Abschrift

Landgericht Erfurt

Az.: 3 O 580/22 (2)

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

[redacted]
- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **Wilde Beuger Solmecke Partnerschaft mbB**, Kaiser-Wilhelm-Ring 27-29, 50672 Köln, Gz.: [redacted]

gegen

Meta Platforms Ireland Ltd., vertreten durch d. Director Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland
- Beklagte -

Prozessbevollmächtigte:
Rechtsanwälte **Freshfields Bruckhaus Deringer**, Bockenheimer Anlage 44, 60322 Frankfurt am Main, Gz.: [redacted]

wegen Persönlichkeitsrechtsverletzung

hat die 3. Zivilkammer des Landgerichts Erfurt durch

Vorsitzenden Richter am Landgericht [redacted]

als Einzelrichter auf Grund der mündlichen Verhandlung vom 13.04.2023

für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger Schadensersatz in Höhe von 500,00 EUR zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 27.07.2022 zu zahlen

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

3. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von EUR 159,94 zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 27.07.2022 zu zahlen.

   Im Übrigen wird die Klage abgewiesen.

4. Der Kläger hat die Kosten des Rechtsstreits zu tragen.

5. Das Urteil ist für beide Parteien gegen Sicherheitsleistung in Höhe von 110% des zu vollstreckenden Betrages vorläufig vollstreckbar

Tatbestand

Die Beklagte ist die Betreiberin der Webseite www.facebook.com und der Dienste auf dieser Seite (nachfolgend: Facebook). Der Kläger nutzt die von der Beklagten betriebene Social Media-Plattform Facebook.

Facebook enthält bei laufender Nutzung der Seite die Funktion, die etwa im Smartphone einer Nutzerin oder eines Nutzers gespeicherten Mobilfunk-Telefonnummern mit den entsprechenden bei Facebook registrierten Daten abzugleichen. Zweck dieser Funktion war und ist, es Nutzerinnen und Nutzern zu ermöglichen, die Facebook-Profile ihr oder ihm aus anderem Kontext bekannter Personen zu identifizieren und ggf. als „Freunde" dem eigenen Profil hinzuzufügen. Die Funktion ermöglicht also, Facebook-Profile zu identifizieren, auch ohne dass die im Profil hinterlegte Nummer für die Öffentlichkeit freigegeben ist. Verhindern konnten (und können) Nutzerinnen und Nutzer dies, indem sie bei den individuellen Einstellungen im Nutzerkonto auswählen, dass sie – entgegen der Standardeinstellungen – von Dritten nicht anhand der Telefonnummer

gefunden werden möchten.

Jedenfalls zum Zeitpunkt der Erstregistrierung des Klägers bis zu dem unten beschriebenen Vorfall Anfang 2019 (im Folgenden: streitgegenständlicher Zeitraum) war die von der Beklagten betriebene Social Media-Plattform Facebook derart konfiguriert, dass Nutzerinnen und Nutzer bei der Anmeldung ihre Mobilfunk-Telefonnummer oder ihre Email-Adresse hinterlegen mussten. Dabei wurde angegeben, dass nur die Nutzerin oder der Nutzer selbst diese sehen kann, die Nummer also nicht für andere sichtbar auf dem Profil der Nutzerin oder des Nutzers veröffentlicht wird („Nur Du kannst Deine Nummer sehen"). Unter der Eingabe-Maske waren zudem jedenfalls im streitgegenständlichen Zeitraum Links zu den Nutzungsbedingungen, zu einer Datenrichtlinie und zu einer Cookie-Richtlinie angebracht. Eine Information der Nutzerinnen und Nutzer über die oben beschriebene Funktion ist jedenfalls an der Stelle, an der die Ersthinterlegung der Mobilfunknummer vorgesehen war, nicht hinterlegt. Auch die dort verlinkte Datenrichtlinie enthält dabei keine Informationen über die oben beschriebene Nutzung der Mobilfunknummer durch Facebook.

Nach erfolgter Registrierung, mithin bei laufender Nutzung von Facebook, war es den Nutzerinnen und Nutzern jedenfalls im streitgegenständlichen Zeitraum möglich, abweichend von der Standardeinstellung das individuelle Facebook-Profil derart einzustellen, dass Dritte das Profil nicht (mehr) anhand der Mobilfunk-Nummer identifizieren konnten. In diesem Zusammenhang wurden von Facebook ab der Hauptseite des Profils eine Reihe von Informationen, Einstellungen bzw. Untereinstellungen wie folgt angeboten:

Im Menüpunkt „Einstellungen" des jeweiligen Nutzerkontos wurden an verschiedenen Orten Funktionalitäten bzw. Informationen zur gespeicherten Telefonnummer angeboten:

Unter dem Unter-Menüpunkt „Kontoeinstellungen" konnte die Nutzerin bzw. der Nutzer ihre bzw. seine Telefonnummer hinterlegen und ändern. Einen Hinweis, wofür diese genutzt wird, gab es hier nicht. Es wurde dort auch nicht erläutert, für welchen Zweck, in welcher Form und in welchem konkreten Umfang die Beklagte die Mobilfunk-Telefonnummern ihrer Nutzerinnen und Nutzer konkret nutzte. Ein Hinweis darauf, dass auch als privat eingestellte Nummern durch Dritte abgeglichen werden können, erfolgte hier nicht.

