OLG München, Hinweisbeschluss v. 13.02.2025 – 24 U 3020/24 e

Titel:

Kein Kontrollverlust durch Verknüpfung einer Mobilfunknummer mit einem Fantasienamen

Normenkette:

DSGVO Art. 4 Nr. 5, Art. 82

Leitsätze:

1. Zwar kann bereits der – selbst kurzfristige – Verlust der Kontrolle personenbezogener Daten einen immateriellen Schaden darstellen. Die betroffene Person muss aber den Kontrollverlust als solchen nachweisen. Kann ein Kontrollverlust nicht nachgewiesen werden, reicht schon die begründete Befürchtung einer Person, ihre personenbezogenen Daten könnten aufgrund eines Verstoßes gegen die Verordnung von Dritten missbräuchlich verwendet werden, für die Begründung eines Schadenersatzanspruchs aus. Die begründete Befürchtung samt ihrer negativen Folgen muss dabei aber ordnungsgemäß nachgewiesen werden. Die bloße Behauptung einer Befürchtung ohne nachgewiesene negative Folgen reicht ebenso wenig, wie ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten. (Rn. 17) (redaktioneller Leitsatz)

2. Ein Kontrollverlust über personenbezogene Daten setzt voraus, dass durch das Scraping eine Verknüpfung, etwa die eines Nutzernamens einer sozialen Plattform mit einer nicht öffentlich geteilten Telefonnummer, hergestellt wurde, die eine missbräuchliche Nutzung ermöglicht. Ist eine solche Verknüpfung, etwa bei der Nutzung eines Fantasienamens, nicht nachvollziehbar, liegt grundsätzlich kein ersatzfähiger immaterieller Schaden vor. Missbräuchlich nutzbar wäre eine Verknüpfung der Mobilfunknummer mit dem Fantasienamen nur dann, wenn der Fantasiename für einen größeren Kreis von Dritten einen Rückschluss auf die tatsächliche Identität des Betroffenen ermöglichen würde. (Rn. 21 – 22) (redaktioneller Leitsatz)

3. Ein Kontrollverlust infolge eines Scraping-Vorfalls setzt voraus, dass der Betroffene zu dem fraglichen Zeitpunkt die Kontrolle über die entsprechenden Daten (noch) hatte, also die Hoheit über die betreffenden Daten nicht bereits zuvor verloren hatte. Bei nicht per se geheimhaltungsbedürftigen Daten, die – wie der Name – ein Identifizierungsmerkmal darstellen oder die üblicherweise – wie die Telefonnummer – dazu verwendet werden, um in Kontakt mit anderen Personen zu treten und daher im täglichen Leben einem größeren Personenkreis zugänglich gemacht werden, ist eine derartige Kontrolle über Daten nicht ohne weiteres anzunehmen und muss daher dargelegt sowie erforderlichenfalls nachgewiesen werden.(Rn. 23) (redaktioneller Leitsatz)

4. Die bloße Behauptung eines erhöhten Spam-Aufkommens nach einem Scraping-Vorfall genügt nicht, um einen kausalen Zusammenhang zwischen dem Datenabgriff und einem daraus resultierenden Kontrollverlust darzulegen. Fehlt es an einer konkreten zeitlichen Einordnung des Anstiegs unerwünschter Nachrichten und an weiteren Anhaltspunkten für eine missbräuchliche Verwendung der betroffenen Daten, kann ein Verstoß gegen die DSGVO nicht mit der erforderlichen Sicherheit festgestellt werden. (Rn. 24 – 25) (redaktioneller Leitsatz)

Schlagworte:

Datenschutzverletzung, Schadenersatzanspruch, Unterlassungsanspruch, Auskunftsanspruch, Scraping, Zweifaktor-Authentifizierung, Soziale Medien

Vorinstanz:

LG Memmingen, Endurteil vom 29.07.2024 – 26 O 1031/23

Rechtsmittelinstanz:

OLG München, Beschluss vom 17.03.2025 – 24 U 3020/24 e

Fundstelle:

GRUR-RS 2025, 3209

Tenor

1. Der Senat beabsichtigt, die Berufung gegen das Urteil des Landgerichts Memmingen vom 29.07.2024, Az. 26 O 1031/23, gemäß § 522 Abs. 2 ZPO zurückzuweisen, weil er einstimmig der Auffassung ist, dass die Berufung offensichtlich keine Aussicht auf Erfolg hat, der Rechtssache auch keine grundsätzliche Bedeutung zukommt, weder die Fortbildung des Rechts noch die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Berufungsgerichts erfordert und die Durchführung einer mündlichen Verhandlung über die Berufung nicht geboten ist.

2. Hierzu besteht Gelegenheit zur Stellungnahme binnen drei Wochen nach Zustellung dieses Beschlusses.

Entscheidungsgründe

I.

1
Die Parteien streiten um Ansprüche auf Schadenersatz, Unterlassung und Auskunft wegen behaupteter Verstöße der Beklagten gegen die Datenschutzgrundverordnung (DSGVO) und deswegen sich ggf. ergebender Ansprüche insbesondere auf Grundlage der DSGVO.

2
Die Beklagte betreibt die Social Media Plattform „www...com“. Der Kläger ist Nutzer dieser Plattform. Zu nicht genauer bekannten Zeitpunkten vor September 2019 sammelten Dritte unter Nutzung automatisierter Verfahren eine Vielzahl der auf der Plattform der Beklagten verfügbaren öffentlichen Informationen (sog. Scraping). Dies geschah unter Nutzung der sog. Kontakt-Importer-Funktion, wobei die Dritten mögliche Handynummern bzw. Listen von möglichen Handynummern hochluden. Der Kontakt-Importer gab, sofern eine der hochgeladenen Nummern mit dem Konto eines Nutzers verknüpft war, der seine Telefonnummer bei seinem ...-Account angegeben und die standardmäßig voreingestellte Suchbarkeitseinstellung „Alle“ nicht geändert hatte, die Information an die Scraper. Die Scraper konnten so die Telefonnummer einem bestimmten ...-Profil zuordnen und veröffentlichten diese Information zusammen mit den öffentlich zugänglichen Informationen des jeweiligen Profils im Internet.

3
Der Kläger nutzte die von der Beklagten angebotene Möglichkeit einer sogenannten Zweifaktor-Authentifizierung und gab zu diesem Zweck seine Mobilfunknummer bei seinem ...-Account an. Bei den Suchbarkeitseinstellungen, mit denen der Nutzer einstellen konnte, von wem er über die Telefonnummer gefunden werden kann, hatte er die Grundeinstellung auf „alle“ nicht geändert.

