Quelle: https://voris.wolterskluwer-online.de/document/baa51346-6a4d-4998-81b3-6db61a20fe14

Bibliografie	
Gericht	OLG Braunschweig
Datum	05.06.2025
Aktenzeichen	2 U 71/24
Entscheidungsform	Urteil
Referenz	WKRS 2025, 17093
Entscheidungsname	[keine Angabe]
ECLI	ECLI:DE:OLGBS:2025:0605.2U71.24.00

Oberlandesgericht Braunschweig
Urt. v. 05.06.2025, Az.: 2 U 71/24

Anforderungen an die Darlegung eines Datenkontrollverlusts i.R.e. sog. Scraping-Vorfalls

Amtlicher Leitsatz

1. **Eine Erklärung mit Nichtwissen ist in eigenen Angelegenheiten unzulässig, wenn der Bestreitende seine Kenntnis vereitelt hat oder die Unkenntnis sich als Pflichtwidrigkeit darstellt.**

2. **Ein Kontrollverlust ist auch dann schlüssig vorgetragen, wenn die Partei keinen vereinzelten Vortrag zum Nichteintritt eines früheren Kontrollverlusts hält, solange der Vortrag der Gegenseite hierzu keinen Anlass bietet.**

In dem Rechtsstreit
(...)
hat der 2. Zivilsenat des Oberlandesgerichts Braunschweig durch (...) auf die mündliche Verhandlung vom 28.05.2025 für Recht erkannt:

Tenor:

Auf die Berufung der Klagepartei wird das Urteil des Landgerichts Braunschweig vom 20.03.2024 unter Zurückweisung der weitergehenden Berufung teilweise abgeändert.

Die Beklagte wird verurteilt, an die Klagepartei immateriellen Schadensersatz in Höhe von 100,00 € nebst Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz seit dem 03.06.2023 zu zahlen.

Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klagepartei künftige materielle und künftige derzeit noch nicht vorhersehbare immaterielle Schäden zu ersetzen, die der Klagepartei durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussagen der Beklagten im Jahr 2019 erfolgte, entstehen

Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten in Höhe von 90,96 € gegenüber der BRR Automotive Rechtsanwaltsgesellschaft mbH freizustellen.

Die weitergehende Klage wird abgewiesen.

© 2026 Wolters Kluwer Deutschland GmbH

Die Kosten des Rechtsstreits erster Instanz und zweiter Instanz tragen die Klagepartei zu 90 % und die Beklagte zu 10 %.

Dieses Urteil und (im Umfang der Zurückweisung der Berufung) das angefochtene Urteil sind ohne Sicherheitsleistung vorläufig vollstreckbar.

Die Revision wird nicht zugelassen.

Streitwert der Berufung: Wertstufe bis 4.000,00 EUR

Gründe

I.

Die Parteien streiten vor dem Hintergrund eines sogenannten Scraping-Vorfalls über Verstöße der Beklagten gegen die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG; im Folgenden: DSGVO) und daran anknüpfend über von der Klagepartei geltend gemachte Ansprüche auf Schadensersatz, Unterlassung und Auskunft.

Die Beklagte mit Sitz in Irland betreibt das soziale Online-Netzwerk F., über das dessen Nutzer untereinander kommunizieren können. Die Klagepartei unterhält seit dem Jahr 2008 bei der Beklagten ein Nutzerkonto, für welches sie persönliche Daten eingestellt hatte. Dazu gehörten die für die Registrierung erforderliche und für alle Nutzer stets öffentlich einsehbare Angabe ihres Namens, Geschlechts und der ihr zugewiesenen Nutzer-ID.

Neben den immer einsehbaren Pflichtangaben können die Nutzer in ihrem Profil weitere Daten zu ihrer Person angeben und innerhalb des von der Beklagten dazu vorgegebenen Rahmens auch darüber entscheiden, welche anderen Gruppen von Nutzern auf diese Daten zugreifen können. War die Suchbarkeits-Einstellung eines Nutzers - wie bei der Klagepartei - im Hinblick auf die Telefonnummer entsprechend der Voreinstellung durch die Beklagte auf "alle" gestellt, erlaubte es die sogenannte Kontakt-Import-Funktion bis September 2019 jedem F.-Nutzer, das Profil eines anderen Nutzers mithilfe der von diesem hinterlegten Telefonnummer zu finden. Mutmaßlich durch Eingabe einer Vielzahl von automatisch erzeugten Telefonnummern und unter Ausnutzung der Kontakt-Import-Funktion ist es unbekannten Dritten gelungen, Telefonnummern zu Nutzerkonten zuzuordnen und Daten der betreffenden Nutzer abzuschöpfen (sog. "Scraping"). Die auf diese Weise erlangten und mit einer Telefonnummer verknüpften Daten von ca. 533 Mio. F.-Nutzern aus 106 Ländern sind im April 2021 im Internet öffentlich verbreitet worden, darunter auch persönliche Daten der Klagepartei.

Die Klagepartei, die von Verstößen der Beklagten gegen die Datenschutz-Grundverordnung ausgeht, verlangt von dieser Schadensersatz, Unterlassung und Auskunft sowie die Erstattung vorgerichtlicher Rechtsanwaltskosten.

Hinsichtlich der weiteren Einzelheiten des Sach- und Streitstands erster Instanz, der dort gestellten Anträge sowie der rechtlichen Erwägungen des Landgerichts, welches die Klage vollständig abgewiesen hat, wird auf den Tatbestand und die Entscheidungsgründe des angefochtenen Urteils vom 20.03.2024 verwiesen.

Gegen dieses ihren Prozessbevollmächtigten am 26.03.2024 zugestellte Urteil hat die Klägerseite mit am 24.04.2024 bei Gericht eingegangenem Anwaltsschriftsatz Berufung einlegen und diese nach Verlängerung der Berufungsbegründungsfrist bis zum 27.06.2024 mit einem am 11.06.2024 bei Gericht eingegangenen Anwaltsschriftsatz begründen lassen.

Die Klägerseite verfolgt ihr erstinstanzliches Klageziel mit einem reduzierten Zahlungsantrag sowie einem teilweise geänderten Unterlassungsantrag weiter, wobei der Auskunftsantrag für erledigt erklärt worden ist, und trägt zur Begründung vor:

Das Landgericht habe verkannt, dass die Klage in vollem Umfang zulässig sei. Das Feststellungsinteresse nach § 256 Abs. 1 ZPO liege vor. Die Klägerseite habe hinreichend dargelegt, dass sie durch Versäumnisse der Beklagten in ihrem Recht auf informationelle Selbstbestimmung verletzt worden sei. Es sei wahrscheinlich, dass durch die Veröffentlichung der Daten der Klagepartei diese an einen kriminellen Dritten gerieten.

Die Unterlassungsanträge seien hinreichend bestimmt. Die abstrakt gehaltenen Bestandteile "unübersichtlich" und "unvollständig" seien im Antrag näher konkretisiert worden.

Unzutreffend sei auch die Annahme des Landgerichts, dass der Klageantrag zu Ziff. 3a im Schwerpunkt auf ein aktives Tun abziele. Denn die Klagepartei fordere von der Beklagten, künftige Kontaktimportfunktionen nur im Einklang mit den einzuhaltenden Sicherheitsvorkehrungen "freizuschalten", um Zugriffe unbefugter Dritter von vornherein zu verhindern.

Darüber hinaus sei die Klage auch begründet. Die Beklagte habe gegen die Datenschutz-Grundverordnung verstoßen, weil sie Daten der Klägerseite, namentlich ihre Telefonnummer, ohne ihre Einwilligung verarbeitet habe. Es habe keine wirksame

© 2026 Wolters Kluwer Deutschland GmbH

Einwilligung nach Art. 6 Abs. 1a DSGVO in die Nutzung ihrer nicht öffentlich geteilten Mobilfunknummer für die Auffindbarkeit durch Dritte vorgelegen. In Betracht komme nur ein voreingestelltes "Einverständnis" im Profil der Klagepartei. Eine solche Opt-Out-Möglichkeit genüge jedoch nicht für eine wirksame Einwilligung. Auch sei die Funktion der Suchbarkeit des Profils durch Dritte anhand der Mobilfunknummer nicht für die Erfüllung des zwischen den Parteien geschlossenen Vertrags erforderlich gewesen. Nach Art. 24 DSGVO sei für den für die Verarbeitung personenbezogener Daten Verantwortlichen, d. h. die Beklagte, eine allgemeine Verpflichtung dahin vorgesehen, dass diese die geeigneten technischen und organisatorischen Maßnahmen umzusetzen habe, um sicherzustellen und nachweisen zu können, dass die Verarbeitung gemäß den in der Datenschutz-Grundverordnung geregelten Pflichten erfolge. In diesem Zusammenhang lege Art. 32 DSGVO die Pflichten des Verantwortlichen fest. Artt. 24 und 32 DSGVO seien nach dem Europäischen Gerichtshof so auszulegen, dass "eine unbefugte Offenlegung von bzw. ein unbefugter Zugang zu personenbezogenen Daten durch einen Dritten" per se "für die Schlussfolgerung (nicht) ausreicht, dass die von dem für die betreffende Verarbeitung Verantwortlichen ergriffenen Maßnahmen nicht im Sinne dieser Bestimmungen geeignet waren, ohne dass ihm die Möglichkeit eingeräumt wird, den Gegenbeweis zu erbringen". Dieses hohe Schutzniveau habe die Beklagte nicht gewährleistet. Schließlich habe die Beklagte gegen die Verpflichtung zur Vornahme datenschutzfreundlicher Voreinstellungen nach Art. 25 Abs. 2 DSGVO verstoßen.

Das Landgericht verkenne, dass der Klägerseite ein ersatzfähiger immaterieller Schaden entstanden sei, der einen Schadensersatzanspruch in Höhe von mindestens 1.000,00 € begründe. Die Klagepartei habe das Vorliegen eines immateriellen Schadens hinreichend dargelegt und bewiesen. Es sei ihr Recht auf informationelle Selbstbestimmung verletzt worden, indem die Daten der Klagepartei, insbesondere ihre auf der Plattform der Beklagten nicht öffentlich einsehbare Mobilfunknummer, im Internet veröffentlicht worden seien. Die Klagepartei habe einen erheblichen Kontrollverlust über ihre Daten erlitten. Ob die Verletzung erheblich sei, sei aber nicht einmal von Relevanz.

Im Ergebnis bedürfe es deshalb keiner weiteren persönlichen Schilderungen des Erlebens der Klägerseite. Dennoch habe die Klagepartei zusätzlich ausgeführt, aufgrund des Scraping-Vorfalls unter Ängsten und Sorgen zu leiden. Sie empfinde beim Öffnen von SMS und E-Mails große Sorge und habe Angst davor, Opfer von Identitätsdiebstählen zu werden. Dass die Klagepartei einen Missbrauch durch Dritte befürchte, stelle einen "immateriellen Schaden" im Sinne von Art. 82 Abs. 1 DSGVO dar.

Die Umstände des Einzelfalls rechtfertigten die Zuerkennung eines Schadensersatzanspruchs in Höhe von mindestens 1.000,00 €. Dabei sei zu berücksichtigen, dass die Beklagte schon im Jahre 2017, also etwa zwei Jahre vor dem unbefugten Zugriff durch Dritte, vor einer Sicherheitslücke im Zusammenhang mit dem Kontakt-Import-Tool gewarnt worden sei. Trotzdem habe es die Beklagte versäumt, geeignete Schutzmaßnahmen zu ergreifen. Dieses Verhalten sei im Sinne der Datenschutz-Grundverordnung mindestens als grob fahrlässig anzusehen.

Die rechtswidrige Verarbeitung der Telefonnummer der Klagepartei sowie die Verstöße gegen Artt. 25 Abs. 2, 32 DSGVO seien für den eingetretenen Schaden kausal.

Der Klägerseite stehe auch ein Anspruch auf Feststellung der Ersatzpflicht für künftig eintretende Schäden zu. Die für eine solche Feststellung erforderliche Möglichkeit künftiger Schäden liege vor.

Auch der geltend gemachte Unterlassungsanspruch stehe der Klägerseite zu. Dieser folge insbesondere aus § 1004 Abs. 1 S. 2 BGB analog i. V. m. § 823 Abs. 1 BGB, § 823 Abs. 2 BGB i. V. m. Art. 6 Abs. 1 DSGVO sowie unmittelbar aus Art. 17 DSGVO. Schließlich sei auch der geltend gemachte Auskunftsanspruch aus Art. 15 Abs. 1 DSGVO gegeben. Das Auskunftsverlangen sei von der Klagepartei dahingehend präzisiert worden, dass ausschließlich Auskunft darüber erteilt werden solle, welche die Klagepartei betreffenden personenbezogenen Daten durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahre 2019 erfolgt sei, durch den Dritten hätten erlangt werden können. Dieser Auskunftsanspruch sei zunächst nicht erfüllt worden. Die von der Beklagten übersandten Informationen bezögen sich insbesondere nicht individuell auf das erklärte Auskunftsbegehren.

Nach Umstellung des Antrags zu Ziff. 3a und Erklärung des ursprünglichen Auskunftsantrags zu Ziff. 4 für erledigt beantragt die Klagepartei zuletzt:

1. Die Beklagte wird verurteilt, an die Klagepartei immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, der aber mindestens 1.000,00 Euro beträgt, nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 03.06.2023 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klagepartei künftige materielle und künftige derzeit noch nicht vorhersehbare immaterielle Schäden zu ersetzen, die der Klagepartei durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussagen der Beklagten im Jahr 2019 erfolgte, entstehen.

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht

© 2026 Wolters Kluwer Deutschland GmbH

festzusetzenden Ordnungsgeldes bis zu 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. eine Verarbeitung personenbezogener Daten des Klägers, namentlich Telefonnummer, F.-ID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt und Beziehungsstatus, über die Eingabe der Telefonnummer des Klägers in das Kontakt-Import-Tool und die darüber hergestellte Verknüpfung der eingegebenen Telefonnummer mit weiteren öffentlichen personenbezogenen Daten des Nutzerprofils des Klägers zu ermöglichen, ohne dass die Beklagten 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,

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

4. Der Antrag zu 4. wird für erledigt erklärt.

5. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten in Höhe von 1.134,55 EURO gegenüber der BRR Automotive Rechtsanwaltsgesellschaft mbH freizustellen.

Die Beklagte schließt sich der Erledigungserklärung an und beantragt im Übrigen,

die Berufung als unzulässig zu verwerfen, jedenfalls aber vollumfänglich zurückzuweisen.