Unter dem Unter-Menüpunkt „Benachrichtigungen – Handy" konnte die Nutzerin bzw. der Nutzer weitere, nicht streitrelevante Einstellungen zur Mobilfunk-Telefonnummer vornehmen. Hier war dabei die Information enthalten, dass standardmäßig nur die jeweilige Nutzerin bzw. der jeweilige Nutzer die Telefonnummer einsehen kann. Über die streitgegenständliche Funktion wurde an

dieser Stelle nicht informiert. Durch einen dort ebenfalls vorgehaltenen Button „Mehr dazu" gelangte man zu weiteren Informationen, wobei auch dort keine Informationen dazu vorgehalten waren, dass die Mobilfunk-Telefonnummer dazu verwendet werden kann, das jeweilige Profil zu identifizieren.

An anderer Stelle in den Einstellungen, nämlich unter dem Reiter „Deine Privatsphäre" und dort unter „Bestimme, wer dich finden kann" – und nur hier – konnten die Nutzerinnen und Nutzer einstellen, dass sie nicht anhand der Mobilfunknummer gefunden werden wollten. Dort wurde auch klargestellt, dass „finden" abhängig von den Einstellungen des Nutzers auch bedeuten kann, dass bei Eingabe der Telefonnummer in die Suchzeile der Website das zugehörige Nutzerprofil angezeigt werden kann. Kein Hinweis fand sich hier auf den Umstand, dass dies auch dann möglich ist, wenn die Telefonnummer auf „nicht öffentlich" bzw. „privat" gestellt worden war.

Des Weiteren stellte die Beklagte im Hilfebereich und dort im Bereich „Privatsphäre, Datenschutz und Sicherheit" weitere Informationen zur Verfügung. Insbesondere wurde dort neben einer Fülle anderer Informationen unter „Wie kann ich festlegen, wer mich über meine Email-Adresse oder Handynummer finden kann" auf die obigen Einstellungsmöglichkeiten hingewiesen.

Zudem stellte Facebook auch an anderer Stelle weitere Informationen zur Verfügung, die nach der Darstellung von Facebook die Nutzerinnen und Nutzer dabei unterstützen sollen, informierte Entscheidungen zu treffen.

Unter dem Profil des Klägers auf Facebook waren zum streitgegenständlichen Zeitraum und sind bis heute die folgenden persönlichen Daten des Klägers öffentlich abrufbar: Telefonnummer, Namen, Wohnort und Mailadresse. Im relevanten Zeitraum waren die Suchbarkeitseinstellungen des Klägers so eingestellt, dass alle anderen Facebook-Nutzer ihr Facebook-Profil mithilfe der Telefonnummer finden konnten. Diese Einstellung entsprach der oben beschriebenen und von Facebook derart voreingestellten Standardeinstellung.

Anfang 2019 wurden von unbekannten Dritten personenbezogene Daten von 533 Millionen Facebook-Nutzerinnen und Nutzern aus 106 betroffene Ländern aus dem Datenbestand von Facebook abgeschöpft („gescrapt") und im Folgenden öffentlich verbreitet. Der Prozess des im Internet unstreitig allgegenwärtigen „Scrapings" funktionierte dabei derart, dass von dritter Seite eine große Zahl an Mobilfunknummern frei und nach dem Zufallsprinzip generiert wurden. Diese wurden sodann über eine von Facebook zu diesem Zeitpunkt zur Suche von „Freunden" zur Verfügung gestelltes Funktion, nämlich das „Contact Import Tool" (CIT), unter Verstoß gegen die einschlägigen Nutzungsbedingungen abgefragt. Soweit die zunächst frei generierte Mobilfunknum-

mer in den Datenbeständen von Facebook tatsächlich existierte, wurden den derart handelnden Dritten von Facebook die Profilseiten der dazu gehörenden Personen angegeben. Diese konnten sodann aufgesucht und die dort öffentlich hinterlegten Daten automatisiert abgegriffen und mit der als dazugehörig identifizierten Telefonnummer verknüpft werden. So konnten automatisiert und umfangreiche Datenpakete zu einer großen Zahl an Personen erstellt werden, die jeweils eine Kombination aus bereits zuvor auf den jeweiligen Profilen öffentlich einsehbaren Daten (je nach Einzelfall insb. FacebookID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus) und der zuvor nicht öffentlich einsehbaren Mobilfunknummer enthielten.

Von dem beschriebenen Scraping-Vorfall Anfang 2019 war auch der Kläger betroffen. Die abgegriffenen Daten des Klägers waren im Folgenden zusammen mit den Daten einer großen Zahl weiterer Nutzerinnen und Nutzer in entsprechenden Dateien zumindest öffentlich zugänglich. Eine Meldung der Beklagten bezüglich der Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde erfolgte ebenso wenig wie eine Benachrichtigung der betroffenen Nutzer.

