen nationale Vorschriften mit sich bringt, die sich auf den Schutz personenbezogener Daten beziehen, aber nicht bezwecken, die Bestimmungen der DS-GVO zu präzisieren (EuGH, Urteil vom 20.06.2024, C-590/22, VersR 2024, 1302, juris Rdnr. 48). Ebenso wenig finden die Haltung und die Beweggründe des Verantwortlichen Eingang, zumindest dann nicht, wenn dies dazu dienen soll, der betroffenen Personen einen Schadensersatz zu gewähren, der geringer ist als der Schaden, der ihr konkret entstanden ist (EuGH, Urteil vom 04.10.2024, C-507/23, NJW 2025, 141, juris Rdnr. 45).

102
Mithin ist in Anbetracht der Ausgleichsfunktion eine auf Art. 82 DS-GVO gestützte finanzielle Entschädigung als „vollständig und wirksam“ anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen, ohne dass ein solcher vollumfänglicher Ausgleich die Verhängung von Strafschadenersatz erfordert (EuGH, Urteil vom 11.04.2024, C-741/21, NJW 2024, 1561, juris Rdnr. 60 f.; EuGH, Urteil vom 04.10.2024, C-507/23, NJW 2025, 141, juris Rdnr. 34, 40; EuGH, Urteil vom 21.12.2023, C-667/21, K & R 2024, 114, juris Rdnr. 84; EuGH, Urteil vom 04.05.2023, C-300/21, NJW 2023, 1930, juris Rdnr. 58 BGH, Urteil vom 28.01.2025, VI ZR 183/22, NJW 2025, 1059, juris Rdnr. 11; EuGH, Urteil vom 20.06.2024, C-590/22, VersR 2024, 1302, juris Rdnr. 42).

103

bb) Ein Betrag von 200,00 € gleicht den konkret erlittenen Schaden des Klägers aus. Betroffen war im Wesentlichen die Mobilfunknummer des Klägers, nachrangig die anderen, ohnehin stets öffentlich einsehbaren Daten wie Name, Geschlecht und F. -ID, die dennoch in der Zusammenschau mit der Telefonnummer ein durchaus sensibles „Datenpaket“ ergaben.

104
Der Kontrollverlust ist dauerhaft, eine Rückerlangung der Kontrolle über die Daten praktisch ausgeschlossen. Der potentielle Empfängerkreis dieser Daten ist grundsätzlich unbegrenzt. Emotionale Beeinträchtigungen ließen sich den Äußerungen des Klägers hingegen nicht entnehmen, wenngleich er mit seiner Aussage seine Unsicherheit und die Sorge über den erlittenen Datenverlust nachvollziehbar zum Ausdruck gebracht hat. So berichtete er unter anderem von SMS mit der Ankündigung einer Paketlieferung und einem Link und von Anrufen, ohne dass sich der Anrufer gemeldet habe. Seine Angaben zeigten auch, dass der Vorgang sein Misstrauen geweckt hat und ihn zu mehr Vorsicht im Umgang mit den Daten im Internet anhält.

105
In der Gesamtwürdigung unter Berücksichtigung der Art der betroffenen Daten und der Beeinträchtigung des Klägers ist die Zahlung von 200,00 € geeignet, die erlittene immaterielle Beeinträchtigung vollständig auszugleichen.

106
d) Ob die weiteren, vom Kläger behaupteten Verstöße der Beklagten gegen die DS-GVO vorliegen und ob diese von Art. 82 Abs. 1 DS-GVO erfasst sind, kann dahingestellt bleiben. Wie oben ausgeführt, ziehen sie ihr Vorliegen unterstellt mit Blick auf die Ausgleichsfunktion der genannten Norm keine Erhöhung des Schadensersatzanspruchs nach sich. Eine Erweiterung oder Vertiefung des Schadens ist mit einer Verletzung der Aufklärungspflicht, einer Verletzung der Pflicht zur Implementierung angemessener technischer und organisatorischer Maßnahmen und einer Verletzung von Benachrichtigungs- und Informationspflichten etc. nicht verbunden. Es handelt sich um ein einheitliches Schadensereignis mit einheitlichen Folgen.

IV.

107
Der Antrag auf Feststellung, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen Schäden zu ersetzen, die dem Kläger durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden, ist zulässig und hat in der Sache Erfolg.