Sie verteidigt die erstinstanzliche Entscheidung und erwidert:

Das Landgericht habe die Klage zu Recht abgewiesen. Die angeblichen Verstöße seien nicht vom Schutzbereich des Art. 82 DSGVO erfasst, sofern es nicht ohnehin an einem Verstoß fehle.

Die Informations- oder Transparenzpflicht nach Artt. 5 Abs. 1 lit. a, 13, 14 DSGVO sei nicht verletzt.

Auch sei keine Einwilligung im Sinne von Art. 6 Abs. 1 S. 1 lit. a DSGVO erforderlich. Die Verarbeitung personenbezogener Daten zur Bereitstellung der F.-Plattform und auch die hiermit verbundene Verarbeitung im Zusammenhang mit der Kontakt-Import-Funktion stütze sich auf keine Einwilligung, sondern auf die Durchführung des jeweiligen Nutzervertrags, mithin auf Art. 6 Abs. 1 S. 1 lit. b DSGVO. Der zwischen den Parteien geschlossene Nutzervertrag beziehe sich auf die Bereitstellung der F.Plattform als soziales Netzwerk. Einem solchen sozialen Netzwerk sei es immanent, dass die einzelnen Nutzer Freunde und generell ihnen bekannte Personen finden und sich miteinander vernetzen könnten. Solche Verknüpfungen würden durch die Verwendung von Funktionen wie der Kontakt-Import-Funktion hergestellt, die, wie im auch Hilfebereich und in der Datenrichtlinie erläutert, die Telefonnummern von Nutzern erforderten.

Die Pflicht zur Implementierung angemessener technischer und organisatorischer Maßnahmen gemäß Artt. 5 Abs. 1 lit. f, 24, 32 DSGVO sei ebenfalls nicht verletzt. Die Beklagte sei nicht verpflichtet gewesen, Schutzmaßnahmen zu ergreifen, um die Erhebung von Informationen zu verhindern, die der Nutzer öffentlich gemacht habe. Die genannte Verpflichtung ziele insbesondere darauf ab, eine *unbefugte* Offenlegung von Daten zu verhindern. Im Zuge des Scraping-Sachverhalts sei jedoch keine unbefugte Offenlegung von Daten erfolgt. Bei den in diesem Rahmen abgerufenen Daten von der F.-Plattform handele es sich entweder um immer öffentliche Nutzerinformationen oder um Daten, die in dem F.-Profil der Klagepartei entsprechend der jeweiligen Zielgruppenauswahl öffentlich einsehbar gewesen seien.

Auch eine Verletzung der Meldepflicht aus Art. 33 DSGVO liege nicht vor. Ebenso wenig habe die Beklagte gegen die Benachrichtigungspflicht gemäß Art. 34 DSGVO verstoßen. Es habe keine "Verletzung des Schutzes personenbezogener Daten" vorgelegen, so dass auch keine Verpflichtung aus Art. 34 DSGVO bestanden habe.

© 2026 Wolters Kluwer Deutschland GmbH

Schließlich liege auch keine Verletzung der Pflicht zum Datenschutz durch Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen nach Art. 25 DSGVO vor. Was die öffentliche Einsehbarkeit einzelner Informationen betreffe, verkenne die Klägerseite, dass nur die Datenpunkte Nutzer-ID, Vor- und Nachnahme sowie Geschlecht vom F.-Profil abgerufen worden und in den durch Scraping abgerufenen Daten enthalten gewesen seien. Eine relevante Pflichtverletzung komme insofern nicht in Betracht. Die öffentliche Einsehbarkeit sei erforderlich gewesen, damit Nutzer leichter mit anderen Nutzern auf der F.-Plattform hätten in Kontakt treten können.

Auch liege keine Verletzung von Art. 25 DSGVO in Bezug auf die Standardeinstellung für die Suchbarkeit der Telefonnummer vor. Die Nutzung der Telefonnummer des Nutzers im Rahmen der Suchfunktion diene dem Unternehmenszweck der Beklagten, Menschen miteinander zu verbinden. Der F.-Dienst habe weltweit ca. 2,8 Milliarden Nutzer, so dass eine Suchbarkeit allein anhand des Namens in der Regel nicht ausreiche, um denjenigen Nutzer zu identifizieren, den der suchende Nutzer finden wolle. Um die Suchbarkeit auf der F.-Plattform nach der Telefonnummer oder der EMail-Adresse zu ändern, könne die Klagepartei jederzeit entsprechende Änderungen ihrer Suchtbarkeitseinstellungen vornehmen. Es sei deshalb angemessen gewesen, die Nutzer durch die Einstellung "alle" suchbar zu machen und ihnen gleichzeitig die Möglichkeit zum Eingreifen über ihre Suchbarkeitseinstellungen zu geben.

In Bezug auf die Telefonnummer sei ohnehin davon auszugehen, dass diese nicht von der F.-Plattform abgerufen, sondern von den Scrapern im Rahmen der Telefonnummernaufzählung bereitgestellt worden sei. Insofern könne nicht von einem "Zugänglichmachen" solcher Daten durch die Beklagte ausgegangen werden, da die Scraper zufällig generierte Telefonnummern eingegeben haben müssten, um auf der F.-Plattform nach Nutzern suchen zu können.

Den von der Klagepartei geltend gemachten Auskunftsanspruch nach Art. 15 Abs. 1 DSGVO habe die Beklagte vollständig erfüllt, und zwar mit dem als Anlage B17 vorgelegten Schreiben. Soweit die Klagepartei Auskunft über die Scraper verlange, sei die Auskunftserteilung nicht möglich.

Jedenfalls treffe die Beklagte kein Verschulden nach Art. 82 Abs. 3 DSGVO. Denn die Beklagte sei für den Scraping-Sachverhalt, durch den der vermeintliche Schaden eingetreten sei, in keinerlei Weise verantwortlich.

Die Klägerseite habe auch keinen immateriellen Schaden im Sinne von Art. 82 DSGVO erlitten. Sie habe keine kompensationsfähige Beeinträchtigung dargelegt; ein angeblicher Kontrollverlust über Daten sei für die Begründung eines immateriellen Schadens nicht ausreichend. Insbesondere könne ein immaterieller Schaden nicht in den behaupteten Spam-Anrufen und -Nachrichten gesehen werden. Dabei handele es sich nur um Alltagserscheinungen und bloße Unannehmlichkeiten. Die erneute Veröffentlichung der Daten im Rahmen des Scraping-Sachverhalts könne zudem keinen Kontrollverlust begründen. Sofern die Klägerseite meine, dass es unerheblich sei, dass der Name, das Geschlecht und die F.-ID als sogenannte immer öffentliche Nutzerinformationen öffentlich sichtbar gewesen seien, da jedenfalls die Verknüpfung mit ihrer Telefonnummer nicht hergestellt gewesen sei, verkenne die Klagepartei, dass die klägerseits akzeptierten Suchbarkeitseinstellungen darüber entschieden, wer das Profil suchen könne, und diese Verknüpfungsmöglichkeit dadurch hergestellt worden sei, dass die Klagepartei im relevanten Zeitraum ihre Suchbarkeitseinstellungen auf "alle" gestellt habe.

Auch bestehe keine Kausalität zwischen den angeblichen Pflichtverletzungen und dem behaupteten Schaden der Klagepartei. Dies gelte auch für einen angeblichen Verstoß gegen Art. 32 DSGVO. Die Öffentlichkeit bestimmter personenbezogener Daten der Klägerseite habe nicht auf einer fehlenden Absicherung der Systeme der Beklagten beruht, sondern auf der Tatsache, dass es sich dabei um immer öffentlich einsehbare Datenpunkte gehandelt habe.

In Bezug auf angebliche Spam-Nachrichten und -Anrufe habe die Klagepartei weder substantiiert dargelegt noch bewiesen, dass sie auf den Scraping-Sachverhalt zurückgingen. Es sei wahrscheinlich, dass die angeblichen Nachrichten und Anrufe auf anderen Umständen beruhten und in keinem kausalen Zusammenhang mit dem streitgegenständlichen Vorfall stünden.

Letztendlich sei die Schadensbemessung durch die Klagepartei offensichtlich rechtsfehlerhaft. Ein Schaden sei allenfalls im symbolischen Bereich denkbar.

Die Unterlassungsanträge seien bereits unzulässig, zumindest aber unbegründet. Eine Wiederholungsgefahr bestehe nicht. Als Teil der Bemühungen zur Verringerung des Scraping-Risikos habe die Beklagte insbesondere die Kontakt-Import-Funktion dahingehend modifiziert, dass keine direkten Kontaktübereinstimmungen mehr angezeigt würden. Folglich sei es Dritten nicht mehr möglich, mittels dieser Funktion Telefonnummern mit bestimmten F.-Nutzern zu verknüpfen. Die Suchbarkeit von Nutzern anhand ihrer Telefonnummer sei von der Beklagten in der F.-Suchfunktion abgeschaltet worden.

II.

Die zulässige Berufung der Klagepartei (§§ 511 Abs. 1 u. Abs. 2 Nr. 1, 517, 519 f. ZPO) ist teilweise begründet.

I. Berufungsantrag zu Ziff. 1

© 2026 Wolters Kluwer Deutschland GmbH

Die Klagepartei kann von der Beklagten nach Art. 82 Abs. 1 DSGVO Ersatz ihres immateriellen Schadens in Höhe von 100,00 € wegen des bei ihr durch den Scraping-Vorfall eingetretenen Kontrollverlusts verlangen; ein weitergehender Anspruch besteht nicht.

1. Die Klage ist insoweit zulässig.

Die Klagepartei hat ihren gewöhnlichen Aufenthalt in der Bundesrepublik Deutschland, so dass die - auch unter der Geltung von § 513 Abs. 2 ZPO zu prüfende (vgl. z. B. BGH, Urteil vom 17.03.2025 - VI ZR 11/14, NJW-RR 2015, 941

[BGH 17.03.2015 - VI ZR 11/14] Rn. 14) - internationale Zuständigkeit deutscher Gerichte aus Art. 82 Abs. 6 i. V. m. Art. 79 Abs. 2 S. 2 DSGVO folgt.
a) Der Anwendungsbereich der Datenschutz-Grundverordnung ist in räumlicher (Art. 3 Abs. 1 DSGVO) und auch sachlicher Hinsicht (Art. 2 Abs. 1 DSGVO) eröffnet. Die bei der in der Europäischen Union (Irland) ansässigen Beklagten gespeicherten Daten der Klagepartei wie Name, Geschlecht, Nutzer-ID und Telefonnummer stellen personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO dar.

b) Auch der zeitliche Anwendungsbereich ist eröffnet (Art. 99 Abs. 2 DSGVO).

aa) Maßgeblich ist der Zeitpunkt des in Streit stehenden Scraping-Vorfalls (vgl.

BGH, Urteil vom 18.11.2024 - VI ZR 10/24, GRUR-RS 2024, 31967 Rn. 19). Der Scraping-Vorfall ist nach dem Vortrag der Klägerseite und auch nach dem von der Beklagten veröffentlichten Artikel vom 06.04.2021 (Anlage B 10) im Jahr 2019 zu verorten, wo es ausdrücklich heißt, man sei zuversichtlich, dass das Problem, welches das Scrapen der Daten im Jahr 2019 ermöglicht habe, nicht mehr bestehe, und dass böswillige Akteure die in Rede stehende Funktion im Jahr 2019 genutzt hätten. Dies genügt nach teilweise vertretener Ansicht bereits, um davon auszugehen zu können, dass die personenbezogenen Daten der Klagepartei im Jahr 2019 abgeschöpft wurden (vgl. z. B. OLG Celle, Urteil vom 05.03.2025 - 5 U 129/24, juris Rn. 8 ff., OLG Oldenburg, Urteil vom 21.05.2024 - 13 U 100/23, BeckRS 2024,12013 Rn. 9).
bb) Das prozessuale Bestreiten der Beklagten mit Nichtwissen ist unbeachtlich. Es steht ncht nur im Widerspruch zu ihren außerprozessual gemachten Angaben, sondern ist darüber hinaus gemäß § 138 Abs. 4 ZPO unzulässig, wonach eine Erklärung mit Nichtwissen nur über solche Tatsachen zulässig ist, die weder eigene Handlungen der Partei noch Gegenstand ihrer eigenen Wahrnehmung gewesen sind. Fehlt es an einer eigenen Wahrnehmung, kommt eine Informationspflicht der Partei in Betracht und können Vorgänge im eigenen Geschäfts- oder Verantwortungsbereich der Partei ihren eigenen Handlungen oder Wahrnehmungen gleich zu achten sein (vgl.

BGH, Urteil vom 15.11.1989 - VIII ZR 46/89, NJW 1990, 453 (454); von Selle in: BeckOK ZPO, Vorwerk/Wolf, 56. Edition, § 138 Rn. 26).
So liegen die Dinge hier. Das Scraping stellt einen Vorgang im Verantwortungsbereich der Beklagten dar, über den sie sich die nötigen Informationen zu beschaffen und sich im Prozess zu erklären hat. Erfolgte das Scraping nicht unter dem Normenregime der DSGVO, also vor ihrem Inkrafttreten, hat eine Negativerklärung dahingehend zu erfolgen, dass es jedenfalls seit dem 25.05.2018 nicht zu dem streitgegenständlichen Scrapingvorfall gekommen ist.

Soweit sich die Beklagte darauf zurückzuziehen sucht, hierzu nicht in der Lage zu sein, unter anderem weil sie sich nicht im Besitz der Rohdaten befinde, welche die durch Scraping abgerufenen Daten enthielten, kann sie damit nicht gehört werden. Die Berufung auf eine fehlende Informationsmöglichkeit entlastet nicht stets und unter anderem dann nicht, wenn sie von der Partei vereitelt wird (vgl. z. B. Lange, NJW 1990, 3233 (3239)). Ähnliches gilt hier, was aus der Wertung des Art. 5 Abs. 2 DSGVO folgt, der dem Verantwortlichen eine Rechenschaftspflicht auferlegt. Den Verantwortlichen trifft nicht nur die Verantwortung für die Einhaltung der Grundsätze von Art. 5 Abs. 1 DSGVO; er muss ihre Einhaltung auch nachweisen können. Diese Nachweispflicht kann er nur durch eine entsprechende Dokumentation oder ein Daten-Managementsystem erfüllen (vgl. Schantz in: BeckOK Datenschutzrecht, Wolff/ Brink/v. Ungern-Sternberg, 51. Edition, Art. 5 Rn. 39). Eine Konkretisierung der Nachweispflicht enthält Art. 30 DSGVO; danach muss der Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten führen. Neben diesen konkreten Verpflichtungen ist je nach Einzelfall eine weitere Dokumentation erforderlich. Die Rechenschaftspflicht führt damit zu umfangreichen zusätzlichen Dokumentations- und Nachweispflichten (Pötters in: Gola/Heckmann/Pötters, DSGVO, 3. Aufl. 2022, Art. 5 Rn. 34).