4
Der Kläger unterhält seinen ...-Account nicht unter seinem richtigen Namen, sondern unter „…“.

5
Das Landgericht Memmingen hat die Klage mit Urteil vom 29.07.2024 vollumfänglich abgewiesen.

6
Der Kläger verfolgt mit seiner Berufung seine Schlussanträge in erster Instanz unverändert weiter.

7
Zusätzlich regt er an, das Verfahren (zunächst) im Hinblick auf das beim EuGH unter C – 655/23 anhängige Vorabentscheidungsverfahren (Vorlage durch den Bundesgerichtshof im Verfahren VI ZR 97/22, Vorlagebeschluss vom 26.09.2023) auszusetzen.

II.

8
Die zulässige Berufung ist nicht begründet. Das Landgericht Memmingen hat die Klage im Ergebnis zu Recht abgewiesen.

9
Dem Kläger stehen Ansprüche im Zusammenhang mit möglichen Verstößen der Beklagten gegen die Datenschutzgrundverordnung (DSGVO) nicht zu.

10

Zu den Berufungsangriffen ist unter Berücksichtigung des Umstands, dass es nicht erforderlich ist, alle Einzelpunkte des Parteivortrags in den Gründen einer Entscheidung auch ausdrücklich zu bescheiden (vgl. dazu BVerfG, NJW 1997, 2310, 2312; BGH, Beschl. v. 20.09.2021 – IX ZR 46/19, BeckRS 2021, 31643 Rn. 1) folgendes anzumerken:

11
1. Soweit die Klagepartei gestützt auf Art. 82 DSGVO einen Anspruch auf Schadenersatz geltend macht, steht ihr dieser Anspruch nicht zu.

12
a) Der Anwendungsbereich der Datenschutzgrundverordnung ist in räumlicher (Art. 3 Abs. 1 DS-GVO) und sachlicher Hinsicht (Art. 2 Abs. 1 DSGVO) eröffnet. Unklar ist jedoch, ob der zeitliche Anwendungsbereich der DSGVO eröffnet ist. Die Datenschutzgrundverordnung gilt nach Art. 99 Abs. 2 DSGVO erst ab dem 25.05.2018. Auch hinsichtlich der Frage der zeitlichen Anwendbarkeit der DSGVO ist die Klagepartei darlegungs- und beweispflichtig.

13
Aus den tatbestandlichen Feststellungen des Urteils des Landgerichts Memmingen ergibt sich nicht, dass das Scraping der den Kläger betreffenden Daten erst nach dem Inkrafttreten der DS-GVO erfolgte. Das Urteil enthält keine konkreten Feststellungen zum Zeitpunkt des Datenabgriffs. Hier ist lediglich als unstreitig festgestellt, dass jedenfalls ab 2019 Scraping von Benutzerdaten von der Plattform der Beklagten erfolgt sei. Dies schließt frühere Zugriffe nicht aus. Eine Feststellung dazu, dass das Abgreifen der den Kläger betreffenden Daten nicht vor dem 25.05.2018 erfolgt sein könne, enthält das Urteil nicht, ebenso wenig eine Auseinandersetzung mit der Frage der zeitlichen Anwendbarkeit der DSGVO.

14
Schlüssiger Vortrag der Klagepartei dazu, dass die Daten des Klägers mit der erforderlichen Gewissheit erst nach Inkrafttreten der DSGVO gescrapt wurden, liegt nicht vor. Die Klagepartei gibt vielmehr an, den genauen Zeitpunkt des Datenlecks bzw. des Datenabgriffs nicht zu kennen. Sie führt aus, es habe (wohl) im September 2019 ein Datenleck gegeben, infolge dessen zahlreiche Daten von Unbekannten abgegriffen und im Internet veröffentlicht worden seien (Bl. 5 d. Klageschrift). Auch die Daten des Klägers seien abgegriffen worden.

15
Dieser Vortrag besagt nicht, dass das Abgreifen der Daten des Klägers nicht schon deutlich früher erfolgt sein kann. Die Einschränkung durch das Wort „wohl“ zeigt, dass es sich nicht um eine Tatsachenbehauptung, sondern eine reine – und als solche auch gekennzeichnete – Vermutung handelt. Selbst wenn man dies anders sehen und von einer entsprechenden schlüssigen Behauptung ausgehen wollte, ist jedenfalls weder unstreitig noch erwiesen, dass das Abgreifen der Daten des Klägers nicht vor dem 25.05.2018 stattgefunden hat. Die Beklagte gibt an, das Datenscraping sei im Rahmen des Scraping-Sachverhalts im Zeitraum von Januar 2018 bis September 2019 erfolgt. Dies sei der relevante Zeitraum. (Bl. 17 f. der Klageerwiderung). Sie verfüge aber über keine Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten enthalten oder von Logdaten, über die der genaue Zeitraum des Abgreifens im Einzelfall bestimmt werden könnte (siehe hierzu etwa Anlage K2). Damit hat die Beklagte ihrer sekundären Darlegungslast genügt. Das ...-Konto des Klägers besteht auch schon seit mindestens dem Jahr 2015 (da zu diesem Zeitpunkt die Suchbarkeitseinstellung letztmals geändert wurde, siehe Anlage B 17). Ein Daten-Scraping vor dem Jahr 2018 ist also möglich.

16
Vor diesem Hintergrund bleibt letztlich unklar, ob die Mobilfunknummer des Klägers vor oder nach Inkrafttreten der DSGVO durch Scraping mit seinem ...-Profil verknüpft wurde. Damit kommt ein Schadensersatzanspruch auf Grundlage der DSGVO schon deshalb nicht in Betracht, weil der Kläger nicht nachgewiesen hat, dass mögliche Verstöße im zeitlichen Anwendungsbereich der DSGVO stattgefunden haben.