108
1. Die bloße Möglichkeit des künftigen Eintritts der geltend gemachten Schäden reicht für ein Feststellungsinteresse aus, weil es nicht um reine Vermögensschäden geht, sondern um Schäden, die aus der vom Kläger behaupteten Verletzung seines Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 GG 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. Eine darüberhinausgehende hinreichende Schadenswahrscheinlichkeit ist nicht erforderlich. Auch die primär als Anspruchsgrundlage herangezogene Vorschrift des Art. 82 DS-GVO hat jedenfalls dann, wenn mit einem möglichen Verstoß gegen Art. 5 DS-GVO auch eine unrechtmäßige Datenverarbeitung gerügt wird, eine Verletzung des Rechts auf Schutz der personenbezogenen Daten gemäß Art. 8 GRCh zum Inhalt (vgl. Art. 1 Abs. 2 DS-GVO). Dabei kann die Möglichkeit ersatzpflichtiger künftiger Schäden ohne Weiteres zu bejahen sein, wenn ein deliktsrechtlich geschütztes absolutes Rechtsgut verletzt wurde und bereits ein Schaden eingetreten ist (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 48).

109
2. Dies ist hier der Fall. Der bereits eingetretene Kontrollverlust des Klägers in Form der Veröffentlichung seiner Daten (insbesondere seines Namens in Verbindung mit seiner Mobilfunknummer) dauert an. Somit besteht die Gefahr der missbräuchlichen Benutzung der Daten fort und ist auch nicht nur rein theoretischer Natur.

110

Entgegen der Ansicht der Beklagten stützt sich der Bundesgerichtshof mit seiner Rechtsprechung nicht maßgeblich auf das grundgesetzlich geschützte Recht der informationellen Selbstbestimmung, sondern verortet die Wertung im Rahmen des Art. 82 DS-GVO.

111
3. Angesichts der feststehenden Rechtsverletzung der Beklagten und der feststehenden Schadensersatzpflicht nach Art. 82 Abs. 1 DS-GVO ist der Feststellungsantrag auch begründet.

V.

112
Der Antrag, die Beklagte zu verurteilen, es zu unterlassen, personenbezogenen Daten des Klägers, namentlich/welche da sind Telefonnummer, F. ID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern, ist unzulässig. Der Antrag ist nicht hinreichend bestimmt.

113
1. Ein Klageantrag ist hinreichend bestimmt i. S. d. § 253 Abs. 2 Nr. 2 ZPO, wenn er den erhobenen Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) absteckt, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennen lässt, das Risiko eines Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abwälzt und eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (BGH, Urteil vom 09.03.2021, VI ZR 73/20, NJW 2021, 1756, juris Rdnr. 15; BGH, Urteil vom 15.01.2019, VI ZR 506/17, NJW 2019, 781, juris Rdnr. 12; BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 52).

114
Eine hinreichende Bestimmtheit ist bei einem Unterlassungsantrag für gewöhnlich gegeben, wenn eine Bezugnahme auf die konkrete Verletzungshandlung 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 (vgl. BGH, Urteil vom 09.03.2021, VI ZR 73/20, NJW 2021, 1756, juris Rdnr. 15; BGH, Urteil vom 15.01.2019, VI ZR 506/17, NJW 2019, 781, juris Rdnr. 12). Die Verwendung auslegungsbedürftiger Begriffe im Klageantrag ist zulässig, wenn über ihren Sinngehalt zwischen den Parteien kein Streit besteht und objektive Maßstäbe zur Abgrenzung vorliegen, oder wenn der Kläger den auslegungsbedürftigen Begriff hinreichend konkret umschreibt und gegebenenfalls mit Beispielen unterlegt oder sein Begehren an der konkreten Verletzungshandlung ausrichtet (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 53).

115
Unterlassungsanträge, die lediglich den Wortlaut eines Gesetzes wiederholen, sind grundsätzlich als unbestimmt anzusehen, wenn nicht entweder bereits der gesetzliche Verbotstatbestand selbst entsprechend eindeutig und konkret gefasst oder der Anwendungsbereich einer Rechtsnorm durch eine gefestigte Auslegung geklärt ist, oder wenn der Kläger hinreichend deutlich macht, dass er nicht ein Verbot im Umfang des Gesetzeswortlauts beansprucht, sondern sich mit seinem Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert. Die Bejahung der Bestimmtheit setzt in solchen Fällen allerdings grundsätzlich voraus, dass zwischen den Parteien kein Streit darüber besteht, dass das beanstandete Verhalten das fragliche Tatbestandsmerkmal erfüllt. Die Wiedergabe des gesetzlichen Verbotstatbestands in der Antragsformulierung ist auch unschädlich, wenn sich das mit dem selbst nicht hinreichend klaren Antrag Begehrte im Tatsächlichen durch Auslegung unter Heranziehung des Sachvortrags des Klägers eindeutig ergibt und die betreffende tatsächliche Gestaltung zwischen den Parteien nicht infrage gestellt ist, sondern sich ihr Streit ausschließlich auf die rechtliche Qualifizierung der angegriffenen Verhaltensweise beschränkt. Eine auslegungsbedürftige Antragsformulierung kann im Übrigen hinzunehmen sein, wenn dies zur Gewährleistung effektiven Rechtsschutzes erforderlich ist (BGH, Urteil vom 28.07.2022, I ZR 205/20, NJW-RR 2022, 1417, juris Rdnr. 12; BGH, Urteil vom 22.07.2021, I ZR 194/20, CR 2022, 199, juris Rdnr. 34; BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 54).