Generell trägt der Verantwortliche nach Art. 5 Abs. 2 DSGVO die Darlegungs- und Beweislast dafür, dass die Daten unter anderem für festgelegte, eindeutige und legitime Zwecke erhoben und auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (EuGH (Große Kammer),

Urteil vom 04.07.2023 - C-252/21, GRUR 2023, 1131 [BGH 25.10.2022 - VI ZR 258/21] Rn. 95 - Meta Platforms Inc. ua/ Bundeskartellamt). Insofern bedeutet das Fehlen von Nachweismöglichkeiten eine Verletzung der Nachweispflicht nach Abs. 2 (Roßnagel in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 5 Rn. 186). Selbst wenn man annimmt, die Nachweispflicht gehe im allgemeinen nicht so weit, dass der Nachweis über die Einhaltung der Grundsätze bei jeder einzelnen Verarbeitung im Sinne einer Protokollierung aller Verarbeitungsvorgänge geführt werden müsse (so Herbst in: Kühling/Buchner/ Herbst, DSGVO, 4. Aufl. 2024, Art. 5 Rn. 80), hat die Beklagte dennoch in der Lage zu sein, darüber Auskunft zu geben, ob unter

© 2026 Wolters Kluwer Deutschland GmbH

der Geltung der DSGVO eine mehr als 500-millionenfache Verarbeitung von Daten im oben beschriebenen Sinne aus Anlass einer automatisiert durchgeführten, randomisierten Telefonnummerneingabe durch unbekannte und unautorisierte Dritte stattgefunden hat. Daraus folgt die Unzulässigkeit eines Bestreitens mit Nichtwissen, welches mit einer eine Verletzung der Nachweispflicht darstellenden mangelnden Kenntnis einer etwaig stattgefundenen Datenverarbeitung begründet wird.
2. Der Antrag auf Zahlung immateriellen Schadensersatzes ist in der Sache teilweise begründet.

a) Nach der Rechtsprechung des Europäischen Gerichtshofs erfordert ein Schadensersatzanspruch im Sinne von Art. 82 Abs. 1 DSGVO 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 erfüllt sein müssen (vgl. z. B.

EuGH, Urteil vom 04.10.2024 - C-507/23, juris Rn. 24). Die Darlegungs- und Beweislast für diese Voraussetzungen trifft den Gläubiger, also die Person, die auf der Grundlage von Art. 82 Abs. 1 DSGVO den Ersatz eines Schadens verlangt (vgl. z. B. EuGH, Urteil vom 11.04.2024 - C-741/21, NJW 2024, 15161 Rn. 35).
b) Dahinstehen kann, ob ein Verstoß gegen die Datenschutz-Grundverordnung im Sinne von Art. 82 Abs. 1 DSGVO nur die unrechtmäßige Verarbeitung von personenbezogenen Daten erfasst oder auch bloße Verstöße gegen abstrakte Pflichten des Verantwortlichen außerhalb eines konkreten Verarbeitungsvorgangs haftungsbegründend sein können. Denn wegen des umfassenden Verarbeitungsbegriffs des Art. 4 Nr. 2 DSGVO wäre auch bei einem engen Verständnis von Art. 82 Abs. 1 DSGVO in Bezug auf den hier streitgegenständlichen Scraping-Vorfall 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, GRUR-RS 2024, 31967 Rn. 23).
c) Die Datenverarbeitung der Beklagten mit Blick auf die Suchbarkeit des Nutzerprofils über die Mobilfunknummer der Klagepartei und die in diesem Zusammenhang von der Beklagten vorgenommene Voreinstellung der Suchtbarkeitseinstellungen auf "alle" entsprach nicht dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. b und c, Art. 25 Abs. 2 S. 1 u. 3 DSGVO).

Der Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO verlangt, dass die Datenverarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt ist. Nach dem diesen Grundsatz konkretisierenden Art. 25 Abs. 2 DSGVO hat der Verantwortliche 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. 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 DSGVO 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 (vgl. BGH, Urteil vom 18.11.2024, a. a. O., Rn. 88).

Diesen Anforderungen wurde die standardmäßige Voreinstellung der Beklagten zum Zeitpunkt des Scraping-Vorfalls nicht gerecht, die für die Suchbarkeit eines Nutzerprofils über die Telefonnummer vorsah, dass "alle" anderen F.-Nutzer eine entsprechende Rufnummernsuche durchführen können, womit ihnen gleichzeitig die immer öffentlichen weiteren Profildaten zugänglich gemacht wurden (ebenso z. B.

OLG Dresden, Urteil vom 10.12.2024 - 4 U 808/24, GRUR-RS 2024, 35688 Rn. 7).
d) Entgegen der Auffassung der Beklagten war diese Form der Datenverarbeitung nicht rechtmäßig.

aa) Insbesondere war sie nicht im Sinne von Art. 6 Abs. 1 Unterabs. 1 lit. b bis f DSGVO erforderlich und deshalb rechtmäßig (die Erforderlichkeit ebenfalls verneinend: BGH, Urteil vom 18.11.2024, a. a. O., Rn. 91).

(1) Die Beklagte meint zu Unrecht, die Suchbarkeit des Nutzerprofils der Klägerseite anhand deren Mobilfunknummer sei für die Erfüllung des Hauptzwecks des mit der Klagepartei geschlossene Nutzungsvertrags, die gegenseitige Auffindbarkeit der Nutzer untereinander zwecks Vernetzung miteinander zu ermöglichen, erforderlich gewesen. Die Verarbeitung personenbezogener Daten ist zur Erfüllung eines Vertrags 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 dafür 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 (vgl.

EuGH, Urteil vom 04.07.2023 - C-252/21, GRUR 2023, 1131 [BGH 25.10.2022 - VI ZR 258/21] Rn. 98 f., 125 - Meta Platforms Inc. u. a./Bundeskartellamt).
(2) Nach Maßgabe dieser Grundsätze war die Suchbarkeit des Nutzerprofils der Klägerseite anhand deren Mobilfunknummer nicht erforderlich im Sinne von Art. 6 Abs. 1 S. 1 lit. b DSGVO (ebenso

© 2026 Wolters Kluwer Deutschland GmbH

OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23, GRUR 2023, 1791 Rn. 93 ff.).
Da sich die Nutzer gegenseitig auch über ihre Namen finden können, ist die Suchbarkeit der Nutzerprofile anhand der Mobilfunknummer zur Erfüllung des von der Beklagten angeführten Hauptzwecks des Nutzervertrags, nämlich der gegenseitigen Auffindbarkeit zwecks Vernetzung, nicht unerlässlich. Gerade zu diesem Zweck ist der Name der Nutzer auch stets öffentlich einsehbar. Auch soweit die Beklagte vor dem Hintergrund der weltweit ca. 2,8 Milliarden Nutzer auf die höhere Trefferwahrscheinlichkeit einer Suche anhand der Telefonnummer verweist, folgt daraus nicht die Erforderlichkeit der Suchbarkeit von Nutzerprofilen anhand der Telefonnummer für unbekannte Dritte. Andernfalls wäre auch nicht nachvollziehbar, dass die Telefonnummer nicht zu den Pflichtangaben zählt, die im Rahmen der Erstanmeldung zwingend anzugeben sind, die Nutzer die standardmäßige Voreinstellung der Suchbarkeit ihres Nutzerprofils anhand ihrer Telefonnummer auf "alle" abwählen können und die Beklagte die Suchmöglichkeit von Nutzern anhand der Telefonnummer in der Suchfunktion zum 06.09.2019 zur Unterbindung des Scraping deaktiviert hat (vgl. OLG Oldenburg, Urteil vom 21.05.2024, - 13 U 100/23, BeckRS 2024, 12013 Rn. 21; OLG Hamm, Urteil vom 15.08.2023, a. a. O., Rn. 98).

bb) Andere Rechtsgrundlagen für die von ihr gewählte Voreinstellung und die Suchbarkeit des Nutzerprofils der Klagepartei anhand deren Mobilfunknummer für "alle" führt die Beklagte nicht an. Insbesondere beruft sie sich ausdrücklich auch nicht auf Art. 6 Abs. 1 Unterabs. 1 lit. a DSGVO, wonach die Datenverarbeitung rechtmäßig ist, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat. Eine wirksame Einwilligung der Klagepartei in die Verwendbarkeit ihrer Telefonnummer im Rahmen der Suchbarkeitsfunktion liegt auch nicht vor.

(1) Nach der Legaldefinition von Art. 4 Nr. 11 DSGVO stellt eine "Einwilligung" der betroffenen Person eine freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung dar, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Die Einwilligung muss sich also auf die konkrete Datenverarbeitung beziehen und zudem auf einem transparenten Ersuchen beruhen, das gemäß Art. 7 Abs. 2 DSGVO in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache erfolgt ist (vgl. a. BGH, Urteil vom 18.11.2024, a. a. O., Rn. 44). Die Darlegungs- und Beweislast für die Einwilligung des Betroffenen trägt nach Art. 7 Abs. 1 DSGVO der für die Datenverarbeitung Verantwortliche (vgl. EuGH, Urteil vom 04.07.2023, a. a. O., Rn. 152).

(2) Im Streitfall hat die Beklagte nicht hinreichend dargelegt, dass die Klagepartei in die Suchbarkeit ihres Nutzerprofils anhand ihrer Mobilfunknummer wirksam eingewilligt hat.

(a) Dafür, dass die Klägerseite bereits im Zuge der Eröffnung ihres Nutzerkontos eine wirksame Einwilligung erklärt haben könnte, indem sie eine Zustimmung zu den damals geltenden Nutzungsbedingungen der Beklagten erklärt hat, ist nichts ersichtlich. Welche Nutzungsbedingungen damals galten und wie sie konkret in das Registrierungsverfahren eingebunden wurden, ist nicht dargetan. Demzufolge kann nicht geprüft werden, ob eine damals erklärte Einwilligung gemessen am Maßstab von Art. 6 Abs. 1 Unterabs. 1 lit. a DSGVO wirksam wäre (vgl. BGH, Urteil vom 18.11.2024, a. a. O., Rn. 43).

Jedenfalls nach der obergerichtlichen Rechtsprechung konnte eine von der Klägerseite möglicherweise vor dem 25.05.2018 in die Suchbarkeit ihres Profils über die Mobilfunknummer erteilte Einwilligung unter Geltung der Datenschutz-Grundverordnung ohnehin keine rechtfertigende Wirkung mehr entfalten. Denn nach Erwägungsgrund 171 S. 3 DSGVO habe eine vorab erteilte Einwilligung bereits den Bedingungen der Datenschutz-Grundverordnung entsprechen müssen, um fortzugelten. Daran fehle es jedoch, weil auch die der Klägerseite im April 2018 von der Beklagten mit Blick auf den Geltungsbeginn der Datenschutz-Grundverordnung zur Verfügung gestellten neuen Nutzungsbedingungen vom 19.04.2018 und die ebenfalls zur Verfügung gestellte neue Datenrichtlinie vom selben Tag den Anforderungen der Datenschutz-Grundverordnung nicht genügten (so OLG Hamm, Urteil vom 15.08.2023, a. a. O., Rn. 102; OLG Dresden, Urteil vom 10.12.2024, a. a. O., Rn. 10).

(b) Der Umstand als solcher, dass die Klagepartei die standardmäßige Voreinstellung der Suchbarkeitsfunktion (zunächst) nicht von "alle" auf "Freunde", "Freunde von Freunden" oder (ab Mai 2019) "nur ich" geändert hat, führt zu keiner Einwilligung. Eine in unmissverständlicher - nicht zwingend ausdrücklicher, wie der Umkehrschluss aus Art. 9 Abs. 2 lit. a DSGVO ergibt (vgl. Reimer in: Sydow/Marsch, DS-GVO/BDSG, 3. Aufl., Art. 6 DSGVO Rn. 18) - Weise abgegebene Einwilligung im Sinne von Art. 4 Nr. 11 DSGVO setzt ein aktives Verhalten des Einwilligenden voraus. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person begründen entsprechend Erwägungsgrund 32 S. 3 DSGVO keine Einwilligung mehr (vgl.

EuGH, Urteil vom 01.10.2019 - C-673/17, NJW 2019, 3433 Rn. 61 f. - Planet49; ders., Urteil vom 11.11.2020 - C-61/19, NJW 2021, 841 Rn. 35 f.). Von daher scheitert eine Einwilligung bereits daran, dass die Beklagte mit ihrer zur Suchbarkeit vorgenommenen Voreinstellung auf "alle" zum Zeitpunkt der Bedingungsänderungen am 19.04.2018 unverändert eine "Opt-Out-Einwilligung" vorsah (vgl. OLG Hamm, Urteil vom 15.08.2023, a. a. O., Rn. 104). Eine bloße Opt-out-Möglichkeit genügt den zu stellenden Anforderungen nicht mehr (vgl. Reimer, a. a. O., Rn. 18).
(c) Eine Einwilligung der Klägerseite ergibt sich auch nicht daraus, dass die Beklagte die Nutzer im April 2018 in Vorbereitung auf den Geltungsbeginn der Datenschutz-Grundverordnung zur Zustimmung zu den aktualisierten Nutzungsbedingungen vom 19.04.2018, zur Kenntnisnahme der aktualisierten Datenrichtlinie und zur Überprüfung der Dateneinstellungen aufgefordert hat.

© 2026 Wolters Kluwer Deutschland GmbH

Eine Einwilligung der Nutzer und damit auch der Klagepartei in die Suchbarkeit ihres Nutzerprofils anhand der Mobilfunknummer scheitert insofern daran, dass es an einer transparenten Information über die Suchbarkeit des Nutzerprofils anhand der Telefonnummer fehlt.