17
b) Von der Problematik des zeitlichen Anwendungsbereichs abgesehen, sind auch die tatbestandlichen Voraussetzungen für einen Schadenersatzanspruch nach Art. 82 DSGVO nicht erfüllt. Voraussetzungen für einen Schadenersatzanspruch nach Art. 82 DSGVO sind ein Verstoß gegen die DSGVO und das Vorliegen

eines materiellen oder immateriellen Schadens sowie eines Kausalzusammenhangs zwischen Schaden und Verstoß, wobei diese Voraussetzungen kumulativ gegeben sein müssen. Die Darlegungs- und Beweislast für das Vorliegen dieser Voraussetzungen trifft die Person, die auf Grundlage von Art. 82 DSGVO den Ersatz eines Schadens verlangt (BGH, Urteil 28.11.2024, VI ZR 10/24, Rn. 21). Unbeschadet der Frage, ob die Verarbeitung der personenbezogenen Daten des Klägers unter Verstoß gegen die DSGVO erfolgte – insoweit spricht einiges dafür, dass die Voreinstellungen der Beklagten in den Suchbarkeitseinstellungen nicht dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. b und c, Art. 25 Abs. 2, S. 2 und 3 DSGVO) entsprochen haben (siehe hierzu BGH a.a.O. Rn. 86 ff.; OLG Hamm, 28.11.2024, I-7 U 52/24 Rn. 27 ff.) – fehlt es jedenfalls an der schlüssigen Darlegung und am Nachweis eines kausalen Schadens, der beim Kläger eingetreten ist. Zwar kann bereits der – selbst kurzfristige – Verlust über die Kontrolle der personenbezogenen Daten einen immateriellen Schaden darstellen. Die betroffene Person muss aber den Kontrollverlust als solchen nachweisen. Kann ein Kontrollverlust nicht nachgewiesen werden, reicht schon die begründete Befürchtung einer Person, ihre personenbezogenen Daten könnten aufgrund eines Verstoßes gegen die Verordnung von Dritten missbräuchlich verwendet werden, für die Begründung eines Schadenersatzanspruchs aus. Die begründete Befürchtung samt ihrer negativen Folgen muss dabei aber ordnungsgemäß nachgewiesen werden. Die bloße Behauptung einer Befürchtung ohne nachgewiesene negative Folgen reicht ebenso wenig, wie ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten. Der Betroffene, der Ersatz des immateriellen Schadens verlangt, muss also geltend machen und ggf. nachweisen, dass der Verstoß gegen die DSGVO für ihn negative Folgen hatte, die einen immateriellen Schaden darstellen (BGH, a.a.O., Rn. 30 ff.).

18
Die ihm obliegende Darlegung und der Nachweis, dass er überhaupt einen Kontrollverlust erlitten hat, sind dem Kläger nicht gelungen.

19
aa) Aufgrund der tatbestandlichen Feststellungen im erstinstanzlichen Urteil, wonach die vom Kläger auf seinem ...-Profil öffentlich zugänglich gemachten Informationen und die mit seinem Konto verknüpfte Telefonnummer zu den abgegriffenen Daten gehörten und im Internet bereit gestellt wurden, steht fest, dass (überhaupt) Daten des Klägers abgegriffen wurden. Zwar hatte die Beklagte erstinstanzlich bestritten, dass Daten des Klägers vom Scraping-Vorfall betroffen waren (vgl. Klageerwiderung, Bl. 7, Bl. 93 f.; Duplik vom 25.06.2024, S. 24, 26 f.) und lediglich angegeben, welche Daten des Klägers potentiell betroffen gewesen sein könnten. Dies spielt allerdings im Hinblick darauf, dass kein Tatbestandsberichtigungsantrag gestellt wurde, in der Berufungsinstanz keine Rolle mehr (siehe OLG Rostock, 20.10.2003, 3 U 6/03).

20
Unklar ist allerdings, welche Daten des Klägers konkret abgegriffen worden sein sollen. Der Tatbestand des landgerichtlichen Urteils verhält sich hierzu nicht. Der Kläger trägt auch nicht substantiiert vor, welche Daten in seinem Fall betroffen gewesen sein sollen. Er führt vielmehr nur allgemein aus, dass alle Daten betroffen gewesen seien, die auf dem jeweiligen Profil auf „öffentlich einsehbar“ gestellt waren (Bl. 11 d. Klageschrift). Soweit erstmals in der Berufungsbegründung unter Bezugnahme auf einen Datenauszug, der in der Replik zu finden sein soll, konkrete Daten als gescrapt angegeben werden, sind dieser Datenauszug und die Fundstelle „Referenznummer As. 168“ nicht auffindbar. Es handelt sich insoweit offensichtlich um ein Versatzstück aus einem anderen Verfahren, das versehentlich in die Berufungsbegründung geraten ist. Der Senat geht daher davon aus, dass, ausgehend von den (nach Angabe der Beklagten) immer öffentlichen Nutzereinstellungen, jedenfalls die Nutzer-ID, das Geschlecht und der Vor- und Nachname, unter dem der Kläger den Account unterhält, betroffen waren und zusammen mit seiner Mobiltelefonnummer veröffentlicht wurden. Dass beim Kläger darüber hinausgehend weitere Daten, wie etwa E-Mail-Adresse oder Geburtsdatum betroffen gewesen sein könnten, wurde von der Beklagten ausdrücklich bestritten (Klagerwiderung, Bl. 111 ff.). Letztlich gibt auch die Klagepartei selbst an, dass jedenfalls Vor- und Nachname, ...-ID sowie Handynummer des Klägers betroffen sein sollen, sowie dass mindestens die Telefonnummer des Klägers nicht ausreichend geschützt worden sei (Replik vom 01.12.2023, S. 31).

21
Die entscheidende Information, die durch das Scraping erlangt wurde und die ein gewisses Missbrauchsrisiko birgt, ist im Ergebnis die Verknüpfung einer Mobilfunknummer mit einem konkreten Namen (so auch: BGH, 18.11.2024, VI ZR 10/24 Rn. 49). Bei dem Namen, unter dem der ...-Account geführt wird, und der Nutzer-ID handelt es sich nach den Nutzungsbedingungen um immer öffentliche