116
2. Nach diesen Grundsätzen ist der Unterlassungsantrag des Klägers nicht hinreichend bestimmt und lässt sich auch unter Heranziehung des Klagevorbringens nicht bestimmt auslegen.

117
Die Begriffe „unbefugte Dritte“, „nach dem Stand der Technik mögliche Sicherheitsmaßnahmen“ und „Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme“ sind unbestimmt und auslegungsbedürftig. Eine gefestigte Auslegung dieser Formulierungen ist nicht ersichtlich und wurde vom Kläger nicht dargetan. Der Kläger begehrt sinngemäß, dass die Beklagte keine Funktion anbietet, die es Dritten erlaubt, auf seine personenbezogenen Daten zuzugreifen, wenn die Beklagte nicht durch geeignete Sicherheitsmaßnahmen einem Missbrauch dieser Funktion entgegenwirkt. Eine Eingrenzung der Verletzungshandlung findet allerdings nur insoweit statt, als auf die Kontakt-Import-Funktion Bezug genommen wird, welche der Kläger als Einfallstor für das Datenscraping identifiziert hat oder jedenfalls annimmt. Der pauschale Hinweis auf eine Ausnutzung der Kontakt-Import-Funktion ist für eine Konkretisierung jedoch nicht hinreichend. Er lässt nicht erkennen, durch welche konkrete Maßnahme die Beklagte gegen die Datenschutz-Grundverordnung verstoßen hat, obwohl eine weiter gehende Konkretisierung etwa durch Hinweis auf die Voreinstellung der Suchbarkeit auf „Alle“ möglich gewesen wäre. Eine Bezugnahme auf den streitgegenständlichen Datenschutzvorfall enthält der Unterlassungsantrag nicht.

VI.

118
Der Antrag, die Beklagte zu verurteilen, die Telefonnummer des Klägers auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der F. -Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird, ist jedenfalls unbegründet.

119
1. Der Antrag ist hinreichend bestimmt. Er lässt sich unter Heranziehung des Klagevorbringens dahingehend auslegen, dass der Kläger ein Unterlassen jeglicher Verarbeitung seiner Telefonnummer durch die Beklagte, die über die notwendige Verarbeitung für die Zwei-FaktorAuthentifizierung hinausgeht, begehrt. Der Kläger macht deutlich, für welche Zwecke die Beklagte seine Telefonnummer noch verarbeiten darf und für welche Zwecke er die Unterlassung der Datenverarbeitung begehrt (vgl. BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 62 ff.).

120
2. Der Kläger hat ein Rechtsschutzbedürfnis für den Antrag.

121
a) 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. Dies ist etwa dann 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 allerdings strenge Maßstäbe. Das Rechtsschutzbedürfnis fehlt (oder entfällt) nur dann, wenn das Betreiben des Verfahrens eindeutig zweckwidrig ist und sich als Missbrauch der Rechtspflege darstellt. Auch darf der Kläger nicht auf einen verfahrensmäßig unsicheren Weg verwiesen werden (BGH, Urteil vom 29.09.2022, I ZR 180/21, NJW-RR 2023, 66, juris Rdnr. 10, 16; BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 66 f.).

122
b) Zu einem vergleichbaren, denselben Scraping-Vorgang im Datenarchiv der Beklagten betreffenden Unterlassungsantrag hat der Bundesgerichtshof entschieden, dass das Rechtsschutzbedürfnis nicht entfällt, weil der Kläger seine Telefonnummer aus seinem Nutzerkonto selbst löschen könnte. Der Kläger würde sich damit der Möglichkeit der Zwei-Faktor-Authentifizierung für die Anmeldung in seinem Nutzerkonto begeben. Der BGH hat allerdings ausgeführt, dass in der Möglichkeit des Nutzers, seine Privatsphäre-Einstellungen so zu ändern, dass sich seine Einwilligung zur Verarbeitung seiner Telefonnummer auf die