(aa) Im ersten Schritt des Bestätigungsverfahren ist der Nutzer entsprechend dem Screenshot auf Seite 32 der Duplik der Beklagten mit pauschalen Hinweisen zur Überprüfung seiner Dateneinstellungen aufgefordert worden. Nach einem Klick auf den Button "Los geht's" erschien entsprechend dem Screenshot auf Seite 33 der Duplik die Bitte, die aktualisierten Nutzungsbedingungen zu akzeptieren. Dort findet sich neben der Schaltfläche "Ich stimme zu" der Text: "Indem du auf "Ich stimme zu" klickst, akzeptierst du die aktualisierten Nutzungsbedingungen". Eine etwaige Einwilligungserklärung der Klägerseite durch Anklicken dieser Schaltfläche kann sich somit nur auf die aktualisierten Nutzungsbedingungen beziehen und nicht auf die verlinkten Inhalte der Datenrichtlinie sowie der Cookie-Richtlinie und auch nicht auf die bisherigen Einstellungen hinsichtlich der Daten, der Privatsphäre und der Sicherheit.

(bb) Die Nutzungsbedingungen vom 19.04.2018 (vgl. Anlage B 19) enthalten zum Datenschutz unter der Überschrift "2. Unsere Datenrichtlinie und deine Privatsphäre-Einstellungen" folgende Ausführungen: "Wir erfassen und verwenden deine personenbezogenen Daten, um die oben beschriebenen Dienste für dich bereitzustellen. In unserer Datenrichtlinie *(Anmerkung: diese ist verlinkt)* erfährst du, wie wir deine Daten erfassen und verwenden. Wir empfehlen dir außerdem, deine Privatsphäre-Einstellungen in deinen Einstellungen *(Anmerkung: diese ist verlinkt)* zu überprüfen. Diese legen die Art und Weise fest, wie wir Daten verwenden."

Eine transparente (Art. 7 Abs. 2 DSGVO) Information über die Suchbarkeit anhand der Telefonnummer, zumal bei einer Voreinstellung auf "alle", ist darin schon dem Wortlaut nach nicht enthalten.

(cc) Unabhängig davon, dass sich eine etwaige Zustimmung nach dem oben Gesagten nur auf die aktualisierten Nutzungsbedingungen und nicht auch auf die dort verlinkte Datenrichtlinie beziehen würde, ergibt sich solches auch nicht aus der Datenrichtlinie selbst. Denn unter der Überschrift "Wie werden diese Informationen geteilt?" wird lediglich die Zielgruppenauswahl erläutert (Anlage B 9, Seite 6).

(dd) Die ebenfalls verlinkten Privatsphäre-Einstellungen enthielten unter der Rubrik "So kann man dich finden und kontaktieren" zwar die Einstellung "Wer kann dich anhand der angegebenen Telefonnummer finden? alle" (vgl. Screenshot auf Seite 9 der Klageschrift; s. a. Screenshot auf S. 23 der Klageerwiderung). Dabei handelt es sich jedoch nicht um eine Information über die Suchbarkeit des Nutzerprofils anhand der Telefonnummer, sondern um die Einstellung der Suchbarkeitsfunktion als solche. Doch selbst wenn man dies ausreichen lassen wollte, begründete jedenfalls die Verlinkung der Privatsphäre-Einstellungen in den Nutzungsbedingungen keine transparente Information über die Suchbarkeit des Nutzerprofils anhand der Telefonnummer. Denn aus Sicht der Klägerseite bestand keine Notwendigkeit, der Empfehlung der Beklagten zur Überprüfung ihrer Privatsphäre-Einstellungen zu folgen. Nach Art. 25 Abs. 2 S. 1 DSGVO ist die Beklagte verpflichtet, Voreinstellungen für die Verarbeitung personenbezogener Daten so auszuwählen, dass nur die für die Zweckerreichung erforderlichen Daten verarbeitet werden. Mithin durfte die Klagepartei darauf vertrauen, dass die Beklagte die jeweils datenschutzfreundlichsten Voreinstellungen ausgewählt hatte. Da die Verarbeitung der Telefonnummer im Rahmen der Suchfunktion zur Erfüllung des Hauptzwecks des sozialen Netzwerks - wie ausgeführt - nicht erforderlich war, konnte die Klägerseite nach Art. 25 Abs. 2 S. 3 DSGVO berechtigter Weise davon ausgehen, dass die Beklagte geeignete Maßnahmen ergriffen hatte, um sicherzustellen, dass ihre Mobilfunknummer durch Voreinstellungen nicht ohne eigenes Zutun einer unbestimmten Zahl von Personen, sondern nur dem kleinstmöglichen Empfängerkreis zugänglich gemacht werden würde (so OLG Oldenburg, Urteil vom 21.05.2024 - a. a. O., Rn. 29).

(ee) Die Ausführungen der Beklagten zu einer Information der Nutzer im Hilfebereich und dort wiederum zur Verwendung der Mobilfunknummer (vgl. insbesondere Anlagen B 5 - 7) sind im Kontext einer von der Klägerseite erklärten Einwilligung in die Datenverarbeitung der Beklagten unbehelflich. Abgesehen davon, dass eine wirksame Einwilligung des Nutzers vor Beginn der Datenverarbeitung vorzuliegen hat, stehen die im Hilfebereich präsentierten Informationen, bei denen es dem Zufall überlassen bleibt, ob und wann sie der Nutzer zur Kenntnis nimmt, in keinem Zusammenhang zu einer für die Annahme einer Einwilligung erforderlichen, unmissverständlich abgegebenen Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen, bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

e) Das Verschulden der Beklagten wird nach Art. 82 DSGVO vermutet, weil sich der Verantwortliche gemäß Art. 82 Abs. 3 DSGVO zu exkulpieren hat. Eine Exkulpation ist der Beklagten nicht gelungen. Dass das Abschöpfen der Daten der Klägerseite in erster Linie auf das kriminelle Verhalten unbekannter Dritten zurückzuführen ist, vermag nichts daran zu ändern, dass die Beklagte mit der von ihr gewählten Voreinstellung und der von ihr durchgeführten Datenverarbeitung zumindest fahrlässig im Sinne von Art. 83 Abs. 2 S. 2 lit. b DSGVO gegen die ihr von der Datenschutz-Grundverordnung auferlegten Pflichten verstoßen hat.

f) Die Klägerseite hat einen immateriellen Schaden in Höhe von 100,00 € erlitten, den sie erstattet verlangen kann. Ein weitergehender Schadensersatzanspruch steht ihr nicht zu.

aa) Nach der Rechtsprechung des Europäischen Gerichtshofs ist Art. 82 Abs. 1 DSGVO dahin auszulegen, dass ein zeitlich

© 2026 Wolters Kluwer Deutschland GmbH

begrenzter Verlust der Kontrolle der betroffenen Person über ihre personenbezogenen Daten ausreichen kann, um einen "immateriellen Schaden" zu verursachen, sofern nachgewiesen wird, dass tatsächlich ein in dem Kontrollverlust bestehender Schaden - so geringfügig er auch sein mag - entstanden ist, ohne dass der Nachweis zusätzlicher spürbarer negativer Folgen erforderlich wäre (vgl.

EuGH, Urteil vom 04.10.2024 - C-200/23, juris Rn. 145, 156). Steht der Kontrollverlust also fest, stellt dieser selbst den immateriellen Schaden dar, ohne dass es sich daraus entwickelnder besonderer Befürchtungen oder Ängste der betroffenen Person bedarf (vgl. BGH, Urteil vom 18.11.2024, a. a. O. Rn. 31).
bb) Richtig ist, dass die Klagepartei ihre "gescrapten" Daten nicht im einzelnen dargestellt hat. Allerdings ist unstreitig, dass die Klagepartei von dem Scraping-Vorfall betroffen ist und die öffentlichen Daten abgeschöpft wurden. Demgemäß ist davon auszugehen, dass jedenfalls ihre Telefonnummer, verknüpft mit den sogenannten immer öffentlichen Daten (Name, User-ID, Geschlecht), im April 2021 im Internet öffentlich verbreitet wurde. Darin liegt zwangsläufig ein Verlust der Kontrolle der Klägerseite über diese sie betreffenden Daten.

(1) Dass hiernach nur die immer öffentlichen Nutzer-Informationen betroffen sind, schließt einen Kontrollverlust nicht aus. Zum einen waren auch diese Informationen nicht allgemein, sondern nur für F.-Nutzer zugänglich, die in der Lage waren, das F.Profil der Klagepartei und damit auch diese Informationen aufzufinden. Damit ist eine allgemein zugängliche Veröffentlichung der Daten im Internet weder qualitativ noch quantitativ vergleichbar. Zum anderen ergibt sich aus der Veröffentlichung im Internet gerade die dauerhafte Preisgabe der mit den Daten der Klagepartei verknüpften Telefonnummer, die den bei der Beklagten abgelegten Daten nicht zu entnehmen war.

(2) Dem Eintritt eines Kontrollverlusts steht auch nicht entgegen, dass die Klagepartei bereits vor der Veröffentlichung ihrer Daten infolge des Scraping-Vorfalls keine Kontrolle mehr über ihre personenbezogenen Daten gehabt hätte, etwa weil diese, verbunden mit ihrer Telefonnummer, bereits zuvor im Internet anderweitig veröffentlicht worden wären (vgl. BGH, Urteil vom 18.11.2024, a. a. O., Rn. 39). Denn in dem Vortrag der Klagepartei, die Kontrolle über ihre Daten durch den Scraping-Vorfall verloren zu haben, liegt die konkludente Behauptung, diese zuvor nicht anderweitig aufgegeben, sondern vor dem Scraping noch über eine entsprechende Kontrolle verfügt zu haben. Soweit der Bundesgerichtshof darauf abgestellt hat, dass es jedenfalls genüge, wenn angegeben werde, die Telefonnummer anderen Personen zuvor nur bewusst und ausgewählt offengelegt zu haben (BGH, Urteil vom 18.11.2024, a. a. O., Rn. 41), bedeutet dies nicht umgekehrt, dass ein Klagevorbringen ohne einen derartigen ausdrücklichen Vortrag zwangsläufig unsubstantiiert oder unschlüssig wäre.

Angesichts der Vielzahl theoretischer Möglichkeiten, die zu einem Kontrollverlust über die eigenen Daten führen können, ist es der Klagepartei trotz der sie an sich treffenden primären Darlegungslast nicht zuzumuten, im Rahmen ihres Vortrags sämtliche dieser Möglichkeiten im einzelnen auszuschließen. Ebenso wenig ist sie gehalten, zu einzelnen dieser Möglichkeiten vorzutragen, solange das Vorbringen der Beklagten hierzu keinen Anlass gibt. Denn in Fällen, in denen das materielle Recht das Nichtvorliegen von Tatsachen zur Anspruchsvoraussetzung erhebt oder sonst nach den Gegebenheiten im konkreten Rechtsstreit das Nichtvorliegen eines Umstands bewiesen werden muss, ist von der nicht darlegungsbelasteten Partei im Rahmen des Zumutbaren das substantiierte Bestreiten der negativen Tatsache unter Darlegung der für das Positivum sprechenden Tatsachen und Umstände zu verlangen (vgl. z. B. BGH, Urteil vom 09.04.1999 - II ZR 331/97, NJW-RR 1999, 1152 unter II1; von Selle in: BeckOK ZPO, Vorwerk/Wolf, 56. Edition, § 138 Rn. 16.1 m. w. N.). Nach der ständigen Rechtsprechung des Bundesgerichtshofs trifft den Prozessgegner der für eine solche negative Tatsache beweisbelasteten Partei eine sogenannte sekundäre Darlegungslast. Seine Darlegungen müssen so konkret sein, dass der beweisbelasteten Partei eine Widerlegung möglich ist (vgl. z. B. BGH, Urteil vom 24.03.2020 - XII 175/08, NJW 2010, 1813

[BGH 24.03.2010 - XII ZR 175/08] Rn. 20; Zöller/Greger, ZPO, 35. Auflage, Rn. 24 vor § 284; jeweils m. w. N.).
Daran fehlt es. Die Beklagte hat im Rahmen ihrer sekundären Darlegungslast einen konkreten vorangegangenen Kontrollverlust durch eine anderweitige, allgemein zugängliche Veröffentlichung der streitgegenständlichen Daten der Klägerseite, die zu ermitteln ihr auch zumutbar ist, nicht dargelegt und ist deren Vortrag folglich nicht substantiiert entgegengetreten.

(3) Nach Auffassung des OLG Celle ist zudem allein das Verhältnis der jeweiligen Klage- zu der jeweiligen Beklagtenpartei maßgeblich. Hat der Kläger dem Beklagten - bspw. im Rahmen eines Vertragsverhältnisses - persönliche Daten übergeben, hat und behält er im Rahmen dieses Verhältnisses auch die Kontrolle über seine Daten. Diese Kontrolle verliert die Klagepartei in der Regel aber dann, wenn die Daten innerhalb der Sphäre der Beklagtenpartei einem Dritten zugänglich gemacht werden (so OLG Celle, Urteil vom 05.03.2025 - 5 U 129/24, juris Rn. 20). Ob diese Sichtweise Zustimmung verdient, bedarf nach dem oben Gesagten indes keiner Entscheidung.

cc) Der der Klägerseite durch den Kontrollverlust entstandene immaterielle Schaden ist angemessen mit 100,00 € zu bewerten.

(1) Für die Schätzungshöhe ist zu berücksichtigen, dass in Anbetracht der Ausgleichsfunktion des in Art. 82 DSGVO vorgesehenen Schadensersatzanspruchs von einer "vollständigen und wirksamen" Entschädigung auszugehen ist, wenn sie den aufgrund des Verstoßes gegen die Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen in der Lage ist.

Ob einer oder mehrere Verstöße gegen die Datenschutz-Grundverordnung festgestellt werden können, kann dahinstehen. Da der in

© 2026 Wolters Kluwer Deutschland GmbH

Art. 82 Abs. 1 DSGVO vorgesehene Schadensersatzanspruch ausschließlich eine Ausgleichsfunktion und keine Abschreckungs- oder Straffunktion erfüllt, führt das Vorliegen mehrerer Verstöße nicht zu einer Erhöhung des Schadensersatzes (vgl. a. dazu BGH, Urteil vom 18.11.2024, a. a. O., Rn. 25 u. 96). Demgemäß ist ohne Relevanz, ob sich die Beklagte weitere Verstöße gegen die Datenschutz-Grundverordnung vorhalten lassen muss, wie etwa einen Verstoß gegen Artt. 24 Abs. 1, 32 DSGVO, wonach der Verantwortliche geeignete technische und organisatorische Maßnahmen umzusetzen hat, um sicherzustellen und den Nachweis erbringen zu können, dass die Verarbeitung gemäß der Datenschutz-Grundverordnung erfolgt, oder einen Verstoß gegen die Meldepflicht nach Art. 33 Abs. 1 DSGVO oder die Benachrichtigungspflicht nach Art. 34 DSGVO. Dabei könnten Verstöße gegen die letztgenannten Bestimmungen ohnehin nicht ursächlich für den eingetretenen Schaden sein (vgl. BGH, Urteil vom 18.11.2024, a. a. O., Rn. 26).