Mit vorgerichtlichem Anwaltsschreiben (Anlage K1, Anlagenband I der Klägerseite) wurde die Beklagte zur Zahlung von 500,00 € immateriellen Schadensersatz sowie zur Unterlassung zukünftiger Zugänglichmachung der klägerischen Daten an unbefugte Dritte aufgefordert. Zudem forderte sie die Beklagte auf, Auskunft zu erteilen; wegen der Einzelheiten, insbesondere des genauen Inhalts des Auskunftsbegehrens, wird Bezug genommen auf die Anlage K1. Die Beklagte wies die Ansprüche auf immateriellen Schadensersatz und auf Unterlassung zurück und erteilte Auskünfte; wegen der Einzelheiten wird Bezug genommen auf die Anlage K2, Bl. Anlagenband I der Klägerseite.

Der Kläger behauptet, die von Facebook vorgehaltene Aufklärung über die Verwendung der von den Nutzerinnen und Nutzern zur Verfügung gestellten Daten sei unverständlich und unzureichend. Die Einstellungsoption, mit der die Suchbarkeit des Profils anhand der Telefonnummer deaktiviert werden konnte, sei nur schwer auffindbar gewesen. Die Einstellungen zur Sicherheit der Telefonnummer auf Facebook seien so undurchsichtig und kompliziert gestaltet, dass die Nutzer mit hoher Wahrscheinlichkeit die Standardeinstellungen beibehielten.

Der Kläger behauptet weiter, der oben dargestellte Scraping-Vorfall bei Facebook Anfang 2019 sei nur möglich gewesen, weil die Beklagte keinerlei Sicherungsmaßnahmen vorgehalten habe, um solch massenhaften Missbrauch des Contact Importer Tools (CIT) zu verhindern. Insbesondere seien weder Sicherheitscaptchas noch anderweitige Mechanismen vorgesehen gewesen, um ungewöhnliche, insb. massenhafte Abfragen von einer IP-Adresse aus zu blocken, obwohl

es sich dabei um ein bekanntes Phänomen gehandelt habe. Es wäre eine Kombination mehrerer Vorsichtsmaßnahmen erforderlich, angemessen und üblich gewesen. Die Beklagte hätte zum einen die maximale Anzahl abgleichbarer Rufnummern begrenzen können. Auch hätte die Suchbarkeit nach Rufnummern per Default auf „Freunde-Freunde" stehen müssen. Ebenfalls wäre nach Bekanntwerden des Missbrauchs die sofortige Abschaltung der fraglichen Funktionalität notwendig gewesen. Auch sei kein Monitoring- und Alarmierungssystem vorhanden gewesen, welches bei Upload von sehr großen Adressbuchchargen einen Befehl zum Einleiten von Maßnahmen abgesetzt hätte.

Der Kläger behauptet, in dem hier streitgegenständlichen Fall seien die folgenden Daten abgegriffen und mit der privaten Mobilfunknummer zu einem Datensatz verbunden worden: Telefonnummer, Namen, Wohnort und Mailadresse. Die Zuordnung der Telefonnummer zu den weiteren Daten eröffne Kriminellen zum Nachteil der Klägerseite eine Vielzahl an Handlungsmöglichkeiten, wie etwa Identitätsdiebstahl, die Übernahme von Accounts oder Phishing-Angriffe. Durch den Vorfall habe der Kläger einen „erheblichen Kontrollverlust" über seine Daten erlitten und verbliebe in einem Zustand großen Unwohlseins und großer Sorge über einen möglichen Missbrauch seiner Daten. Seit dem Vorfall erhalte der Kläger zudem unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail mit Inhalten wie Betrugsversuchen und Viren. Der Kläger fürchte jedes Mal Betrug und verspüre Unsicherheit.

Der Kläger meint, bereits die Verwendung der Mobilfunk-Telefonnummer für die Auffindbarkeit durch Dritte verstoße gegen die einschlägigen Bestimmungen der DSGVO. Insbesondere liege hierfür keine Einwilligung des Klägers vor und die Funktion sei auch sonst datenschutzrechtlich nicht zu rechtfertigen. Die Konfiguration der Seiten von Facebook verstoße zudem gegen den Grundsatz des „Privacy by Design" bzw. „by default". Sie hafte zudem wegen des unzureichenden technischen Schutzes der Daten und wegen unzureichender Auskünfte und Informationen im Anschluss an den Vorfall. Der Kläger ist der Auffassung, es sei für den erlittenen Datenverlust die Zahlung eines Betrages in Höhe von mindestens 1.000,00 € angemessen.

Der Kläger ist zudem der Auffassung, ihm stehe nach §§ 1004 analog, 823 Abs. 1 und aus Abs. 2 BGB i.V.m. Art. 6 Abs. 1 DSGVO sowie Art. 17 DSGVO gegen die Beklagte ein Anspruch auf Unterlassung, seine personenbezogenen Daten in Zukunft ohne vorherige ausreichende Belehrung zu veröffentlichen und diese zukünftig unbefugten Dritten zugänglich zu machen, zu.

Der Kläger beantragt,

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

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

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

a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

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

senger App, hier ebenfalls explizit die Berechtigung verweigert wird.

4. die Beklagte zu verurteilen der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.

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

Die Beklagte beantragt,

die Klage abzuweisen.