Nutzung der Zwei-Faktor-Authentifizierung beschränkt, und die Suchbarkeitseinstellungen bezüglich seiner Telefonnummer seit Mai 2019 auf „Nur ich“ abzuändern, ein im Verhältnis zu einem entsprechenden Unterlassungstitel einfacherer und dementsprechend auch billigerer Weg liege. Der Bundesgerichtshof hat in dem von ihm entschiedenen Rechtsstreit das Rechtsschutzbedürfnis gleichwohl nicht verneinen können, weil das dortige Berufungsgericht keine Feststellungen zu dem Vortrag des Klägers getroffen hatte, dass sich aus einer von der Beklagten erteilten Information mit der Überschrift „Möglicherweise verwenden wir deine Telefonnummer für diese Zwecke“ die Besorgnis von Verarbeitungsvorgängen jenseits der ZweiFaktor-Authentifizierung ergebe (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, juris Rdnr. 68 f.).

123
Gerade auf diese Information stellt der Kläger des hiesigen Verfahrens ebenfalls ab, so dass von einem Rechtsschutzbedürfnis auszugehen ist.

124
3. Der Antrag ist jedoch unbegründet.

125
Dass die Telefonnummer des Klägers über die Suchfunktion auch dann noch ermittelt werden kann, wenn er diese auf die Zwei-Faktor-Authentifizierung begrenzt und im Übrigen die Suchbarkeitseinstellungen auf „Nur ich“ stellt, hat der Kläger nicht schlüssig dargelegt. Er hat sich darauf zurückgezogen, die Behauptung der Beklagten, das Auffinden des NutzerProfils und der dort hinterlegten Daten mittels Eingabe der Telefonnummer im Kontakt-Import-Tool sei nur dann möglich gewesen, wenn die Suchbarkeitseinstellung in dem jeweiligen Profil auf „Everyone“ gestellt gewesen sei, zu bestreiten und der Beklagten eine sekundäre Darlegungs- und Beweislast für die neu implementierte „Nur ich“-Funktion und die Beschränkung der Verwendung der Telefonnummer auf die Zwei-Faktor-Authentifizierung zuzusprechen. Allerdings hat der Kläger die Voraussetzungen für einen Unterlassungsantrag vorzutragen und nachzuweisen. Auf den Schriftsatz der Beklagten vom 12.02.2025, in dem diese mit Blick auf die BGH-Rechtsprechung nochmals ausführlich zu den Grenzen der Suchbarkeit eines Profils mittels Telefonnummer vorgetragen hat, ist er nicht mehr eingegangen.

126
Die Beklagte hat unter Verweis auf ihre Klageerwiderung und Anlage B6 klargestellt, dass die Frage, ob sie die Telefonnummer für die aufgeführten Zwecke verwende, davon abhänge, wofür der Nutzer diese hinterlege und wie er seine diesbezüglichen Einstellungen vorgenommen habe. Mit dem Wort „möglicherweise“ und der ihm folgenden Auflistung bringe sie transparent zum Ausdruck, welche Verwendungen der Telefonnummer in Betracht kommen und dass die Verwendung der Telefonnummer von Fall zu Fall unterschiedlich sein könne.

127
Tatsächlich steht die Anlage B6 in Zusammenhang mit den weiteren Erläuterungen im Hilfebereich zu den Privatsphäre-Einstellungen, die der Nutzer tätigen kann. Die Ausführungen sind nicht so zu verstehen, dass eine Verarbeitung und Nutzung der Telefonnummer unabhängig von den individuellen Einstellungen eines Nutzers gleichwohl für die aufgeführten Zwecke erfolge (vgl. OLG Koblenz, Urteil vom 11.02.2025, 3 U 145/24, juris Rdnr. 57).

VII.

128
Da der Kläger den zunächst in der Berufungsbegründung angekündigten Auskunftsantrag zurückgenommen hat, war darüber vom Senat nicht mehr zu entscheiden.

VIII.

129
Der Zinsanspruch folgt aus §§ 291, 288 Abs. 1 BGB.

IX.

130

Der Kläger hat Anspruch auf Erstattung der vorgerichtlichen Rechtsanwaltskosten nach Art. 82 Abs. 1 DS-GVO unter dem Gesichtspunkt erforderlicher Kosten einer zweckentsprechenden Rechtsverfolgung.

131
Die Kosten der Rechtsverfolgung und deshalb auch die Kosten eines mit der Sache befassten Rechtsanwalts gehören, soweit sie zur Wahrnehmung der Rechte erforderlich und zweckmäßig waren, grundsätzlich zu dem wegen einer unerlaubten Handlung zu ersetzenden Schaden (BGH, Urteil vom 17.11.2015, VI ZR 492/14, NJW 2016, 1245, juris Rdnr. 9). Dabei ist maßgeblich, wie sich die voraussichtliche Abwicklung des Schadensfalls aus der Sicht des Geschädigten darstellt.