einsehbare Daten. Die Kontrolle über diese Daten hatte der Kläger bereits vor dem Scraping-Vorfall allein dadurch, dass er sein ...profil erstellte, selbst aus der Hand gegeben (so auch: OLG Dresden, 10.12.2024, 4 U 808/24 Rn. 28). Denn diese sind für andere Personen, auch wenn diese nicht bei ... angemeldet sind, ohnehin einsehbar und abrufbar. Dass er insoweit die Kontrolle selbst aus der Hand gegeben hat, räumt der Kläger ein (Berufungsbegründung, Bl. 19). Soweit er in diesem Zusammenhang ausführt, er wäre aber in der Lage gewesen, durch Schließen des Accounts für die Zukunft die Kontrolle über diese öffentlichen Daten wieder zu gewinnen, während er die Scraping-Veröffentlichung im Internet nicht zurücknehmen könne, überzeugt dies den Senat nicht. Denn auch wenn er den Account für die Zukunft schließen würde, könnte er bereits erfolgte Zugriffe und auf dieser Grundlage möglicherweise erfolgte Veröffentlichungen und Weiterverbreitungen nicht mehr zurücknehmen. Anders als der Name und die Nutzer-ID stammte die Mobilfunknummer nicht vom öffentlich einsehbaren ...-Profil des Klägers. Das von der Klagepartei beschriebene System der Telefonnummergenerierung kann unabhängig von dem Scraping-Vorfall bei der Beklagten eingesetzt werden. Um festzustellen, ob es sich um eine aktive Telefonnummer handelt, hätte es nicht der Benutzung des Kontakt-Importer-Tools der Beklagten bedurft, vielmehr hätte ein Anruf auf der Nummer ausgereicht (so auch: OLG Hamm, 28.11.2024, I-7, U 52/24 Rn. 42). Der Kläger hat hierzu selbst vorgetragen (Replik, Seite 12), die Trefferwahrscheinlichkeit für denkbare deutsche elfstellige Telefonnummern sei hoch, da diese in der Masse vergeben und aktiv seien. Der Kontrollverlust kann also im Ergebnis nur die Verknüpfung der Telefonnummer mit dem ...-Profil und dort mit dem Namen (und ggf. weiteren personenbezogenen Daten) betreffen. Dass weitere Daten außer Benutzername und ...-ID bei ihm betroffen waren, hat der Kläger – wie bereits ausgeführt – nicht dargelegt und nachgewiesen.

22
Hinsichtlich der Verknüpfung der Mobilfunknummer mit einem Namen, besteht vorliegend die Besonderheit, dass sich der Kläger nicht mit seinem richtigen Nachnamen auf ... angemeldet hatte, sondern als „…“. Soweit er sich darauf beruft, dass pseudonomysierte Daten im Sinne von Art. 4 Nr. 5 DSGVO ebenfalls (in gewissem Umfang, je nach Wahrscheinlichkeit der Re-Identifikation im jeweiligen Verarbeitungskontext) zu schützen seien, betrifft dies nicht die vorliegende Konstellation. Pseudonymisierung im Sinne dieser Vorschrift meint einen durchgeführten Verarbeitungsvorgang, an dessen Ende die ursprünglich personenbezogenen Daten ihrer individualisierender Merkmale beraubt sind und ohne weitere Informationen eine Identifizierung nicht mehr möglich ist, was die Verarbeitungsrisiken für den Betroffenen senken und die Verantwortlichen und Auftragsbearbeiter bei der Einhaltung ihrer Datenschutzpflichen unterstützen soll, weil die zusätzlichen Informationen, die zur Identifizierung nötig sind, gesondert aufbewahrt werden können (Plath, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, § 4 Rn. 17 f.). Um einen solchen Verarbeitungsvorgang geht es vorliegend nicht. Hier hat der Kläger vielmehr selbst einen Fantasienamen gewählt, unter dem er bei ... auftritt. Missbräuchlich nutzbar wäre diese Verknüpfung der Mobilfunknummer mit dem Fantasienamen nur dann, wenn der Fantasiename für einen größeren Kreis von Dritten einen Rückschluss auf die tatsächliche Identität des Klägers ermöglichen würde. Dazu, dass seine Identifizierung über den Fantasienamen möglich wäre, etwa weil er diesen in größerem Umfang im Verkehr verwendet, hat der Kläger nichts vorgetragen. Es handelt sich zudem schon gar nicht um einen hinreichend unterscheidungskräftigen Namen. Somit ist vorliegend für einen Kontrollverlust des Klägers nichts ersichtlich. Es spricht nichts dafür, dass über die gescrapten Daten für Dritte eine Verbindung zwischen der Handynummer und dem wirklichen Namen des Klägers herstellbar war bzw. ist. Eine irgendwie geartete Nutzbarkeit des Wissens, dass eine Person, die ihr ...profil unter dem Fantasienamen „…“ führt, eine bestimmte Mobilfunknummer verwendet, ist nicht ersichtlich.

23
bb) Ein Kontrollverlust durch das erfolgte Scraping bei ... setzt außerdem voraus, dass der Kläger zu dem fraglichen Zeitpunkt die Kontrolle über die entsprechenden Daten (noch) hatte, also die Hoheit über die betreffenden Daten nicht bereits zuvor verloren hatte. Bei nicht per se geheimhaltungsbedürftigen Daten, die – wie der Name – ein Identifizierungsmerkmal darstellen oder die üblicherweise – wie die Telefonnummer – dazu verwendet werden, um in Kontakt mit anderen Personen zu treten und daher im täglichen Leben einem größeren Personenkreis zugänglich gemacht werden, ist eine derartige Kontrolle über Daten nicht ohne weiteres anzunehmen (so auch: OLG Hamm, 28.11.2024, I-7 U 52/24 Rn. 38). Zwar hat der Kläger einen Kontrollverlust, wenn auch nur sehr pauschal und mit einem Satz, hinreichend schlüssig dargelegt. Er hat vorgetragen, dass er seine Telefonnummer stets bewusst und zielgerichtet weitergegeben und diese nicht wahl- und grundlos der Öffentlichkeit, wie etwa im Internet, zugänglich gemacht habe. Dies genügt noch für einen schlüssigen und hinreichend substantiierten Klagevortrag (vgl.

BGH, Urteil vom 28.11.2024, VI ZR 10/24, Rn. 39 f.). Allerdings hat die Beklagte, den Kontrollverlust bestritten (Klageerwiderung, Bl. 67, 102 f., Bl. 145) und die für den Schaden beweisbelastete Klagepartei für den Kontrollverlust keinen Beweis erbracht (siehe hierzu auch BGH, a.a.O. Rn. 37: „Das Risiko der Nichterweislichkeit … verbleibt freilich beim Anspruchssteller“). Die Frage der Erweislichkeit hatte in dem vom Bundesgerichtshof entschiedenen Verfahren keine Rolle mehr gespielt, weil dort das Berufungsgericht bereits von einer nicht ausreichenden Substantiierung des Klagevortrags ausgegangen war. (Dies wird im dortigen Verfahren nach der Zurückverweisung erst zu klären sein – siehe BGH, a.a.O. Rn. 45).