Sie behauptet, sie habe die Nutzerinnen und Nutzer ausführlich darüber aufgeklärt, welche Informationen öffentlich seien und was dies für die Nutzerinnen und Nutzer bedeute. Die Optionen zur Änderung der Einstellungen bezüglich der Mobilfunknummer seien klar und einfach zu finden gewesen.

Die Beklagte behauptet weiter, es habe im streitgegenständlichen Zeitraum keine einschlägigen Standards zur Bekämpfung von Scraping gegeben. Sie habe jedoch im Einklang mit der üblichen Praxis während des relevanten Zeitraumes über Übertragungsbegrenzungen bezüglich Datenabfragen, die pro Nutzer oder von einer bestimmten IP-Adresse in einem bestimmten Zeitraum gemacht werden können, Systeme zur Boterkennung und Captcha – Anfragen verfügt. Die Übertragungsbeschränkungen dienten der Abschreckung, könnten Scraping jedoch nicht vollständig verhindern. Auch entwickele sie ihre Maßnahmen fortlaufend weiter. Sie beschäftige ein ganzes Team von Datenwissenschaftlern, -analysten und Softwareingenieuren zur Bekämpfung

von Scraping, das External Data Misuse-Team (EDM-Team). Das EDM-Team solle Scraping-Aktivitäten erkennen, unterbrechen und – soweit möglich – verhindern. Außerdem gehe die Beklagte mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren gegen Scraper vor. Ferner habe sie ihre Systeme insofern angepasst, als dass das Verknüpfen von Telefonnummern mit bestimmten Facebook-Nutzern durch die Kompakt-Importier-Funktion nicht mehr möglich gewesen sei. Sie habe außerdem im Nachgang den „Social Connection Check" eingeführt und die Kontakt-Importer-Funktion dergestalt überarbeitet, dass sie die Anzeige direkter Kontaktübereinstimmungen durch eine Liste mit Kontaktvorschlägen, der „Menschen, die du kennen könntest" – Funktion (sog. PYMK-Funktion) ersetzte.

Die Beklagte behauptet, der streitgegenständliche Vorfall habe kein signifikant höheres Risiko für den Kläger begründet. Die meisten der betroffenen Daten seien ohnehin öffentlich einsehbar gewesen, und die Kombination mit der Telefonnummer erhöhe das damit einhergehende Risiko nicht in relevanter Weise.

Die Beklagte ist der Auffassung, die Anträge zu 1 bis 3 seien bereits unzulässig.

Die Beklagte ist schließlich der Auffassung, das Auskunftsbegehren am Maßstab des Art. 15 DSGVO bereits erfüllt zu haben. Die von dem Kläger begehrten Informationen seien überwiegend bereits von Art 15 DSGVO nicht erfasst, weil sie sich auf Verarbeitungstätigkeiten Dritter und nicht auf solche der Beklagten beziehen würden. Art. 15 Abs. 1 DSGVO verpflichte den Verantwortlichen indes lediglich zur Auskunft in Bezug auf die eigene Verarbeitungstätigkeit.

Entscheidungsgründe

Die Klage ist mit Ausnahme des Antrages zu 3. a. zulässig und in dem aus dem Tenor ersichtlichen Umfang begründet, im Übrigen unbegründet.

Die Klage ist mit Ausnahme des Antrages zu 3. a. zulässig

Das Landgericht Erfurt ist in internationaler, sachlicher und örtlicher Hinsicht zuständig.

Die internationale Zuständigkeit der deutschen Gerichtsbarkeit folgt aus Art. 79 Abs. 2 S. 2 DS-

GVO, nachdem die Klägerseite ihren gewöhnlichen Aufenthalt in Deutschland hat.

Gemäß § 79 Abs. 2 DSGVO sind für Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter im Ausgangspunkt die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Nach S. 2 der Vorschrift können solche Klagen wahlweise auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat, es sei denn, es handelt sich – was vorliegend nicht der Fall ist - bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist. Sinn und Zweck dieser Zuständigkeitsregelung ist die Gewährleistung (und Erleichterung) eines effektiven Rechtsschutzes durch die betroffenenfreundliche Möglichkeit einer Klageerhebung am Aufenthaltsort, wobei damit nicht der „tatsächliche", sondern der „gewöhnliche" Aufenthaltsort gemeint ist, wie der Wortlaut der englischen Sprachfassung („habitual residence") verdeutlicht (Spindler/Dalby, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, DS-GVO Art. 79 Rn. 19).

Diese Voraussetzungen liegen vor. Die Beklagte ist Verantwortliche bzw. Auftragsverarbeitende im Sinne der DSGVO. Gemäß Art. 4 Nr. 7, 8 DSGVO sind Verantwortliche natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Auftragverarbeitende sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Die Beklagte hat vorliegend als Betreiberin der Plattform allein über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden, sodass sie insoweit als Verantwortliche im Sinne der DSGVO anzusehen ist (vgl. EuGH, Urteil vom 5. Juni 2018 – C-210/16 –, Rn. 30, juris); sie ist auch keine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist. Die Klägerseite als betroffene Person hat ihren Wohnsitz in Weimar, sodass die deutsche Gerichtsbarkeit international zuständig ist.