(2) Bei der Schätzung des Schadens sind insbesondere die etwaige Sensibilität der konkret betroffenen personenbezogenen Daten und deren typischerweise zweckgemäße Verwendung zu berücksichtigen. Daneben spielen die Art des Kontrollverlusts (begrenzter/unbegrenzter Empfängerkreis), seine Dauer und die Möglichkeit der Wiedererlangung der Kontrolle, etwa durch Entfernung einer Veröffentlichung aus dem Internet oder Änderung der betroffenen personenbezogenen Daten (zum Beispiel Rufnummernwechsel oder neue Kreditkartennummer) eine Rolle (vgl. BGH, Urteil vom 18.11.2024, a. a. O., Rn. 99). Auf die Frage, ob Art. 82 Abs. 1 DSGVO dahingehend auszulegen ist, dass bei der Bemessung der Höhe des zu ersetzenden immateriellen Schadens der Umstand als anspruchsmindernd berücksichtigt werden kann, dass der betroffenen Person neben dem Anspruch auf Schadensersatz ein Unterlassungsanspruch zusteht (vgl. BGH, Vorlage-

Beschluss vom 26.09.2023 - VI ZR 97/22, juris Rn. 41 ff.), kommt es dagegen nicht an, weil die Klagepartei keinen Unterlassungstitel erwirkt (vgl. unten Ziff. III).
(3) Dies zugrunde gelegt, erscheint es bei einer Gesamtabwägung im Streitfall angemessen, den notwendigen Ausgleich für den eingetretenen Kontrollverlust mit 100,00 € zu bemessen (s. dazu auch BGH, Urteil vom 18.11.2024, a. a. O., Rn. 100).

dd) Ein Anspruch auf weitergehenden Schadensersatz steht der Klagepartei nicht zur Seite, insbesondere auch nicht unter dem Gesichtspunkt der von ihr geltend gemachten psychischen Beeinträchtigungen. Der Eintritt derartiger Beeinträchtigungen, zumal in einem Ausmaß mit Schadensqualität, lässt sich nicht feststellen.

(1) Die Klagepartei trägt hierzu vor, dass diejenigen, die von dem Datenleck betroffen seien, seit Veröffentlichung der Datensätze massenhaft Spam-SMS erhielten. Auch die Klägerseite, die weder die Telefonnummer noch die E-Mail-Adresse selbst so eingestellt habe, dass sie öffentlich für jedermann sichtbar gewesen seien, habe pro Tag eine unterschiedlich hohe Anzahl an Spam-E-Mails, Spam-SMS und Anrufen erhalten. Dadurch habe sie Ängste und Sorgen erlitten. Sie empfinde Sorge beim Öffnen von SMS und E-Mails und habe Angst, dass dadurch Spyware auf ihr Handy oder den Computer gelange, Bankdaten oder Kreditkartendaten gestohlen würden oder sie Opfer eines Identitätsdiebstahls werde. Um Betrugsversuchen vorzubeugen, habe sie die EMail-Adresse gewechselt, das F.-Passwort und die Sichtbarkeitseinstellungen geändert sowie Änderungen an den Einstellungen am Spamfilter vorgenommen.

(2) Zwar hat der Europäische Gerichtshof entschieden, dass die durch einen Verstoß gegen die Datenschutz-Grundverordnung ausgelöste Befürchtung einer betroffenen Person, ihre personenbezogenen Daten könnten von Dritten missbräuchlich verwendet werden, für sich genommen einen "immateriellen Schaden" im Sinne von Art. 82 Abs. 1 DSGVO darstellen könne. Allerdings kann die bloße Behauptung einer solchen Befürchtung ohne nachgewiesene negative Folgen nicht zu einem Schadensersatz nach dieser Bestimmung führen; vielmehr müssen die Befürchtung und ihre negativen Folgen ordnungsgemäß nachgewiesen sein (vgl. z. B.

EuGH, Urteil vom 20.06.2024 - C-590/22, ZD 2024, 519 Rn. 32, 35 f. - PS GbR).
Daran fehlt es; der Klagepartei ist der ihr hiernach obliegende Nachweis nicht gelungen.

(a) Das Landgericht hat die Klagepartei, wie in der Rechtsprechung des Bundesgerichtshofs nahegelegt (vgl. Urteil vom 18.11.2024, a. a. O., Rn. 101), persönlich angehört, ohne sich jedoch die Überzeugung davon verschaffen zu können, dass die von der Klägerseite vorgetragenen psychischen Beeinträchtigungen tatsächlich bestehen.

An diese Feststellungen der ersten Instanz ist der Senat gemäß § 529 Abs. 1 Nr. 1 ZPO gebunden, soweit nicht konkrete Anhaltspunkte Zweifel an der Richtigkeit oder Vollständigkeit der entscheidungserheblichen Feststellungen begründen und deshalb eine erneute Feststellung gebieten. Konkrete Anhaltspunkte in diesem Sinn sind alle objektivierbaren, rechtlichen oder tatsächlichen Einwände gegen die erstinstanzlichen Feststellungen, wobei bloß subjektive Zweifel sowie abstrakte Erwägungen und Vermutungen nicht ausreichen (vgl. z. B.

BGH, Beschluss vom 21.03.2018 - VII ZR 170/17, NJW-RR 2018, 651 Rn. 15; ders., Urteil vom 16.08.2016 - X ZR 96/14, GRUR 2016, 1260 Rn. 17).
Derartige Zweifel begründende konkrete Anhaltspunkte hat die Klägerseite nicht dargetan. Die Feststellungen des Landgerichts erscheinen im Gegenteil plausibel und nachvollziehbar begründet. Die Ausführungen des Landgerichts sind weder widersprüchlich noch unvollständig und verstoßen auch nicht gegen Denkgesetze oder Erfahrungssätze.

© 2026 Wolters Kluwer Deutschland GmbH

(b) Im Rahmen ihrer persönlichen Anhörung hat die Klagepartei angegeben, den Account bei der Beklagten immer noch mit demselben Namen zu nutzen; allerdings habe sie eine andere E-Mail-Adresse hinterlegt. Ihre Handynummer nutze sie weiter, ebenso die Messenger-App von F.. Daneben habe sie einen Instagram-Account und nutze auch das Netzwerk Xing sowie WhatsApp. Sie habe 2019 aus der Presse erfahren, dass es ein Datenleck bei der Beklagten gegeben habe; geprüft habe sie dies jedoch erst im Jahre 2023. Etwa im Jahre 2020 habe sie vermehrt Anrufe bekommen, später auch vermehrt Spam-E-Mails. Es habe Phasen gegeben, in denen dies etwa ein- oder zweimal pro Woche geschehen sei, dann habe es aber auch wieder Ruhephasen gegeben.

(c) Dies genügt nicht, um die Feststellung eines auf den Scraping-Vorfall zurückzuführenden, weitergehenden Schadens der Klägerseite treffen zu können.

Anrufe und Spam-E-Mails, die die Klagepartei in unregelmäßigen Abständen und in einem Ausmaß von bis zu zwei pro Woche seit dem Jahre 2020 erhalten haben will, sind mit Blick auf ihren Umfang und die zeitliche Nähe zu dem Scraping-Vorfall nicht derart auffällig, dass der Schluss auf einen Zusammenhang zu dem Scraping naheläge. Vielmehr ist gerichtsbekannt, dass Belästigungen dieser Art auch eine Vielzahl von anderen Ursachen haben können.

Die von der Klagepartei geschilderten psychischen Beeinträchtigungen sind darüber hinaus nicht glaubhaft. Wäre die Klagepartei im Hinblick auf ihre personenbezogenen Daten tatsächlich dermaßen sensibilisiert, dass ein Kontrollverlust zu echter Sorge führen würde, hätte sie nicht, wie im Rahmen der Anhörung geschildert, erst im Jahre 2023 eine Überprüfung ihrer eigenen Betroffenheit vorgenommen, sondern dies unmittelbar veranlasst, nachdem sie im Jahre 2019 von dem Datenleck bei der Beklagten aus der Presse erfahren hatte. Zudem ist die Klagepartei intensiv im Bereich der sozialen Medien engagiert, was sich mit den von ihr befürchteten Missbrauchsgefahren ebenfalls nicht in Einklang bringen lässt. So nutzt sie weiterhin den Account bei der Beklagten einschließlich der Messenger-App; sie hat lediglich eine andere E-Mail-Adresse hinterlegt. Ebenso wird die Handynummer fortlaufend genutzt und ist die Klagepartei weiter auf Instagram, Xing und bei WhatsApp aktiv. Einen nachvollziehbaren Grund für das Unterbleiben einer Änderung der Telefonnummer hat die Klägerseite nicht angegeben. Dies spricht dafür, dass die unkontrollierte Zuordnung ihrer Mobilfunktelefonnummer keinen nachhaltigen Einfluss auf die Gemütslage der Klagepartei in Form der begründeten Befürchtung einer missbräuchlichen Verwendung und daraus resultierender psychischer Beeinträchtigungen gehabt haben kann (ähnlich OLG Hamm, Urteil vom 15.08.2023, a. a. O., Rn. 145).

(d) Die Voraussetzungen für eine Vernehmung der Klägerseite als Partei liegen nicht vor. § 445 Abs. 1 ZPO erlaubt nur die Vernehmung des Gegners der beweispflichtigen Partei; die für die Vernehmung der beweispflichtigen Partei selbst nach § 447 ZPO erforderliche Zustimmung der Gegenseite hat die Beklagte nicht erteilt. Auch eine Vernehmung nach § 448 ZPO scheidet aus, weil für die insoweit erforderliche gewisse "Anfangswahrscheinlichkeit" (vgl. dazu exempl.

BGH, Urteil vom 28.10.2020 - VIII ZR 230/19, NZM 2020, 1106 Rn. 35 m. w. N.) nach dem oben Gesagten nichts ersichtlich ist.
g) Schließlich ist der Verstoß der Beklagten gegen die Datenschutz-Grundverordnung auch kausal für den der Klagepartei entstandenen immateriellen Schaden in Form des Kontrollverlusts.

Ohne den Verstoß der Beklagten gegen den Grundsatz der Datenminimierung, d. h. ohne die unter Verstoß gegen den Grundsatz der datenschutzfreundlichen Voreinstellungen vorgenommene, nicht von einer Einwilligung der Klagepartei gedeckte und von "allen" Nutzern für eine Datensuche verwendbare Verknüpfung der Mobilfunknummer der Klägerseite mit ihren immer öffentlichen Daten, die so für "alle" anhand der Mobilfunknummer auffindbar waren, hätten die das Scraping initiierenden Dritten die Daten der Klägerseite nicht abschöpfen können.

3. Der Zinsanspruch auf den Zahlbetrag von 100,00 € ergibt sich unter dem Gesichtspunkt des Verzugs (§§ 280 Abs. 2, 286 Abs. 1 S. 1, 288 Abs. 1 BGB). Die Klagepartei hat die Beklagte mit vorprozessualem Schreiben vom 19.05.2023 (Anlage K18) unter Fristsetzung bis zum 02.06.2023 gemahnt, indem sie für den Fall des fruchtlosen Verstreichens der Frist eine gerichtliche Geltendmachung angekündigt hat.

II. Berufungsantrag zu Ziff. 2

Daneben hat die Klägerseite Anspruch auf Feststellung der Verpflichtung der Beklagten, ihr alle zukünftigen Schäden zu erstatten, die ihr durch den unbefugten Zugriff auf ihre im Datenarchiv der Beklagten gespeicherten persönlichen Daten noch entstehen.

1. In Bezug auf künftige Schäden ist der Antrag zulässig und begründet.

a) Das nach § 256 Abs. 1 ZPO erforderliche Feststellungsinteresse liegt vor. Die bloße Möglichkeit des künftigen Eintritts der geltend gemachten Schäden genügt, weil es nicht um reine Vermögensschäden geht, sondern um Schäden, die aus der von der Klägerseite behaupteten Verletzung ihres Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG, mithin des allgemeinen Persönlichkeitsrechts resultieren sollen. Der Bundesgerichtshof hat hierzu ausgeführt, dass auch die primär als Anspruchsgrundlage herangezogene Vorschrift des Art. 82 DSGVO dann, wenn - wie hier - mit einem möglichen Verstoß gegen Art. 5 DSGVO auch eine unrechtmäßige Datenverarbeitung gerügt werde, eine Verletzung des Rechts auf Schutz der personenbezogenen Daten gemäß Art. 1 Abs. 2 DSGVO zum Inhalt habe. Die

© 2026 Wolters Kluwer Deutschland GmbH

Möglichkeit ersatzpflichtiger künftiger Schäden sei ohne Weiteres zu bejahen, wenn ein deliktsrechtlich geschütztes absolutes Rechtsgut verletzt werde und - wie hier - bereits ein Schaden eingetreten sei (vgl. BGH, Urteil vom 18.11.2024, a. a. O., Rn. 48).

b) Im Streitfall wurde die Klagepartei durch den oben dargestellten Verstoß der Beklagten gegen die Datenschutz-Grundverordnung in ihrem Recht auf informationelle Selbstbestimmung verletzt. Infolge der andauernden Veröffentlichung der personenbezogenen Daten der Klagepartei besteht auch das Risiko einer missbräuchlichen, insbesondere betrügerischen Nutzung dieser Daten mit der Folge eines materiellen Schadens fort, den die Klägerseite bei dessen Eintritt nach Art. 82 Abs. 1 DSGVO von der Beklagten erstattet verlangen kann.

Umfasst ist auch - wie beantragt - die Erstattung noch nicht vorhersehbarer immaterieller Schäden. Verletzungsfolgen, die zum Beurteilungszeitpunkt noch nicht eingetreten waren und deren Eintritt objektiv nicht vorhersehbar war, mit denen also nicht oder nicht ernstlich gerechnet werden musste und die deshalb zwangsläufig bei der Bemessung des Schmerzensgeldes unberücksichtigt bleiben müssen, werden von der vom Gericht ausgesprochenen Rechtsfolge nicht umfasst und können deshalb Grundlage für einen Anspruch auf weiteres Schmerzensgeld sein (vgl. z. B.