24
Im hier vorliegenden Verfahren hatte die Klagepartei die Parteieinvernahme des Klägers, hilfsweise seine informatorische Anhörung, als Beweis angeboten. Die Voraussetzungen für eine Parteieinvernahme nach § 447 ZPO lagen aber mangels Einverständnisses der Beklagten nicht vor. Die Beklagte hat vielmehr für alle Behauptungen, für die die Klagepartei die eigene Parteivernehmung anbietet, ihr Einverständnis verweigert (Duplik, Bl. 42). Somit hätte sich das Gericht die erforderliche Überzeugung nur durch eine informatorische Anhörung des Klägers verschaffen können (siehe zu dieser Möglichkeit Zöller, ZPO, 35. Aufl., 2024 § 141 Rn. 1a). Der Kläger ist aber zum Verhandlungstermin, trotz ordnungsgemäßer Ladung und Anordnung des persönlichen Erscheinens – ausdrücklich auch zur Aufklärung des Sachverhalts – unentschuldigt nicht erschienen. Allein daraus, dass der Kläger nach eigenen Angaben durch Spam-Anrufe, Spam-SMS und E-Mails belästigt wird, lässt sich nichts dafür herleiten, dass es zu einem Kontrollverlust (erst) durch den Scraping-Vorfall bei ... gekommen ist. Der Kläger hat nämlich angegeben (Anlage K4, Fragebogen), er könne nicht einordnen, wann diese begonnen haben bzw. wann ein starker Anstieg zu verzeichnen gewesen sei (nicht einmal in welchem Jahr), so dass auch eine zeitliche Zuordnung zum Scraping-Vorfall bzw. zur Veröffentlichung der Daten aus diesem Vorgehen im Internet nicht möglich ist. Hinzu kommt, dass – nach dem Beklagtenvortrag – die E-Mail-Adresse, die angeblich auch von vermehrtem Spam-Aufkommen betroffen sein soll, gar nicht durch Scraping von der Plattform der Beklagten abgerufenen worden sein kann, weil sie sich nicht unter den vom Kläger als öffentlich einsehbar eingestellten Nutzerdaten befand. Im Übrigen spricht – worauf die Beklagte zu Recht hinweist – der Umstand, dass der Kläger jedenfalls mit seiner Festnetznummer, seinem Namen und seiner Adresse freizügig im Internet umgeht (Einstellung auf der Internetseite „Das Telefonbuch“), jedenfalls prima facie nicht für einen restriktiven Umgang des Klägers mit seinen personenbezogenen Daten. Deshalb können auch die vom Kläger behaupteten an einen Kontrollverlust anknüpfenden Folgen, wie Belastungen durch ein erhöhtes Spam-Aufkommen, Zeitbedarf für Vorsichtsmaßnahmen und Nachfragen, psychologische Auswirkungen etc. – unabhängig von der Frage ihrer Nachweisbarkeit – nicht mit der erforderlichen Sicherheit kausal auf einen Verstoß der Beklagten gegen Vorschriften der DSGVO zurückgeführt werden.

25
Vor diesem Hintergrund und insbesondere mit Blick auf den Umstand, dass der Kläger den Beginn des Anstiegs von Spamvorfällen zeitlich nicht eingrenzen kann, fehlt es bereits an der schlüssigen Darlegung einer Befürchtung, die gerade an die hier im Raum stehenden Scraping-Vorfälle ... anknüpft, geschweige denn an einem Nachweis. Davon abgesehen hat die Klagepartei bis jetzt ihre Suchbarkeitseinstellungen auf ... nicht verändert, was ebenfalls gegen das Bestehen entsprechender Befürchtungen und Ängste spricht. Bestünden tatsächlich solche Befürchtungen und Ängste, hätte die Klagepartei allen Grund gehabt, zumindest das ursprüngliche Einfallstor für den Datenabfluss umgehend zu schließen. Dass der Kläger ernsthaft einen Kontrollverlust und eine missbräuchliche Verwendung seiner Daten infolge des Scraping-Vorfalls befürchten könnte, erscheint auch deshalb nicht plausibel, weil die Mobilfunknummer nur mit seinem auf ... verwendeten Fantasienamen verknüpft wurde. Betrugsversuche unter Verwendung dieses Namens könnte der Kläger unschwer erkennen.

26
Soweit sich der Kläger auf die Verletzung von Auskunfts-, Informations- und Meldepflichten aus der DSGVO beruft, wären diese Pflichten jedenfalls nachgehend zu einem etwaigen Kontrollverlust gewesen, können diesen also nicht verursacht haben, ebenso wenig etwaige weitere immaterielle Schäden. Sonstige Schäden, die gerade aus einen Verstoß gegen Auskunfts-, Informations- und Meldepflichten resultieren, hat der Kläger nicht dargelegt.

27
c) Ein Schadenersatzanspruch auf Grundlage nationalen Rechts (etwa aus § 280 Abs. 1 BGB in Verbindung mit dem Nutzungsvertrag oder aus Art. 823 Abs. 1 BGB in Verbindung mit Art. 2 Abs. 1, Art. 1 Abs. 1 GG)

kommt nicht in Betracht. Unbeschadet der Frage, ob und inwieweit Vorschriften des nationalen Rechts neben den Vorschriften der DSGVO anwendbar sind, fehlt es jedenfalls an der Darlegung und am Nachweis eines konkreten Schadens im Sinne von §§ 249 ff. BGB, der nach den Vorgaben des nationalen Rechts jedenfalls eine fühlbare Beeinträchtigung voraussetzt. Vorliegend ist die Erheblichkeits-/Bagatellgrenze, die nach nationalem Recht zu Grunde zu legen ist, ersichtlich nicht überschritten. Insbesondere vermag eine Verletzung des allgemeinen Persönlichkeitsrechts eine Geldentschädigung nur zu begründen, wenn es sich um einen schwerwiegenden Eingriff handelt. Ein solcher steht – selbst wenn man einen Kontrollverlust des Klägers entgegen der Auffassung des Senats bejahen wollte – ersichtlich nicht im Raum, da vorliegend keine Beeinträchtigung der Intim- oder Privatsphäre, sondern höchstens der Sozialsphäre im Raum steht (so auch: OLG Hamm, a.a.O. Rn. 61 f.).

28
Der außerhalb des zeitlichen Anwendungsbereichs der DSGVO in Betracht kommende § 7 BDSG schließlich, sah nach h.M. nur einen Ausgleich materieller Schäden vor (siehe BeckOK, Datenschutzrecht, 23. Edition, Stand 01.08.2017). Solche hat der Kläger aber nicht geltend gemacht.