Es kann offenbleiben, ob Art 79 Abs. 2 DSGVO in seinem vorliegend eröffneten Anwendungsbereich die allgemeinen Zuständigkeitsvorschriften der EuGVVO verdrängt (in diesem Sinne etwa Bergt in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, DS-GVO Art. 79 Rn. 15 m.w.N., Albrecht/Jotzo, Das neue Datenschutzrecht der EU, Teil 8: Rechtsbehelfe, Haftung und Sanktionen Rn. 29) oder die Vorschriften daneben anwendbar bleiben (in diesem Sinne wohl

Gola/Heckmann/Werkmeister, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, DS-GVO Art. 79 Rn. 15). Denn auch nach den Vorschriften der EuGVVO ist keine abweichende ausschließliche Zuständigkeit im Sinne des Art. 24 EuGVVO begründet, sondern folgt die internationale Zuständigkeit der deutschen Gerichtsbarkeit vorliegend sowohl aus Art. 7 Nr. 1 lit. b) als auch Art. 18 Abs. 1 Alt. 2, Art. 17 Abs. 1 lit. c) EuGVVO (vgl. (vgl. BGH, Urteil vom 29. Juli 2021 – III ZR 179/20 –, BGHZ 230, 347-389, Rn. 24). Nach Art. 18 EuGVVO kann ein Verbraucher gegen eine Vertragspartei, die ihre Tätigkeit auf den Mitgliedsstaat, in dem der Verbraucher seinen Wohnsitz hat, ausrichtet, vor dem Gericht seines Wohnsitzes Klage erheben.

Vorliegend nutzt die Klägerseite als Privatperson die Plattform der Beklagten, die dabei gewerblich handelt (EuGH, Urteil vom 5. Juni 2018 – C-210/16 –, Rn. 60, juris) und ihre Tätigkeit z.B. durch entsprechende Sprachoptionen auch speziell auf das Gebiet der Bundesrepublik und hier ansässige Nutzer ausgerichtet hat. Im Übrigen wäre aufgrund der Natur der Sache die Leistung der Beklagten, nämlich das Zurverfügungstellen der Nutzungs- und Kommunikationsmöglichkeiten, am Wohnsitz des Schuldners zu erbringen, so dass sich bereits aus Art. 7 Nr. 1 lit. b) 2. Spiegelstrich EuGVVO die internationale Zuständigkeit deutscher Gerichte ergibt.

In sachlicher Hinsicht ist das erkennende Gericht gemäß §§ 23 Nr. 1, 71 Abs. 1 GVG zuständig, nachdem der Wert des Streitgegenstandes die Summe von 5.000,00 € übersteigt.

Die örtliche Zuständigkeit des Landgerichts folgt sowohl aus § 44 Abs. 1 S. 2 BDSG als auch aus Art. 7 Nr. 1 lit. b) EuGVVO.

Art. 79 Abs. 2 S. 1 DS-GVO regelt nur die internationale, nicht auch die örtliche Zuständigkeit (BR-Drs. 110/17, Anl., 111; Paal/Pauly/Frenzel, 3. Aufl. 2021, BDSG § 44 Rn. 1). Insoweit bestimmt § 44 Abs. 1 S. 2 BDSG, dass Klagen der betroffenen Person gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Anwendungsbereich der Verordnung (EU) 2016/679 oder der darin enthaltenen Rechte der betroffenen Person auch bei dem Gericht des Ortes erhoben werden können, an dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat. Diese Voraussetzungen liegen vor, nachdem die Klägerseite ihren gewöhnlichen Aufenthalt im hiesigen Gerichtsbezirk hat.

Im Übrigen folgt die örtliche Zuständigkeit auch aus Art. 7 Nr. 1 lit. b) EuGVVO, der – anders als die Art 17, 18 EuGVVO, die wie auch Art. 4 EuGVVO nur die internationale Zuständigkeit regeln – auch eine Regelung zur örtlichen Zuständigkeit enthält (Geimer in: Zöller, Zivilprozessordnung, 34. Aufl. 2022, Artikel 7 (Artikel 5 LugÜ), Rn. 1).

Die Klageanträge sind mit Ausnahme des Antrages zu 3. a. gemäß § 253 Abs. 2 Nr. 2 ZPO hinreichend bestimmt.

Nach § 253 Abs. 2 Nr. 2 ZPO muss die Klageschrift neben einem bestimmten Antrag eine bestimmte Angabe des Gegenstandes und des Grundes des erhobenen Anspruchs enthalten. Damit werden der Streitgegenstand abgegrenzt und die Grenze der Rechtshängigkeit und der Rechtskraft festgelegt sowie Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts bestimmt. Eine ordnungsgemäße Klageerhebung erfordert dabei eine Individualisierung des Streitgegenstandes. Die Klägerseite muss die gebotene Bestimmung des Streitgegenstandes vornehmen und kann sie nicht zur Disposition des Gerichts stellen. Eine an sich schon in der Klage gebotene Klarstellung kann von der Partei aber noch im Laufe des Verfahrens nachgeholt werden (vgl. zuletzt BGH, Urteil vom 17. Januar 2023 – VI ZR 203/22 –, Rn. 15 m.w.N., juris).

Hieran gemessen ist der Klageantrag zu 1 (mittlerweile) hinreichend bestimmt.