BGH, Urteil vom 14.02.2006 - VI ZR 322/04, NJW-RR 2006, 712 Rn. 7 m. z. N.).
2. Soweit der Feststellungsantrag dagegen ursprünlich auch auf bereits eingetretene Schäden gerichtet gewesen ist, hat die Klagepartei die Berufung mit Schriftsatz vom 19.05.2025 zurückgenommen.

III. Berufungsantrag zu Ziff. 3

In Bezug auf den Berufungsantrag zu Ziff. 3 bleibt die Berufung ohne Erfolg.

1. Der Unterlassungsantrag zu Ziff. 3a ist sowohl unzulässig als auch unbegründet.

a) Der Antrag ist unzulässig.

aa) Allerdings ist der Unterlassungsantrag zu Ziff. 3a nach der Antragsänderung mit Schriftsatz vom 19.05.2025 hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO. Die Umformulierung des Antrags, die die inhaltliche Reichweite des Antrags unberührt lässt, dient lediglich dem Zweck, den Bedenken gegen die Bestimmtheit der ursprünglichen Formulierung Rechnung zu tragen, und stellt keine an § 533 ZPO zu messende Klageänderung dar, die im Übrigen sachdienlich wäre.

(1) Ein Klageantrag ist hinreichend bestimmt, 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 Ungenauigkeit auf den Beklagten abwälzt und eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt. Ein Unterlassungsantrag darf vor diesem Hintergrund nicht derartig undeutlich gefasst sein, dass die Entscheidung darüber, was dem Beklagten verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt (std. Rspr., vgl. z. B.

BGH, Urteil vom 09.03.2021 - VI ZR 73/20, NJW 2021, 1756 Rn. 15; ders., Urteil vom 28.07.2022 - I ZR 205/20, MMR 2023, 198, Rn. 12).
(2) Diesen Anforderungen genügt der Antrag zu Ziff. 3a. Die Klagepartei hat die künftig zu unterlassende Verletzungshandlung insofern weiter konkretisiert, als sie deutlich gemacht hat, dass es um die Verarbeitung der personenbezogenen Daten bei Eingabe der Telefonnummer der Klägerseite in das Kontakt-Import-Tool sowie die darüber hergestellte Verknüpfung der angegebenen Telefonnummer mit weiteren öffentlichen personenbezogenen Daten des Nutzerprofils der Klagepartei geht. Diese soll nicht erfolgen, ohne dass die Beklagte Sicherheitsmaßnahmen in Form einer Implementierung von Sicherheits-CAPTCHAs und der Überprüfung massenhafter IP-Abfragen vorhält. Damit lässt die Antragsfassung erkennen, durch welche konkrete Maßnahme die Beklagte gegen die Datenschutz-Grundverordnung verstoßen haben soll (vgl. BGH, Urteil vom 18.11.2024, a. a. O., Rn. 57 f.).

Die Formulierung "vergleichbare Sicherheitsmaßnahmen" führt nicht zur Unbestimmtheit des Antrags. Sie dient ersichtlich dem Zweck, der Beklagten in der Wahl der von ihr zu ergreifenden Maßnahmen eine Auswahl zu lassen, solange diese geeignet sind, dass konkrete Rechtsschutzziel zu erreichen (vgl. zu diesem Aspekt BGH, Urteil vom 18.11.2024, a. a. O., Rn. 56).

bb) Der Antrag zu Ziff. 3a, der dahin auszulegen ist, dass die Beklagte ein Kontakt-Import-Tool nur unter Implementierung von Sicherheitsmaßnahmen in Form von SicherheitsCAPTCHAs und der Überprüfung massenhafter IP-Abfragen oder vergleichbaren Methoden durchführen soll, stellt sich in seinem Schwerpunkt jedoch als verkappter Leistungsantrag auf Implementierung solcher Sicherheitsmaßnahem, was ein aktives Tun erfordert, dar. Er ist damit im Hinblick auf § 890 Abs. 2 ZPO, aber auch im Hinblick § 259 ZPO unzulässig (OLG Hamm Urteil vom 10.01.2025 - 7 U 68/24, GRUR-RS 2025, 10403 Rn. 38 m. w. N.).

cc) Dem Antrag fehlt darüber hinaus das Rechtsschutzbedürfnis. Das Rechtsschutzschutzbedürfnis fehlt, wenn eine Klage oder ein Antrag objektiv schlechthin sinnlos ist, der Kläger also unter keinen Umständen mit seinem prozessualen Begehren irgendeinen schutzwürdigen Vorteil erlangen kann (vgl.

© 2026 Wolters Kluwer Deutschland GmbH

BGH, Urteil vom 29.09.2022 - I ZR 180/21, NJW-RR 2023, 66, Rn. 10), oder wenn das verfolgte Begehren auf einem einfacheren Weg zu erlangen ist (BGH, Urteil vom 30.09.2009 - VIII ZR 29/09, NJW-RR 2010, 19 Rn. 20; Bacher in: Vorwerk/Wolf, ZPO, 55. Edition, § 253 Rn. 29).
So liegen die Dinge hier, weil die Klägerseite eine Verarbeitung ihrer personenbezogenen Daten über die Eingabe ihrer Telefonnummer in das Kontakt-Import-Tool nebst darüber hergestellter Verknüpfung der Telefonnummer mit ihren öffentlichen personenbezogenen Daten im Falle von Sicherheitsmaßnahmen der Beklagten, die aus Sicht der Klagepartei dem Stand der Technik nicht genügen, auf einfache Weise dadurch verhindern kann, dass sie über die Vornahme entsprechender Einstellungen keine Einwilligung zu einer derartigen Datenverarbeitung erteilt.

b) Der Antrag ist darüber hinaus unbegründet.

aa) Nach Artt. 24 Abs. 1 S. 1, 32 Abs. 1 DSGVO trifft der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das Vorliegen eines Verstoßes hiergegen unter den Voraussetzungen des Unterlassungsantrags lässt sich indes, ohne dass es hierauf noch entscheidend ankäme, nicht prüfen, weil Vortrag der Klagepartei insbesondere zum aktuellen Stand der Technik sowie dazu, dass und warum es sich bei der Implementierung von Sicherheits-CAPTCHAs um geeignete technische Maßnahmen in diesem Sinne handelt, nicht gehalten worden ist.

bb) Unabhängig hiervon ist der Antrag auch deshalb unbegründet, weil der Klagepartei weder aus § 1004 Abs. 1 S. 2 BGB i. V. m. § 823 Abs. 1 BGB noch aus §§ 280 Abs. 1, 241 Abs. 2 BGB in Verbindung mit dem Nutzungsvertrag ein entsprechender Anspruch auf Unterlassung zusteht.

aa) Sowohl ein vertraglicher als auch ein gesetzlicher Unterlassungsanspruch, sofern die Datenschutz-Grundverordnung einen Rückgriff auf letzteren überhaupt erlaubt (vgl. dazu BGH, Vorlage-

Beschluss vom 26.09.2023 - VI ZR 97/22, juris Rn. 27 ff.), setzen eine Wiederholungsgefahr oder zumindest eine Erstbegehungsgefahr voraus (std. Rspr., vgl. z. B. BGH, Urteil vom 29.07.2021 - III ZR 192/20, GRUR-RS 2021, 23182 Rn. 115), an der es hier fehlt. Allerdings wird durch einen erfolgten Verstoß die tatsächliche Vermutung für seine Wiederholung begründet, so dass infolge einer stattgefundenen Rechtsverletzung auch regelmäßig von Wiederholungsgefahr auszugehen ist. Dabei sind an ihre Entkräftung strenge Anforderungen zu stellen. Die Widerlegung der tatsächlichen Vermutung für das Vorliegen der Wiederholungsgefahr ist etwa dann anzunehmen, wenn der Eingriff durch eine einmalige Sondersituation veranlasst war (vgl. z. B. BGH, Urteil vom 27.04.2021 - VI ZR 166/19, NJW 2021, 3334 Rn. 120). Allgemein kann der Verletzer/Störer die Vermutung der Wiederholungsgefahr widerlegen, indem er Tatsachen darlegt und nötigenfalls beweist, die ernsthaft nahelegen, dass es künftig nicht mehr zu einer weiteren Störung kommen wird (vgl. BGH, Urteil vom 15.09.2003 - II ZR 367/02, NJW 2003, 3702 unter 2d; Spohnheimer in: Gsell/Krüger/Lorenz/Reymann, BGB, § 1004 Rn. 270.3). Der Einwirkende darf nicht mehr verurteilt werden, wenn er beweist, dass Maßnahmen getroffen worden sind, die nach menschlicher Voraussicht die schädlichen Einwirkungen allenfalls auf ein zu duldendes Maß zurückführen, und eine Beseitigung der Schutzeinrichtung nach Lage der Verhältnisse nicht in Frage kommen kann. Erscheint nämlich eine Wiederholung der Beeinträchtigung ausgeschlossen, ist der Unterlassungsgläubiger befriedigt (BGH, Urteil vom 14.10.1994 - V ZR 76/93, NJW 1995, 132 (134); Staudinger/Thole, BGB, Neubearbeitung 2023, § 1004 Rn. 463 m. w. N.; Fritzsche in: Hau/Poseck, BGB, 73. Edition, § 1004 Rn. 94).
bb) So liegen die Dinge im Streitfall, denn die Beklagte hat die Kontaktimportfunktion auf der Plattform am 10.10.2018 und die des F.-Messengers am 06.09.2019 deaktiviert und durch eine "People-You-May-Know"-Funktion ("Personen, die du kennen könntest"Funktion) ersetzt. Bei dieser kann zwar gleichfalls ein Nutzer seine Kontakte mitsamt Telefonnummer hochladen. Das System zeigt ihm dann aber nicht mehr allein aufgrund der Telefonnummer nur den einen passenden konkret-individuellen Nutzer - "one-to-one" - an, sondern nur noch eine Liste von mehreren Personen, die aufgrund anderer zusätzlicher Zuordnungskriterien der hochgeladenen Kontakte, z. B. des Namens, zuzuordnen sein könnten. Das "Friend Centre" wurde bereits am 11.12.2018 in ähnlicher Weise geändert (vgl.

OLG Dresden Urteil vom 10.12.2024 - 4 U 808/24, GRUR-RS 2024, 35688 Rn. 28). Weitere Scraping-Vorfälle unter Ausnutzung der Sichtbarkeits- und Suchbarkeitseinstellungen bezüglich der Telefonnummer hat es bei der Beklagten seitdem nicht mehr gegeben.
Nach Ablauf eines Zeitraums von mehr als fünf Jahren seit dem Scraping-Vorfall ist vor diesem Hintergrund nicht mehr davon auszugehen, dass es zu einem dem streitgegenständlichen Vorfall im Kern gleichartigen Datenzugriff durch Dritte kommen könnte. So erscheint es etwa nach Auffassung des OLG Dresden angesichts des mit einem erheblichen Programmieraufwand verbundenen Abschaltens der Kontaktimportfunktion und der Sanktionierung der Beklagten durch die irische Datenschutzbehörde ausgeschlossen, dass die Beklagte gleichwohl diese Funktion in der Zukunft wieder implementieren und überdies mit einer datenschutzrechtlich unzulässigen Systemvoreinstellung versehen könnte (

OLG Dresden, Urteil vom 10.12.2024 - 4 U 808/24, GRUR-RS 2024, 35688, Rn. 28). Dieser zutreffenden Sichtweise schließt sich der Senat an.

© 2026 Wolters Kluwer Deutschland GmbH

2. Der Berufungsantrag zu Ziff. 3b ist ebenfalls unzulässig, zumindest aber unbegründet.

a) Allerdings hat der Bundesgerichtshof für einen wortgleichen Antrag ausgeführt, dass er trotz seiner weiten Formulierung bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO sei. Er lasse sich dahingehend auslegen, dass die Klagepartei ein Unterlassen jeglicher Verarbeitung der Telefonnummer durch die Beklagte, die über die notwendige Verarbeitung für die Zwei-Faktor-Authentifizierung hinausgehe, begehre. Die Klägerseite begehre, dass die Beklagte ihre Telefonnummer nicht - wie zur Zeit des Scraping-Vorfalls - auf Basis einer von ihr erteilten Einwilligung weiterverarbeite, da diese Einwilligung nach ihrem Verständnis mangels Transparenz unwirksam sei, weil ihr das Ausmaß der Datenverarbeitung betreffend ihrer Telefonnummer bei Erteilung der Einwilligung nicht verständlich gewesen sei (vgl. BGH, Urteil vom 18.11.2024, a. a. O., Rn. 62 f.).

b) Dem Antrag fehlt jedoch das nötige Rechtsschutzbedürfnis. Wie bereits dargelegt, fehlt das Rechtsschutzschutzbedürfnis unter anderem dann, wenn der Kläger unter keinen Umständen mit seinem prozessualen Begehren irgendeinen schutzwürdigen Vorteil erlangen kann oder wenn das verfolgte Begehren auf einem einfacheren Weg zu erlangen ist. Davon ist hier auszugehen.

aa) Zwar kann die Klagepartei nicht darauf verwiesen werden, ihre Telefonnummer in einer Weise zu löschen, dass sie sich der Möglichkeit der Zwei-Faktor-Authentifizierung für die Anmeldung zum Nutzerkonto begeben würde. Doch hat die Klagepartei die Möglichkeit, ihre Privatsphäre-Einstellungen so zu ändern, dass sie ihre Einwilligung zur Verarbeitung der Telefonnummer auf die Nutzung der Zwei-Faktor-Authentifizierung beschränkt. Denn die Klagepartei konnte die Suchbarkeitseinstellungen bezüglich ihrer Telefonnummer selbst bei der Kontakt-Import-Funktion seit Mai 2019 auf "nur ich" abändern. Darin liegt im Verhältnis zu einem entsprechenden Unterlassungstitel ein einfacherer und dementsprechend auch günstigerer Weg, der das Rechtsschutzbedürfnis entfallen lässt. Seit Einführung der "People-You-May-Know"-Funktion ist die Anzeige direkter Kontaktübereinstimmungen, für die eine unerwünschte Verwendung der Telefonnummer ausgeschlossen werden müsste, ohnehin entfallen. Darüber hinaus kann die Klagepartei nach dem Vortrag der Beklagten im Schriftsatz vom 23.05.2025 ihre Telefonnummer inzwischen auch aus ihrem Konto entfernen und sie dann für die Zwei-Faktor-Authentifizierung erneut registrieren. Alternativ besteht die Möglichkeit, die Telefonnummer zu entfernen und weiterhin zwei andere Methoden der Zwei-Faktor-Authentifizierung zu nutzen.