132
Ist die Verantwortlichkeit für den Schaden und damit die Haftung von vornherein nach Grund und Höhe derart klar, dass aus der Sicht des Geschädigten kein vernünftiger Zweifel daran bestehen kann, dass der Schädiger ohne weiteres seiner Ersatzpflicht nachkommen werde, so wird es grundsätzlich nicht erforderlich sein, schon für die erstmalige Geltendmachung des Schadens gegenüber dem Schädiger einen Rechtsanwalt hinzuzuziehen. In derart einfach gelagerten Fällen kann der Geschädigte grundsätzlich den Schaden selbst geltend machen, so dass sich die sofortige Einschaltung eines Rechtsanwalts nur unter besonderen Voraussetzungen als erforderlich erweisen kann, wenn etwa der Geschädigte aus Mangel an geschäftlicher Gewandtheit oder sonstigen Gründen wie etwa Krankheit oder Abwesenheit nicht in der Lage ist, den Schaden selbst anzumelden (BGH, Urteil vom 08.11.1994, VI ZR 3/94, NJW 1995, 446, juris Rdnr. 9).

133
Der Kläger hatte die Beklagte über seine Prozessbevollmächtigten mit E-Mail vom 14.09.2021 unter anderem zur Zahlung von Schadensersatz in Höhe von 500,00 € auffordern lassen. Dieser Anspruch steht ihm dem Grunde, wenn auch nicht in der Höhe zu. Aufgrund der ungeklärten Rechtslage durfte sich der Kläger zu diesem Zeitpunkt bereits vorgerichtlich anwaltlicher Begleitung bedienen.

134
Der Anspruch berechnet sich nach dem Gegenstandswert der berechtigten Inanspruchnahme der Beklagten in Höhe von insgesamt 700,00 € (200,00 € für die Zahlung und 500,00 €, mit dem der Feststellungsantrag bemessen wird) mit einer 1,3 Gebühr nach Nr. 2003 VV RVG, der Pauschale nach Nr. 7002 VV RVG und der Umsatzsteuer nach Nr. 7008 VV RVG, somit 159,94 €.

X.

135
Die Kostenentscheidung beruht für die erste Instanz auf §§ 91 Abs. 1, 92 Abs. 1 ZPO, für die Berufungsinstanz zusätzlich auf §§ 97 Abs. 1, 516 Abs. 3 ZPO.

136
Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt aus §§ 708 Nr. 10, 711, 713 ZPO.

137
Die Streitwertfestsetzung ergibt sich aus §§ 47 Abs. 1 S. 1, 48 Abs. 1 S. 1 GKG in Verbindung mit § 3 ZPO. Maßgeblicher Zeitpunkt für die Bewertung des Gebührenstreitwerts ist nach § 40 GKG der Zeitpunkt der Antragstellung, die den Rechtszug einleitet, in der Berufungsinstanz also die Einreichung der Berufungsanträge. Später eingetretene wertreduzierende Antragsänderungen (z. B. teilweise Berufungsrücknahme, teilweise Klagerücknahme, teilweise Erledigterklärung etc.) bleiben in Bezug auf den Gebührenstreitwert außer Betracht (OLG München, Beschluss vom 13.12.2016, 15 U 2407/16, NJW-RR 2017, 700, juris Rdnr. 16; Toussaint/Elzer, Kostenrecht, 54.

138
Auflage 2024, § 40 GKG Rdnr. 11). Der Senat bemisst die Anträge wie folgt:

„Ziffer 1. 1.000,00 € Ziffer 2. 500,00 € Ziffer 3. a) 1.000,00 € Ziffer 3. b) 1.000,00 € Ziffer 4. 500,00 €

Der Antrag auf Zahlung der Kosten für die vorgerichtliche Rechtsverfolgung wirkt nicht streitwerterhöhend (BGH, Beschluss vom 25.09.2007, VI ZB 22/07, NJW-RR 2008, 374, juris Rdnr. 4 ff.).“

XI.

139
Die Revision ist nicht zuzulassen, die Voraussetzungen des § 543 Abs. 2 ZPO liegen nicht vor.

140
Die von beiden Parteien aus unterschiedlichen Gründen beantragte Aussetzung des Verfahrens konnte unterbleiben. Zu den für den hiesigen Rechtsstreit entscheidungserheblichen Fragen hat sich der Bundesgerichtshof ausdrücklich erklärt.