Allerdings handelt es sich entgegen der Auffassung der Klägerseite bei den Ansprüchen wegen „Verstößen der Beklagten gegen die Datenschutzgrundverordnung" und dem Anspruch auf Ersatz immaterieller Schäden wegen einer etwaig unzureichenden Information hierüber um unterschiedliche Streitgegenstände.

Zu dem Lebenssachverhalt, der die Grundlage der Streitgegenstandsbestimmung bildet, zählen alle Tatsachen, die bei einer vom Standpunkt der Parteien ausgehenden natürlichen Betrachtungsweise zu dem durch den Vortrag der Klagepartei zur Entscheidung gestellten Tatsachenkomplex gehören. Ob ein oder mehrere Sachverhalte vorliegen, hängt davon ab, ob das Geschehen bei natürlicher Betrachtungsweise nach der Verkehrsauffassung einen einheitlichen Vorgang darstellt (Anders, in Anders/Gehle, Zivilprozessordnung, 81. Aufl. 2023, § 253 ZPO Rz. 30 m.w.N.). Der Streitgegenstand wird durch den gesamten historischen Lebensvorgang bestimmt, auf den sich das Rechtsschutzbegehren der Klagepartei bezieht, dies gilt unabhängig davon, ob einzelne Tatsachen dieses Lebenssachverhalts von den Parteien vorgetragen worden sind oder nicht, und auch unabhängig davon, ob die Parteien die nicht vorgetragenen Tatsachen des Lebensvorgangs kannten und hätten vortragen können. Diesen Lebenssachverhalt kann das Gericht unabhängig davon unter allen in Betracht kommenden Gesichtspunkten prüfen, gleich, ob die Klagepartei ihre Klage auf diese Gesichtspunkte gestützt hat oder nicht.

Von diesen Grundsätzen ausgehend macht die Klägerseite - wie die Beklagte zutreffend rügt - zwei Streitgegenstände geltend. Sie macht bei der anzulegenden natürlichen Betrachtungsweise einerseits Ansprüche im Zusammenhang mit der gerügt unzureichenden datenschutzrechtli-

chen Erfassung und – im Rahmen ihrer Speicherung und Verarbeitung - Sicherung der Daten der Klägerseite ab der Anmeldung in dem von der Beklagten bereitgehalteten Sozialen Netzwerk über das "Scraping" bis zur unzureichenden Mitteilung hierüber an die zuständige Datenschutzbehörde geltend, die sämtlich aufgrund des sogenannten „Scrapings" der Daten bei einer natürlichen Betrachtungsweise einen einheitlichen Lebenssachverhalt darstellen, weil sämtliche gerügten Pflichtverletzungen sich erst mit dem „Scraping" der Daten aktualisierten. Andererseits macht sie eine unzureichende Erfüllung des Informationsanspruches der Klägerseite geltend, welche aufgrund der Zäsur in Gestalt der Anfrage der Klägerseite an die Beklagte bei natürlicher Betrachtungsweise einen anderen Lebenssachverhalt darstellt.

Die gesamten Ausführungen der Klägerseite genügen jedenfalls mittlerweile einer genügenden Konkretisierung des Streitgegenstandes.

Der Antrag zu 2. ist ebenfalls hinreichend bestimmt. Er lässt sich unter Berücksichtigung der Ausführungen in der Replik so auslegen, dass lediglich der Ersatz künftiger materieller Schäden begehrt wird.

Der Klageantrag zu 3. a. ist nicht hinreichend bestimmt.

Nach § 253 Abs. 2 Nr. 2 ZPO darf ein Unterlassungsantrag - und nach § 313 Abs. 1 Nr. 4 ZPO eine darauf beruhende Verurteilung - nicht derart undeutlich gefasst sein, dass der Streitgegenstand und der Umfang der Prüfungs- und Entscheidungsbefugnis des Gerichts (§ 308 Abs. 1 ZPO) nicht erkennbar abgegrenzt sind, sich der Beklagte deshalb nicht erschöpfend verteidigen kann und die Entscheidung darüber, was dem Beklagten verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt. Aus diesem Grund sind Unterlassungsanträge, die lediglich den Wortlaut eines Gesetzes wiederholen, grundsätzlich als zu unbestimmt und damit als unzulässig anzusehen. Abweichendes kann gelten, wenn der gesetzliche Verbotstatbestand eindeutig und konkret gefasst ist, sein Anwendungsbereich durch eine gefestigte Auslegung geklärt ist oder der Kläger hinreichend deutlich macht, dass er kein Verbot im Umfang des Gesetzeswortlauts beansprucht, sondern sich mit seinem Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert. Die Bestimmtheit des Unterlassungsantrags setzt in solchen Fällen allerdings grundsätzlich voraus, dass zwischen den Parteien kein Streit darüber besteht, dass das beanstandete Verhalten das fragliche Tatbestandsmerkmal erfüllt. Die Wiedergabe des ge-

setzlichen Verbotstatbestands in der Antragsformulierung ist auch unschädlich, wenn sich das mit dem nicht hinreichend klaren Antrag Begehrte durch Auslegung unter Heranziehung des Sachvortrags des Klägers eindeutig ergibt und die betreffende tatsächliche Gestaltung zwischen den Parteien nicht in Frage steht, sondern sich deren Streit auf die rechtliche Qualifizierung der angegriffenen Verhaltensweise beschränkt. Eine auslegungsbedürftige Antragsformulierung kann im Übrigen hinzunehmen sein, wenn eine weitergehende Konkretisierung nicht möglich und die gewählte Antragsformulierung zur Gewährung effektiven Rechtsschutzes erforderlich ist (vgl. BGH, Urteil vom 26. Januar 2017 – I ZR 207/14 –, Rn. 18 m.w.N., juris).