29
2. Der unter Ziff. 3) geltend gemachte Feststellungsantrag teilt im Ergebnis das Schicksal des Leistungsantrags. Mangels Nachweises eines Kontrollverlusts oder einer sonstigen Beeinträchtigung des Klägers ist hier, weil (anders als in dem vom BGH entschiedenen Fall im Hinblick auf die dort revisionsrechtlich zu unterstellenden Tatsachen) schon ein Primärschaden nicht vorliegt, der Eintritt zukünftiger Folgeschäden tatsächlich nicht zu erwarten, so dass dieser Antrag bereits unzulässig ist. Bei Eintritt etwaiger Schäden durch missbräuchliche Verwendung personenbezogener Daten wäre auch nicht aufklärbar, ob diese auf den Scraping-Vorfall zurückzuführen sind. Im übrigen erscheint (selbst wenn man – anders als der Senat – einen Kontrollverlust unterstellen wollte) die Annahme, dass sich aus einer (ggf. fortdauernden) Veröffentlichung des ...-Fantasienamens des Klägers in Verbindung mit seiner Telefonnummer das Risiko einer betrügerischen Nutzung und daraus resultierender Schäden ergeben könnte, lediglich theoretischer Natur. Davon abgesehen stünde auch insoweit die (zeitliche) Anwendbarkeit der Vorschriften der DSGVO zum Zeitpunkt des Abgreifens der Daten des Klägers nicht mit der erforderlichen Gewissheit fest.

30
3. Die Klage ist im Hinblick auf den Unterlassungsantrag Ziff. 4 a) unzulässig. Der Antrag ist nicht hinreichend bestimmt. Hinsichtlich der Einzelheiten wird auf die Begründung des Bundesgerichtshofs im Verfahren VI ZR 10/24 Bezug genommen (BGH, Urteil vom 18.11.2024, VI ZR 10/24, Rn. 52 ff.), die einen im wesentlichen inhaltsgleichen Antrag betrifft.

31
4. Auch der Klageantrag unter Ziff 4 b) (Unterlassung der Verarbeitung der Telefonnummer des Klägers auf der Grundlage einer Einwilligung, 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 Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert wird) ist unzulässig. Es fehlt am erforderlichen Rechtsschutzbedürfnis.

32
Das Rechtsschutzbedürfnis ist zu verneinen, wenn eine Klage oder ein Antrag objektiv schlechthin sinnlos ist, wenn also der Kläger unter keinen Umständen mit seinem prozessualen Begehren irgendeinen schutzwürdigen Vorteil erlangen kann. Dies ist etwa der Fall, wenn ein einfacherer oder billigerer Weg zur Erreichung des Rechtsschutzziels besteht oder der Antragsteller kein berechtigtes Interesse an der beantragten Entscheidung hat. Das Rechtsschutzbedürfnis entfällt dann, wenn das Betreiben des Verfahrens eindeutig zweckwidrig ist und sich als Missbrauch der Rechtspflege darstellt (BGH, Urteil 28.11.2024, VI ZR 10/24 Rn. 67 f.). Auch unter Berücksichtigung des anzuwendenden strengen Maßstabs ist dieser Fall hier gegeben. Nichts anderes ergibt sich mit Blick auf die Erläuterung des Klägers, er begehre mit seinem Antrag die Unterlassung der Verarbeitung derjenigen Daten, in deren Verwendung er aufgrund der in der Klageschrift dargestellten Unübersichtlichkeit der Einstellungsbedingungen tatsächlich gar nicht wirksam eingewilligt habe.

33

aa) Zum einen ist der Kläger, spätestens seit dem Auskunftsschreiben der Beklagten (und erst recht aufgrund der ausgetauschten Schriftsätze im vorliegenden Verfahren) umfassend über die Suchbarkeits- und Sichtbarkeitsfunktionen, insbesondere über die Möglichkeit einer Suchbarkeit mittels seiner Mobilfunknummer, informiert. Gleichwohl hat er – nach dem unbestrittenen Vortrag der Beklagtenseite – bis jetzt die Einstellung hinsichtlich der Suchbarkeit der Telefonnummer nicht verändert, sondern es bei der Einstellung „alle“ belassen. Es ist nicht ersichtlich, welche Information dem Kläger ab Erhalt des Auskunftsschreibens gefehlt hat oder jetzt noch fehlt, um zu entscheiden, ob er von dieser Art der Nutzung seiner Telefonnummer Gebrauch machen will oder nicht. Vor diesem Hintergrund stellt sich im Grunde bereits die Frage, ob die Weiterbenutzung der Plattform, ohne die Suchbarkeitseinstellungen zu ändern, nicht bereits als nachträglich erteilte wirksame konkludente Einwilligung zu werten ist (in diesem Sinne: OLG Hamm, a.a.O., Rn. 69, unter Bezugnahme von Erwägungsgrund 62 S. 1 Var. 1 DSGVO, der dahingehend lautet, dass eine Pflicht, Informationen zur Verfügung zu stellen, sich erübrigt, wenn die betroffene Person die Information bereits hat). Dies kann aber im Ergebnis im Hinblick auf die nachfolgenden Erwägungen dahinstehen.

34
bb) Eine erneute Verwendung der Telefonnummer des Klägers im Kontakt-Importer-Tool scheidet nämlich bereits deswegen aus, weil dieses Tool in dieser Form nicht mehr existiert. Die Kontakt-Importer-Funktion wurde auf der Plattform am 10.10.2018 und die des ...-Messengers am 06.09.2019 abgeschaltet. Eine Funktion auf der Plattform der Klagepartei, die eine eindeutige Zuordnung einer Telefonnummer zu einem Profil ermöglichen würde, gibt es nicht mehr. Es ist zwar noch möglich, Telefonnummern und Kontaktlisten hochzuladen. Der Nutzer erhält mit dieser Funktion jedoch als Ergebnis nur eine Liste der Profile von Personen, die er, auch aufgrund anderer Zuordnungskriterien (zum Beispiel Namen) kennen könnte (people-you-may-know-Funktion). Dass dem so ist, kann – was der Kläger nicht bestreitet – durch jeden ...-Nutzer selbst durch Eingabe einer Telefonnummer überprüft werden. Von weiteren Missbrauchsfällen nach 2019 und dem Bekanntwerden der Scraping-Vorfälle im Jahr 2021 wurde nichts berichtet. Solches trägt auch der Kläger nicht vor. Nachdem die Beklagte die Veränderungen der Nutzungsmöglichkeiten gerade deswegen vorgenommen hat, um einen Missbrauch, wie in der Vergangenheit durch die Scraping-Vorfälle geschehen, zu vermeiden und außerdem von der irischen Datenschutzbehörde wegen der hier gegenständlichen Scraping-Vorfälle mit einer empfindlichen Strafe belegt wurde (mag diese nun rechtskräftig sein oder nicht), ist auch nicht ernsthaft damit zu rechnen, dass die Beklagte wieder ein der Kontakt-Importer-Funktion entsprechendes Tool einführen wird (siehe zum Ganzen und den durchgeführten technischen Änderungen auch: OLG Dresden, 10.12.2024, 4 U 808/24 Rn. 45 ff.).