Gründe, die dem entgegenstehen würden und für einen Fortbestand des Rechtsschutzbedürfnisses sprechen könnten, sind von der Klagepartei nicht aufgezeigt worden. Zu dem von ihr für den Unterlassungsantrag in Anspruch genommenen Rechtsschutzbedürfnis trägt sie nur vor, es genüge nicht, die PrivatssphäreEinstellungen selbst zu ändern, weil sie im Frontend keinen Einfluss auf die von der Beklagten einzurichtenden Sicherheitsmaßnahmen der Webseite im Backend habe.

Abgesehen davon, dass sich dieser Vortrag allein auf den Unterlassungsantrag zu Ziff. 3a beziehen dürfte, ist nichts dafür ersichtlich, dass die von der Beklagten dem Nutzer zur Verfügung gestellten Optionen zur Datenschutzeinstellung die ihnen jeweils zugewiesene technische Funktion nicht erfüllen würden. Insbesondere hat die Klägerseite aber auch nicht dargelegt, dass die Beklagte die Telefonnummer trotz der beschriebenen Überarbeitung der Suchbarkeitsfunktion bzw. selbst im Falle einer Änderung der Suchbarkeitseinstellung der vormaligen Kontakt-Import-Funktion auf "nur ich" außerhalb der Zwei-Faktor-Authentifizierung verarbeitet oder jedenfalls eine solche Verarbeitung droht, und es keine Einstellungen gibt, über welche die Klägerseite dies selbst unterbinden könnte.

bb) Soweit - insofern allerdings ohne Orientierung am Vortrag der Klagepartei - die Beklagte und nicht die Klägerseite zu Informationen der Beklagten im Hilfebereich zu dem Thema "Wozu verwendet F. meine Mobilnummer" (Anlage B 6) ausführt, gilt folgendes:

Abgesehen davon, dass die Klagepartei hierzu keinen Vortrag gehalten, ihr Rechtsschutzbegehren also auch nicht hierauf gegründet hat, liefert die Beklagte an dieser Stelle unter der Überschrift "Möglicherweise verwenden wir deine Mobilnummer für diese Zwecke" verschiedene Informationen, aus denen sich die Besorgnis einer weitergehenden Verarbeitung und Nutzung der Telefonnummer, der die Klagepartei nicht durch Vornahme entsprechender Einstellungen entgegenwirken könnte, ebenfalls nicht ergibt.

Die Beklagte hat die Nutzer an der genannten Stelle im Hilfebereich und im relevanten Zeitraum über vier mögliche Verwendungen ihrer Telefonnummer informiert: zur Hilfe im Falle des Vergessens des Passworts, zum Schutz des Kontos bei Logins über unbekannte Geräte, um Personen vorzuschlagen, die der Nutzer kennen könnte, und schließlich zur Präsentation relevanter Anzeigen. Diese Information bringt zum Ausdruck, dass die Mobilnummer je nach Einstellung und (ggf. vom Nutzer erklärten) Bedarf (so verlangt etwa die Hilfe bei der Anmeldung die Eingabe der Mobilnummer durch den Nutzer, worin ohnehin eine Einwilligung durch diesen in die Verwendung der Nummer liegt) abschließend für diese vier Zwecke genutzt wird. Dagegen ist sie bei einer Auslegung vom objektiven Empfängerhorizont aus (§§ 133, 157 BGB) nicht dahingehend zu verstehen, dass sich die Beklagte weitere unbenannte Nutzungszwecke vorbehält (ebenso OLG Hamm, Urteil vom 10.01.2025 - 7 U 68/24, GRUR-RS 2025, 10403 Rn. 42).

Auch insofern besteht ein einfacherer und billigerer Weg im teilweisen Widerruf der Einwilligung in die Verwendung der eigenen Rufnummer, und zwar für alle Zwecke, die der Authentifizierung nicht dienen (vgl. Art. 7 Abs. 3 Satz 1 DSGVO), bzw. in der Registrierung der Telefonnummer ausschließlich für die Zwei-Faktor-Authentifizierung. Anhaltspunkte dafür, dass die Beklagte die Rufnummer der Klagepartei dennoch für andere Zwecke weiterverwenden würde, sind nicht vorhanden, zumal die Beklagte für

© 2026 Wolters Kluwer Deutschland GmbH

diesen Fall mit einer Geldbuße nach Art. 83 DSGVO zu rechnen hätte.

c) Unabhängig hiervon ist der Antrag mit Blick auf den von der Klagepartei im Antrag hergestellten Zusammenhang zu einer "Verwendung des Kontakt-Import-Tools" zumindest unbegründet, weil der Klagepartei mangels Wiederholungsgefahr oder wenigstens Erstbegehungsgefahr auch insofern weder aus § 1004 Abs. 1 S. 2 BGB i. V. m. § 823 Abs. 1 BGB noch aus §§ 280 Abs. 1, 241 Abs. 2 BGB in Verbindung mit dem Nutzungsvertrag ein Anspruch auf Unterlassung einer Verarbeitung ihrer Telefonnummer auf der Grundlage der gegebenen Einwilligung zusteht. Hinsichtlich der dafür maßgeblichen Gründe wird auf die obigen Ausführungen Bezug genommen.

IV. Berufungsantrag zu Ziff. 4

Im Hinblick auf den Auskunftsantrag haben die Parteien den Rechtsstreit in der zweiten Instanz übereinstimmend in der Hauptsache für erledigt erklärt.

V. Berufungsantrag zu Ziff. 5

Der mit dem Berufungsantrag zu Ziff. 5 geltend gemachte Anspruch auf Freistellung von vorgerichtlichen Rechtsanwaltskosten in Höhe von 1.134,55 € ist nur teilweise i. H. v. 90,96 € begründet.

1. Grundsätzlich umfasst Art. 82 Abs. 1 DSGVO auch einen materiell-rechtlichen Kostenerstattungsanspruch für die anwaltliche Tätigkeit. Die Kosten der Rechtsverfolgung, zu der auch die Kosten eines mit der Sache befassten Rechtsanwalts zählen, gehören grundsätzlich zu dem wegen einer unerlaubten Handlung zu ersetzenden Schaden (std. Rspr., vgl. BGH, Urteil vom 18.11.2024, a. a. O., Rn. 78 ff.). Allerdings hat der Schädiger nicht alle durch das Schadensereignis adäquat verursachten Rechtsanwaltskosten zu ersetzen, sondern nur solche, die aus Sicht des Geschädigten zur Wahrnehmung seiner Rechte erforderlich und zweckmäßig waren (ebenfalls std. Rspr., vgl. z. B.

BGH, Urteil vom 05.12.2017 - VI ZR 24/17, NJW 2018, 935 Rn. 6).
2. Im Streitfall werden die außergerichtlichen Kosten für das vorprozessuale und als "Zahlungsaufforderung" überschriebene Schreiben vom 19.05.2023 (Anlage K18) geltend gemacht. Die Beklagte ist hier unter Fristsetzung bis zum 02.06.2023 aufgefordert worden, mit Blick auf den Scraping-Vorfall immateriellen Schadensersatz in Höhe von 2.500,00 € zu zahlen, ihre Verpflichtung zur Leistung materiellen Schadensersatzes für zukünftige Schadensfolgen dem Grunde nach anzuerkennen, ein Verhalten zu unterlassen, das in einer dem ursprünglichen Berufungsantrag zu Ziff. 3a entsprechenden Weise beschrieben worden ist, und schließlich Auskunft über die personenbezogenen Daten, welche von der Beklagten verarbeitet worden sind, zu erteilen. Die hiermit verbundenen Kosten waren nur teilweise erforderlich und zweckmäßig.

a) Nach dem oben Gesagten war diese Aufforderung nur mit Blick auf einen Zahlbetrag in Höhe von 100,00 € sowie hinsichtlich der Verpflichtung zur Leistung materiellen Schadensersatzes für zukünftige Schadensfolgen erforderlich und zweckmäßig. Da die Klagepartei nicht davon ausgehen konnte, die Beklagte werde ohne Weiteres ihrer Ersatzpflicht nachkommen, und es sich auch nicht um einen schlichten, absolut einfach liegenden Fall handelt, durfte sie berechtigterweise ihre Bevollmächtigten mit der Wahrnehmung ihrer Interessen beauftragen.

b) Im Hinblick auf den geltend gemachten Unterlassungsanspruch erscheint das Aufforderungsschreiben jedoch nicht zweckmäßig, weil der Anspruch in einer der ursprünglichen Fassung des Unterlassungsantrags entsprechenden und damit unbestimmten, das von der Beklagten zu unterlassende Verhalten nicht eindeutig beschreibenden Weise (vgl. BGH, Urteil vom 18.11.2024, a. a. O., Rn. 55 ff.) formuliert worden ist.

Die Aufforderung zur Auskunft ist allgemein auf die von der Beklagten verarbeiteten personenbezogenen Daten bezogen und steht in keinem erkennbaren Zusammenhang zu dem im Eingang des Aufforderungsschreibens vom 19.05.2023 dargestellten Anlass des Schreibens, nämlich dem Scraping-Vorfall. Die geltend gemachte Auskunft erschöpft sich zudem in dem Grundfall des Art. 15 Abs. 1 DSGVO, also der Mitteilung der verarbeiteten personenbezogenen Daten, die durch Übersendung einer entsprechenden Kopie nach Art. 15 Abs. 3 S. 1 DSGVO erfolgt. Eine solche Mitteilung vermag jedoch jeder Nutzer der Plattform der Beklagten durch ein einfaches Schreiben selbst anzufordern; der Beauftragung eines Rechtsanwalts bedarf es dazu nicht. Gründe, die dafür sprechen, dass die Klagepartei, etwa aus Mangel an geschäftlicher Gewandtheit oder aus sonstigen Gründen wie Krankheit oder Abwesenheit, zur Abfassung selbst eines solch schlichten Anschreibens nicht in der Lage gewesen sein sollte, sind weder vorgetragen noch sonst ersichtlich.

3. Weitere Voraussetzung für einen Erstattungsanspruch ist grundsätzlich, dass der Geschädigte im Innenverhältnis zur Zahlung der in Rechnung gestellten Kosten verpflichtet ist. Das ist vorliegend der Fall.

Ob eine vorprozessuale anwaltliche Zahlungsaufforderung eine Geschäftsgebühr nach Nr. 2300 RVG VV auslöst oder als der Vorbereitung der Klage dienende Tätigkeit nach § 19 Abs. 1 S. 2 Nr. 1 RVG zum Rechtszug gehört und daher mit der Verfahrensgebühr nach Nr. 3100 RVG VV abgegolten ist, ist eine Frage des Innenverhältnisses, nämlich der Art und des Umfangs des im Einzelfall erteilten Mandats. Erteilt der Mandant den unbedingten Auftrag, im gerichtlichen Verfahren tätig zu werden (vgl.

© 2026 Wolters Kluwer Deutschland GmbH

Vorb. 3 Abs. 1 S. 1 RVG VV), lösen bereits Vorbereitungshandlungen die Gebühren für das gerichtliche Verfahren aus, und zwar auch dann, wenn der Anwalt zunächst nur außergerichtlich tätig wird. Für das Entstehen der Geschäftsgebühr nach Nr. 2300 VV RVG ist dann kein Raum mehr. Beschränkt sich der Auftrag dagegen nur auf die außergerichtliche Tätigkeit des Anwalts oder wird der Prozessauftrag unter der aufschiebenden Bedingung erteilt, dass zunächst vorzunehmende außergerichtliche Einigungsversuche erfolglos bleiben, wird er also nur (aufschiebend) bedingt für den Fall des Scheiterns des vorgerichtlichen Mandats erteilt, steht der Prozessauftrag der Gebühr aus Nr. 2300 RVG VV nicht entgegen (vgl.

BGH, Urteil vom 22.06.2021 - VI ZR 353/20, NJW-RR 2021, 1070 Rn. 7).
Hier hat die Klagepartei die Beklagte mit vorprozessualem Schreiben vom 19.05.2023 (Anlage K18) unter Fristsetzung bis zum 02.06.2023 gemahnt, wobei seitens des Prozessbevollmächtigten für den Fall des fruchtlosen Verstreichens der Frist angekündigt worden ist, der Mandantschaft zu einer gerichtlichen Geltendmachung zu raten. Dies spricht indiziell dafür, dass sich der Auftrag auf die außergerichtliche Tätigkeit beschränkt hat und es einer nachfolgenden Beratung zwischen Anwalt und Mandant überlassen bleiben sollte, final über die Klageerhebung zu entscheiden.

4. Für die Verpflichtung zur Leistung von Schadensersatz für künftige materielle Schäden erscheint ein Gegenstandswert in Höhe der Hälfte des für den - sich ursprünglich auf gegenwärtige und künftige materielle und aktuell auf künftige materielle und immaterielle Schäden beziehenden - Berufungsantrag zu Ziff. 2 anzusetzenden Streitwerts und damit von 250,00 € angemessen. Demgemäß sind die Gebühren für die Zahlungsaufforderung vom 19.05.2023 unter Berücksichtigung eines berechtigterweise geltend gemachten Zahlbetrags von 100,00 € nach einem Gegenstandswert von 350,00 € zu bemessen.

Für eine 1,3-fache Geschäftsgebühr nach Nr. 2300 VV RVG errechnen sich nach einem Gegenstandswert bis zur Wertstufe von 500,00 € Gebühren in Höhe von 63,70 €. Hinzu tritt die Pauschale für Entgelte für Post- und Telekommunikationsdienstleistungen nach Nr.7002 VV RVG in Höhe 20 %, mithin von 12,74 €, so dass sich insgesamt 76,44 € netto und zzgl. Umsatzsteuer (vgl. Nr. 7008 VV RVG) 90,96 € brutto errechnen.

VI.

1. Die Kostenentscheidung folgt aus §§ 91a Abs. 1, 92 Abs. 1 u. Abs. 2 Nr. 1, 97 Abs. 1 u. Abs. 2, 516 Abs. 3 S. 2 ZPO.

Soweit der Rechtsstreit hinsichtlich des Auskunftsantrags in der zweiten Instanz übereinstimmend von den Parteien in der Hauptsache für erledigt worden ist, war gemäß § 91a Abs. 1 ZPO unter Berücksichtigung des bisherigen Sach- und Streitstands nach billigem Ermessen über die Kosten zu entscheiden. Dabei kommt es vornehmlich darauf an, wem die Kosten des Rechtsstreits aufzuerlegen gewesen wären, wenn die Hauptsache nicht einvernehmlich für erledigt erklärt worden wäre (std. Rspr., vgl. z. B.