Hieran gemessen weist der Klageantrag zu 3. a. keine ausreichende Bestimmtheit auf.

Der Antrag beschränkt sich bereits im Ausgangspunkt nicht auf die Wiedergabe des – überdies nicht eindeutig und konkret gefassten - gesetzlichen Verbotstatbestandes des Art. 32 Abs. 1 DSGVO, sondern greift aus den dort genannten, zur Gewährleistung eines angemessenen Schutzniveaus zu berücksichtigenden Umständen (Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen) isoliert den Stand der Technik heraus. Unabhängig davon, dass damit mit Blick auf die Begründetheit des Antrages bereits der Maßstab des Art. 32 Abs. 1 DSGVO verkürzt wiedergegeben wird, ist aus dem Antrag bei dieser Fassung nicht hinreichend ersichtlich, welche Maßnahmen die Beklagte konkret zur Erfüllung ihrer Pflicht zu ergreifen hat. Ohne eine solche Konkretisierung ist für die Beklagte aber nicht klar, wann sie ihrer Pflicht Genüge getan hat und wann sie sich einer Haftung bzw. einer Vollstreckung aussetzen würde. Darüber hinaus wäre für das Vollstreckungsgericht - auch und insbesondere angesichts des unbestimmten Standes der Technik - nicht hinreichend deutlich, welche Maßnahmen zu welchem Zeitpunkt von der Beklagten veranlasst werden müssten.

Dies gilt vorliegend umso mehr, als Gegenstand des Unterlassungsantrages nicht lediglich die Unterlassung der Gewährleistung desjenigen Schutzniveaus zum Zeitpunkt des streitgegenständlichen sogenannten „Scraping" Vorfalles ist, sondern darüber hinausgehend und mit Blick auf etwaige zukünftige Entwicklungen und Verstöße die Unterlassung der Zugänglichmachung von personenbezogenen Daten über eine Software zum Importieren von Kontakten ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen. In der Sache beansprucht die Klägerseite damit aber lediglich ein Verbot im Umfang des - zudem nur unvollständig berücksichtigten - Gesetzeswortlaut des Art 32 Abs. 1 DSGVO. Die auslegungsbedürftige Antragsformulierung lässt sich auch durch Auslegung unter Heranziehung des Sachvortrags der Klägerseite nicht eindeutig präzisieren, da insoweit kein Vortrag erfolgt ist. Sie ist entgegen der Auffassung der Kläger-

seite auch nicht unter dem Gesichtspunkt der Gewährung effektiven Rechtsschutzes ausnahmsweise hinzunehmen. Es steht der Klägerseite frei, eine hinreichende Konkretisierung zu erreichen, indem sie ihr Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert, was sie vorliegend nicht getan hat.

Hinsichtlich des Klageantrages zu 2. liegt auch das erforderliche Feststellungsinteresse im Sinne des § 256 Abs. 1 ZPO vor.

Bei der streitgegenständlichen Verletzung eines absoluten Rechtsguts ist ein Feststellungsinteresse im Sinne des § 256 Abs. 1 ZPO zu bejahen, wenn künftige Schadensfolgen (wenn auch nur entfernt) möglich, ihre Art und ihr Umfang, sogar ihr Eintritt aber noch ungewiss sind (Greger in: Zöller, Zivilprozessordnung, 34. Aufl. 2022, § 256 Feststellungsklage, Rn. 9).

Die Klägerseite hat die Möglichkeit des Eintritts zukünftiger materieller Schäden hinreichend dargelegt. Unter Berücksichtigung des Umstandes, dass die im Wege des "Scrapings" erlangten personenbezogenen Daten im Internet veröffentlicht worden sind, erscheint es bei lebensnaher Betrachtung möglich, dass es bei der Klägerseite aufgrund der Veröffentlichung der Telefonnummer und weiterer persönlicher Daten wie Name der Klägerseite im Internet zu künftigen materiellen Schäden, etwa durch betrügerische Anrufe oder die missbräuchliche Verwendung der Identität, etwa im Deliktsfeld der Onlinebetrugskriminalität, kommt.

Die Klage ist im Hinblick auf die Anträge zu 1., 2. und 5. in dem aus dem Tenor ersichtlichen Umfang begründet, im Übrigen unbegründet.

Die Kammer schließt sich diesbezüglich den zutreffenden und ausführlichen Ausführungen des Landgerichts Lübeck in dem Urteil vom 25.05.2023, 15 O 74/22, zitiert bei Juris ,an.