35
cc) Hinzu kommt, dass die Beklagte sich nicht berühmt, der Kläger habe ihr eine entsprechende Einwilligung ausdrücklich erteilt. Sie geht vielmehr davon aus, sie sei zur Vorgabe der Voreinstellung auf „alle“ und zur Verwendung der personenbezogenen Daten im Rahmen des Kontakt-Importer-Tools berechtigt gewesen, weil die Verarbeitung dieser Daten zur Erfüllung des Vertragszwecks erforderlich sei. Damit sei – nach Auffassung der Beklagten – die Verarbeitung gerade nicht wegen einer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO), sondern nach Art. 6 Abs. 1 lit. b DSGVO rechtmäßig (siehe Seite 41 der Berufungserwiderung: „Denn die Verarbeitung personenbezogener Daten zur Bereitstellung der ...-Plattform – und somit auch die damit verbundene Verarbeitung im Zusammenhang mit der Kontakt-Importer-Funktion – stützt sich auf die Durchführung des jeweiligen Nutzervertrages, mithin auf Art. 6 Abs. 1 S. 1 lit. b) DSGVO. … Eine Einwilligung i.S.v. Art. 6 Abs. 1 S. 1 lit. a) DSGVO ist in diesem Fall weder relevant noch eine Voraussetzung für die rechtmäßige Datenverarbeitung“). Wenn sich die Beklagte aber schon in der Vergangenheit nicht auf eine Einwilligung gestützt hat und sogar einräumt, dass eine solche von ihr nicht eingeholt wurde (siehe Bl. 107 der Klageerwiderung), so ist auch für die Zukunft nicht zu erwarten, dass sie sich auf eine (aus ihrer Sicht ohnehin nicht vorhandene und nicht notwendige Einwilligung) für eine Verarbeitung stützen wird. Zu befürchten wäre allenfalls, dass die Beklagte ihr Handeln erneut als durch Art. 6 Abs. 1 lit b DSGVO gerechtfertigt ansehen würde. Ein derartiges Vorgehen der Beklagten wäre vom Inhalt des Unterlassungsantrags jedoch nicht erfasst.

36
dd) Sofern man den Unterlassungsantrag des Klägers unter Berücksichtigung des zugrunde liegenden Scraping-Sachverhalts großzügig (und im Grunde gegen dessen eigene Erläuterungen) dahingehend auslegen wollte, dass er ein Unterlassen jeglicher Verarbeitung seiner Telefonnummer begehre, die über

die notwendige Verarbeitung im Rahmen der Zwei-Faktor-Identifzierung hinausgehe (vgl. hierzu BGH, Urteil 28.11.2024, VI ZR 10/24 Rn. 68 ff.), so kann der Kläger dieses Ziel auf einfachere Art und Weise erreichen.

37
Angesichts der Informationen der Beklagten über die Möglichkeiten der Einstellung der Suchbarkeitsfunktion, nicht zuletzt aber aufgrund des vorliegenden Verfahrens, weiß der Kläger, dass er die Suchbarkeitseinstellung auf „nur ich“ abändern und dennoch die Zwei-Faktor-Identifizierung weiter nutzen kann. Dies stellt, ebenso wie der Widerruf einer etwaigen Einwilligung – der nach Art. 7 DSGVO ohne weiteres jederzeit möglich wäre – einen einfacheren und billigeren Weg dar (so auch BGH, a.a.O. Rn. 69). Der BGH hatte in dem von ihm entschiedenen Verfahren diese Möglichkeit nur deswegen als nicht ausreichend erachtet, weil nach dem Vortrag des dortigen Klägers nicht auszuschließen war, dass die Beklagte (laut der Angabe in ihrer online-Information mit der Überschrift: „Möglicherweise verwenden wird deine Telefonnummer für diese Zwecke“) seine Telefonnummer für weitere Zwecke verwendete. Hierzu und zu einer etwaigen Abhilfemöglichkeit des (dortigen) Klägers habe das Berufungsgericht keine Feststellungen getroffen (BGH, a.a.O. Rn. 69). Diese Problematik erachtet der Senat im vorliegenden Verfahren nicht als einschlägig, da die Beklagte nach ihrem unbestrittenen Vortrag mit dieser Information („Möglicherweise verwenden wird deine Telefonnummer für diese Zwecke“) nur allgemein über alle möglichen Verwendungszwecke informiert, für die der ...-Nutzer seine Telefonnummer freischalten kann, aber eben nicht alle Verwendungszwecke auf alle Nutzer zutreffen, weil nicht alle Nutzer alle Verwendungszwecke nutzen (Klageerwiderung, Seite 27). Das heißt, tatsächlich wird die Telefonnummer nur für den bzw. die Zwecke verwendet, für die sie vom jeweiligen Nutzer freigegeben ist. Damit hätte der Kläger sehr wohl die Möglichkeit, durch entsprechende Änderung seiner Einstellungen die Verwendung seiner Telefonnummer durch ... auf die Funktion der „Zweifaktor-Authentifizierung“ zu beschränken. Dies räumt der Kläger auch ein (Berufungserwiderung, Bl. 20, 26; Berufungsbegründung vom 30.10.2024, Bl. 30). Er ist jedoch der Auffassung, er sei hierzu nicht verpflichtet, weil die Möglichkeit, Rechtsverletzungen durch eigene Handlungen vorzubeugen, den Unterlassungsanspruch nicht entfallen lasse. Richtig daran ist, dass der Kläger nicht zu einer entsprechenden Änderung seiner Suchbarkeitseinstellung verpflichtet ist. Dies ändert aber nichts daran, dass er eine Unterlassung nicht im Klageweg durchsetzen kann, soweit er in der Lage ist, selbst unschwer Abhilfe zu schaffen. Wie bereits gesagt, besteht für eine Klage dann kein berechtigtes Interesse und auch kein Rechtsschutzbedürfnis. Der weitere Einwand des Klägers, die Zulassung der Möglichkeit, eine Person nicht nur durch Eingabe einer spezifischen Telefonnummer aufzufinden, sondern im Wege des Suchlaufs unter Nutzung der technischen Möglichkeiten des Kontakt-Importer-Tools, weise einen eigenständigen Verletzungsgehalt auf, lässt nicht erkennen, wie dies die Zulässigkeit eines Unterlassungsanspruchs begründen soll.