BGH, Beschluss vom 07.05.2007 - VI ZR 233/05 NJW 2007, 3429 Rn. 7). Billigem Ermessen entspricht es hier, dass die diesbezüglichen Kosten erster Instanz von der Beklagten und die Kosten des Berufungsverfahrens von der Klagepartei zu tragen sind.
a) Der Auskunftsantrag war ursprünglich begründet und hat sich infolge der erst im Zuge des Rechtsstreits seitens der Beklagten erteilten Auskunft erledigt, so dass grundsätzlich die Beklagte die hierauf entfallenden Kosten zu tragen hat.

aa) Nach Art. 15 Abs. 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet worden sind; ist dies der Fall, hat sie einen Anspruch auf Auskunft über diese personenbezogenen Daten und bestimmte weitere Informationen, insbesondere auch die Empfänger von personenbezogenen Daten (Art. 15 Abs. 1 lit. c DSGVO). Zur Erfüllung der Auskunftspflicht stellt der Verantwortliche nach Art. 15 Abs. 3 S. 1 DSGVO eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.

Demgemäß hatte die Klagepartei Anspruch gegen die Beklagte auf Auskunft darüber, welche sie betreffenden personenbezogenen Daten von unbefugten Dritten durch den Scraping-Vorfall erlangt werden konnten. Auch insoweit handelt es sich um einen Datenverarbeitungsvorgang, für den die Beklagte verantwortlich im Sinne von Art. 15 Abs. 1 DSGVO ist. Denn unter "Verarbeitung" im Sinne von Art. 4 Nr. 2 DSGVO ist jeder Vorgang im Zusammenhang mit personenbezogenen Daten zu verstehen, unter anderem auch das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder jede andere Form der Bereitstellung.

bb) Diesen Anspruch hat die Beklagte erst im Verlauf des Rechtsstreits erfüllt (§ 362 Abs. 1 BGB). Sie hat während des Klageverfahrens zunächst mit außerprozessualem Schreiben vom 25.09.2023 (Anlage B15) zum Auskunftsbegehren Stellung genommen und auf allgemeine öffentliche Erklärungen im M. Newsroom Blog und im F.Hilfebereich verwiesen. In Bezug auf das individuelle Konto der Klagepartei ist jedoch ausgeführt worden, dass die Beklagte nicht in der Lage sei, das angebliche F.-Konto der Klägerseite mit den von ihr bereitgestellten Informationen zu identifizieren. Für weitere Informationen ist die Klagepartei zur Bereitstellung zusätzlicher Informationen aufgefordert worden, die zur Bestätigung ihrer Identität nötig seien, namentlich die mit dem F.-Konto verbundene E-Mail-Adresse oder URL mitzuteilen. Nachdem die zur Identifikation nötigen Daten schließlich vorgelegen haben, hat die Beklagte ihre Auskunft mit weiterem außergerichtlichen Schreiben vom 18.01.2024 (Anlage B 17)

© 2026 Wolters Kluwer Deutschland GmbH

ergänzt und darin ausgeführt, dass es sich bei den Informationen über die Klagepartei, soweit sie in den durch Scraping abgerufenen Daten enthalten gewesen seien, um auf F. öffentlich zugängliche Daten gehandelt habe. Die Beklagte halte zwar keine Kopie der Rohdaten vor, welche die durch Scraping abgerufenen Daten beinhalte, doch sei es ihr gelungen, der Nutzer-ID der Klagepartei die Datenkategorien Nutzer-ID, Vor- und Nachnahme sowie Geschlecht zuzuordnen, die in den durch Scraping abgerufenen Daten erschienen und mit den auf dem F.-Profil der Klagepartei verfügbaren Informationen übereinstimmten.

Damit hat die Beklagte den zu stellenden Anforderungen genügt. Der Klägerseite ist so im Rahmen der Möglichkeiten der Beklagten ausreichend deutlich gemacht worden, welche individuellen personenbezogenen Daten der Klagepartei durch das Scraping abgeschöpftt wurden.

Soweit das Landgericht mit Blick auf die geforderte Auskunft in den Entscheidungsgründen (Seite 23 LGU) auf Schreiben der Beklagten vom 23.08.2021 (Anlage K2) und vom 10.01.2022 (Anlage B16) Bezug nimmt, dürfte es sich um Schreiben aus Parallelverfahren handeln, was lediglich klarstellend anzumerken ist.

b) Die Kosten des Rechtsmittelverfahrens mit Blick auf den Antrag zu Ziff. 4 fallen dagegen der Klagepartei zur Last, weil die Erledigungserklärung bereits in der ersten Instanz hätte abgegeben werden können. Dass ein Kläger in der Lage war, eine (einseitige) Erledigungserklärung bereits vor dem erstinstanzlichen Gericht abzugeben, schließt nach der Rechtsprechung des Bundesgerichtshofs eine solche Erklärung und die hiermit verbundene Umstellung auf einen Feststellungsantrag in der Berufungsinstanz zwar nicht aus. Allerdings kommt in einem solchen Fall die Anwendung des § 97 Abs. 2 ZPO in Betracht. Dem steht nicht entgegen, dass das erstinstanzliche Gericht es versäumt hat, auf die Notwendigkeit der Antragsumstellung hinzuweisen (vgl. z. B.

BGH, Urteil vom 11.12.2015 - V ZR 26/15, BeckRS 2016, 5218, Ls. 2 u. 3). Entsprechendes muss gelten, wenn sich die Gegenseite der Erledigungserklärung anschließt und demgemäß eine Kostenentscheidung nach § 91a ZPO zu treffen ist.
2. Die Entscheidung zur vorläufigen Vollstreckbarkeit ergibt sich aus §§ 708 Nr. 10, 713 ZPO.

VII.

Veranlassung, das Verfahren analog § 148 ZPO bis zur Vorabentscheidung des Gerichtshofs der Europäischen Union im Vorabentscheidungsverfahren zum Az. C-273/25 auszusetzen, besteht nicht. Hinsichtlich der Frage, ob der Kontrollverlust der betroffenen Person über ihre personenbezogenen Daten bereits für sich genommen einen immateriellen Schaden begründet, besteht aufgrund der Entscheidungen des Gerichtshofs vom 14.12.2023 (NJW 2024, 1091 = GRUR-RS 2023, 35786 und GRUR 2024 - Gemeinde Ummendorf), vom 25.01.2024 (NJW 2024, 320 = GRUR-RS 2024, 530), vom 11.04.2024 (GRUR 2024, 784 - juris), vom

20.06.2024 (C-590/22, GRUR-RS 2024, 13978 und NJW 2024, 2599) und vom 04.10.2024 (C-200/23, GRUR-RS 2024, 26255) kein Klärungsbedarf mehr. Die Rechtslage ist durch die Rechtsprechung des Gerichtshofs in einer Weise geklärt, dass für einen vernünftigen Zweifel keinerlei Raum bleibt ("acte éclairé", vgl. EuGH NJW 2021, 3303 Rn. 33 ff.; EuGH NJW 1983, 1257 (1258)) (so ausdrücklich BGH, Urteil vom 18.11.2024, a. a. O., Rn. 82).
Auch die zweite Vorlagefrage vermag eine Aussetzung des Verfahrens nicht zu rechtfertigen. Es geht dort darum, ob eine Klagepartei unter den im Vorlagebeschluss genannten Bedingungen nicht bereits vor dem Datenschutzverstoß die Kontrolle über ihre vom Scraping betroffenen personenbezogenen Daten verloren hat, was zum Ausschluss des Schadensersatzanspruchs führt. Die Vorlage zielt damit nicht auf die dem Gerichtshof der Europäischen Union obliegende Auslegung von Unionsrecht, konkret Art. 82 Abs. 1 DSGVO ab, sondern die für die Annahme eines Datenkontrollverlusts zu treffenden nötigen Feststellungen, die indes dem nationalen Recht zu entnehmen sind.

VIII.

Gründe zur Zulassung der Revision im Sinne von § 543 Abs. 2 ZPO liegen nicht vor. Weder hat die Rechtssache grundsätzliche Bedeutung noch erfordern die Fortbildung des Rechts oder die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Revisionsgerichts. Es handelt sich um eine Entscheidung, die anerkannte Grundsätze der höchstrichterlichen Rechtsprechung zur Anwendung bringt.

IX.

Der Streitwert beläuft sich auf 3.500,00 € und war mithin auf die Wertstufe bis 4.000,00 € festzusetzen.

Der Streitwert ist nach nach allgemeinen Regeln nach freiem Ermessen und in nicht vermögensrechtlichen Angelegenheiten unter Berücksichtigung aller Umstände des Einzelfalls, insbesondere des Umfangs und der Bedeutung der Sache und der Vermögens- und Einkommensverhältnisse der Parteien nach Ermessen zu bestimmen (§ 48 Abs. 2 S. 1 GKG, § 48 Abs. 1 GKG i. V. m. § 3 ZPO). Dies zugrunde gelegt ergibt sich folgendes:

Der Streitwert für den Berufungsantrag zu Ziff. 1 entspricht dem geltend gemachten Zahlbetrag und beläuft sich deshalb auf

© 2026 Wolters Kluwer Deutschland GmbH

1.000,00 €.

Der Streitwert für den Berufungsantrag zu Ziff. 2, mit welchem die Verpflichtung der Beklagten zum Ersatz etwaiger künftiger und gegenwärtiger Schäden festgestellt werden soll, orientiert sich an dem Antrag zu Ziff. 1 und den hiermit zum Ausdruck gebrachten Vorstellungen der Klagepartei von der Schadenshöhe. Er ist mit einem Bruchteil zu bemessen, wobei 50 %, mithin 500,00 € angemessen erscheinen. Nachdem das streitgegenständliche Datenleck bereits fünf Jahre vor dem Zeitpunkt der Berufung aufgetreten ist, bleibt realistischer Weise kaum Raum für einen jetzt noch eintretenden künftigen Schaden der Klägerseite.

Für die beiden Unterlassungsanträge (Berufungsanträge zu Ziff. 3a und Ziff. 3b) erscheinen jeweils 750,00 €, insgesamt also ein Wert von 1.500,00 € angemessen.

Bei einem Unterlassungsantrag nach einer erfolgten Verletzungshandlung ist das Interesse des Anspruchstellers an der Unterbindung weiterer gleichartiger Verstöße maßgeblich, welches insbesondere durch die Art des Verstoßes, seine Gefährlichkeit und Schädlichkeit für den Inhaber des verletzten Rechts bestimmt wird. Daneben kann auch anderen, von der bereits erfolgten Verletzungshandlung unabhängigen Faktoren - etwa dem Grad der Wahrscheinlichkeit zukünftiger Zuwiderhandlungen - Rechnung zu tragen sein (vgl.

BGH, Urteil vom 12.05.2016 - I ZR 1/15, GRUR 2016, 1275 Rn. 35 - Tannöd). Schließlich darf auch das Gesamtgefüge der Bewertung nichtvermögensrechtlicher Streitgegenstände nicht aus den Augen verloren werden (so BGH, Beschluss vom 26.11.2020 - III ZR 124/20, GRUR-RS 2020, 34934, Rn. 11). Unter Berücksichtigung dieser Maßstäbe erscheint eine Festsetzung des Wertes der Unterlassungsanträge auf insgesamt 1.500,00 € sachgerecht (ebenso BGH, Beschluss vom 10.12.2024 - VI ZR 7/24, GRUR 2025, 269 Rn. 15 - Scraping-Verfahren). Insoweit ist zu berücksichtigen, dass das Ausmaß einer vom Wert des Unterlassungsanspruchs gespiegelten künftigen Beeinträchtigung, die durch den Unterlassungsantrag vermieden werden soll, kaum wesentlich oberhalb der bereits stattgehabten Beeinträchtigung liegen wird, die die Klagepartei selbst mit 1.000,00 € bemisst. Hinzu tritt, dass es sich bei Verfahren der vorliegenden Art um Massenverfahren handelt und das Interesse der Klagepartei vornehmlich auf den Zahlungsantrag gerichtet ist, während die übrigen Anträge gewöhnlich der Anreicherung des Prozessstoffs ohne wesentliches eigenes materielles Interesse der Klagepartei dienen (so OLG Celle, Urteil vom 04.04.2024 - 5 U 31/23, GRUR-RS 2024, 6435 Rn. 59; OLG Oldenburg, Urteil vom 30.04.2024 - 13 U 89/13, GRUR-RS 2024, 12098 Rn. 55).
Der Wert des Auskunftsanspruchs (Berufungsantrag zu Ziff. 4) richtet sich nach dem wirtschaftlichen Interesse des Anspruchstellers an der Erteilung der Auskunft. Da die Auskunft im allgemeinen die Geltendmachung des Leistungsanspruchs erst vorbereiten und erleichtern soll, ist es gerechtfertigt, den Wert des Auskunftsanspruchs mit einem Bruchteil, nämlich einem Zehntel bis einem Viertel des Leistungsanspruchs und umso höher anzusetzen, je geringer die Kenntnisse des Anspruchstellers von den zur Begründung des Leistungsanspruchs maßgeblichen Tatsachen sind (vgl. z. B.

BGH, Beschluss vom 12.10.2011 - XII ZB 127/11, NJW-RR 2012, 130 Rn. 13 f.; ders., Beschluss vom 28.01.2021 - III ZR 162/20, GRUR-RS 2021, 2286 Rn. 14).
Hieran gemessen ist der Auskunftsanspruch vorliegend mit 500,00 € sowohl ausreichend als auch angemessen bewertet. Der Umstand, dass der Auskunftsanspruch nach der Datenschutzgrundverordnung nicht zwingend der Vorbereitung eines anderen Anspruchs dient, rechtfertigt keinen höheren Ansatz (vgl.

OLG Dresden, Beschluss vom 31.07.2023 - 4 W 396/23, BeckRS 2023, 21123 Rn. 12).
Der Berufungsantrag zu Ziff. 5 ist gemäß § 43 Abs. 1 GKG nicht streitwertrelevant.

Hinweis:

Hinweis: Das Dokument wurde redaktionell aufgearbeitet und unterliegt in dieser Form einem besonderen urheberrechtlichen Schutz. Eine Nutzung über die Vertragsbedingungen der Nutzungsvereinbarung hinaus - insbesondere eine gewerbliche Weiterverarbeitung außerhalb der Grenzen der Vertragsbedingungen - ist nicht gestattet.

© 2026 Wolters Kluwer Deutschland GmbH