38
ee) Dass der Kläger kein wirkliches Interesse daran hat, die Nutzung und Suchbarkeit seiner Telefonnummer auf der Plattform ... zu beschränken, zeigt sich daran, dass er, obwohl die Problematik nun seit mehreren Jahren bekannt ist, bis heute weder von der Möglichkeit eines Widerrufs der (angeblichen) Einwilligung Gebrauch gemacht noch die Einstellung hinsichtlich der Suchbarkeit seiner Telefonnummer geändert hat. Dies belegt, dass er entweder die Suchbarkeitsfunktion im jetzt noch möglichen Rahmen weiter nutzen will oder jedenfalls keinen Missbrauch (mehr) befürchtet und deswegen nicht daran interessiert ist, die Nutzbarkeit seiner Telefonnummer einzuschränken. Selbst wenn der Kläger die ihm mögliche Einstellungsänderung für nicht ausreichend halten sollte, um eine zweckwidrige Verwendung seiner Telefonnummer zu verhindern (was er nicht vorgetragen hat), wäre davon auszugehen, dass er zumindest zum vorübergehenden Schutz bis zum Ausgang des Verfahrens diese Möglichkeit zum „Selbstschutz“ ergriffen hätte, falls er einen Missbrauch fürchtet. Dass er dies nicht getan hat, zeigt sein mangelndes Interesse daran, das mit dem Unterlassungsantrag vermeintlich angestrebte Ziel tatsächlich zu erreichen. Das Unterlassungsbegehren ist daher als „venire contra factum proprium“ im Sinne von § 242 BGB zu werten. Außerdem müsste die Beklagte, um jede über die Zwei-Faktor-Identifizierung hinausgehende Verarbeitung der Telefonnummer zu vermeiden, dem Kläger entweder die Nutzung von ... vollständig verweigern oder aber in die von ihm selbst gewählten (und beibehaltenen) Nutzereinstellungen eingreifen und ihn von allen sonstigen Nutzungsmöglichkeiten der Telefonnummer ausschließen, die anderen Nutzern zur Verfügung stehen. Es erscheint dem Senat widersprüchlich und rechtsmissbräuchlich, dass der Kläger die Beklagte verpflichten will, die von ihm in Kenntnis des Scraping-Vorfalls fortgesetzte Nutzung seines ...-Accounts ihrerseits nachträglich einzuschränken.

39
ff) Da somit beide Unterlassungsanträge bereits unzulässig sind, kommt es auf die Fragen, ob sich aus Art. 17 oder 18 DSGVO ein Unterlassungsantrag überhaupt ableiten lässt und ob (andernfalls) die DSGVO insoweit eine abschließende Regelung im Bereich des Datenschutzes darstellt oder daneben Unterlassungsansprüche aus nationalem Recht, etwa basierend auf § 1004 BGB anwendbar sind, nicht mehr an. Eine Aussetzung des Verfahrens im Hinblick auf das Vorabentscheidungsverfahren des Europäischen Gerichtshofs C 655 – 23, in dem diese Fragen aufgrund einer Vorlage durch den Bundesgerichtshof zu klären sind, war daher nicht veranlasst. Aus demselben Grund konnte auch offen bleiben, ob sich aus dem Nutzungsvertrag ein entsprechender Anspruch ergeben könnte (§§ 280, 241 Abs. 2 BGB), was aus Sicht des Senats ohnehin nicht nahe liegt.

40
Im Übrigen ist davon auszugehen, dass ein Unterlassungsantrag auch nicht begründet wäre. Regelmäßig setzt ein Unterlassungsanspruch nämlich eine Wiederholungsgefahr voraus. Mangels nachweisbaren Verstoßes gegen die DSGVO (Verstoß innerhalb des zeitlichen Anwendungsbereichs der DSGVO nicht nachgewiesen, siehe oben) fehlt es vorliegend schon an einer Wiederholungsgefahr. Zwar kann auch eine erstmals ernsthaft drohende Beeinträchtigung ausreichen. Aber auch für eine solche fehlen vorliegend Anhaltspunkte.

41
5. Der unter Ziff. 5 geltend gemachte Auskunftsanspruch aus Art. 15 DSGVO ist nicht begründet (BGH, Urteil vom 28.11.2024, VI ZR 10/24 Rn. 74 ff.). Die Beklagte ist nicht verpflichtet, Auskunft über die ihr nicht bekannten Scraper zu erteilen, weil ihr das nicht möglich ist. Was sie an Informationen erteilen konnte, hat sie erteilt, so dass insoweit der Anspruch durch Erfüllung, § 362 Abs. 1 BGB, erloschen ist.

42
6. Da die Klage in der Hauptsache keinen Erfolg hat, besteht auch kein Anspruch auf Ersatz der vorgerichtlich angefallenen Rechtsanwaltskosten.

43
Da die Berufung keine Aussicht auf Erfolg hat, legt das Gericht aus Kostengründen die Rücknahme der Berufung nahe. Im Falle der Berufungsrücknahme ermäßigen sich vorliegend die Gerichtsgebühren von 4,0 auf 2,0 Gebühren (vgl. Nr. 1222 des Kostenverzeichnisses zum GKG).

44
Das Gericht beabsichtigt den Streitwert auf 6.500,00 € festzusetzen (Ziff. 1 + 2 (Schadenersatz)): 4.000,00 €; Ziff 3 (Feststellung): 500,00 €; Ziff. 4 a) und b): jeweils 750,00 €, Ziff. 5 (Auskunft): 500,00 €. Es besteht Gelegenheit zur Stellungnahme zur beabsichtigten Streitwertfestsetzung ebenfalls innerhalb der gesetzten Frist.