Das Landgericht Lübeck hat diesbezüglich Folgendes ausgeführt:

„Der Antrag zu 1., soweit er immateriellen Schadensersatz wegen Datenschutzverstößen im Zusammenhang mit dem Scraping von Daten im Jahr 2019 betrifft, ist in Höhe von 500 € begründet. Die Klägerseite kann von der Beklagten aus § 82 DSGVO Zahlung von 500 € verlangen.

Es sind mehrere haftungsbegründende Verstöße der Beklagten gegen die einschlägigen Bestimmungen der DSGVO festzustellen.

Zum ersten liegt eine rechtswidrige Verarbeitung von Daten der Klägerseite durch die Beklagte vor.

Grundsätzlich gilt im Anwendungsbereich der DSGVO, dass jede Datenverarbeitung rechtswidrig ist, wenn nicht eine der in Art. 6 DSGVO genannten Bedingungen für eine rechtmäßige Datenverarbeitung erfüllt ist. Die rechtswidrige Datenverarbeitung kann sodann Schadensersatzansprüche nach Art. 82 DSGVO auslösen (BeckOK DatenschutzR/Albers/Veit, 42. Ed. 1.11.2021, DS-GVO Art. 6 Rn. 115). Dies ist hier der Fall. Vorliegend ist nicht festzustellen, dass die von der Beklagten vorgenommene Verarbeitung der Mobilfunknummer der Klägerseite zur Auffindbarkeit durch Dritte rechtmäßig gewesen ist. Weder liegt eine wirksame Einwilligung nach Art. 6 Abs. 1 a DSGVO hierzu vor noch war die Verarbeitung für die Erfüllung des zwischen den Parteien geschlossenen Vertrags erforderlich nach Art. 6 Abs. 1 b DSGVO , noch ist festzustellen, dass die Verarbeitung zur Wahrung der berechtigten Interessen der Klägerseite oder Dritten erforderlich war, Art. 82 ABs. 1 f DSGVO.

Dabei legt das Gericht zugrunde, dass die folgenden Einzeldaten verarbeitet und im Folgenden im Zuge des „Scraping"-Vorfalls abgegriffen wurden: Telefonnummer, Namen, Wohnort und Mailadresse.

Es liegt keine wirksame Einwilligung der Klägerseite in die Nutzung ihrer nicht öffentlich geteilten Mobilfunknummer für die Auffindbarkeit durch Dritte vor.

Wirksame Einwilligungen in Datenverarbeitungsvorgänge müssen gemäß Art. 4 Nr. 11 DSGVO freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich sowie durch Erklärung oder eine sonstige eindeutige bestätigende Handlung erfolgen (vgl. nur BeckOK DatenschutzR/Albers/Veit, 42. Ed. 1.11.2021, DS-GVO Art. 6 Rn. 29-39). Im Hinblick auf die letzte Anforderung präzisiert dabei Erwägungsgrund 32 diese Vorgabe dahingehend, dass Stillschweigen oder vorangekreuzte Kästchen nicht genügen. Sogenannte „Opt out"-Varianten zur Einholung einer Einwilligung sind demnach nicht zulässig, weil nicht ausgeschlossen werden kann, dass die Nutzerinnen oder Nutzer die dem voreingestellten Ankreuzkästchen beigefügte Information nicht gelesen haben (BeckOK DatenschutzR/Albers/Veit, 42. Ed. 1.11.2021, DS-GVO Art. 6 Rn. 29-39). Explizit schreibt hierzu insb. auch der EuGH (EuGH (Große Kammer), Urteil

vom 1.10.2019 – C-673/17 -, NJW 2019, 3433, Rn. 60 ff.):

„Die VO 2016/679 sieht mithin nunmehr ausdrücklich eine aktive Einwilligung vor. Hierzu ist festzustellen, dass nach dem 32. Erwägungsgrund der Verordnung die Einwilligung unter anderem durch Anklicken eines Kästchens beim Besuch einer Internetseite zum Ausdruck kommen könnte. Dagegen wird in diesem Erwägungsgrund ausdrücklich ausgeschlossen, dass „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit" eine Einwilligung darstellen können. Folglich liegt eine wirksame Einwilligung iSv Art. 2 Buchst. f und Art. 5 III der RL 2002/58 iVm Art. 4 Nr. 11 und Art. 6 I Buchst. a der VO 2016/679 nicht vor, wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss.

Für den vorliegenden Fall folgt hieraus, dass eine wirksame Einwilligung der Klagepartei in die vorgenannte Datenverarbeitung der Beklagten nicht gegeben ist.

Allein aus dem Umstand, dass die Suchbarkeit für Dritte anhand der Mobilfunknummer voreingestellt war, kann nach der genannten Rechtsprechung des Europäischen Gerichtshofes keine wirksame Einwilligung fingiert werden. Weiterer Vortrag dazu, wodurch die Klägerseite in der erforderlichen aktiven Weise ihre Einwilligung zu der gegebenen Nutzung erteilt haben könnte, liegt nicht vor. Insbesondere ist kein Vortrag dahingehend feststellbar, dass im Kontext der Erstregistrierung durch Klick auf den Button „Registrieren" eine entsprechende Einwilligung abgegeben wurde. Zwar wurde die Klägerseite in diesem Kontext unstreitig auf die Nutzungsbedingungen und die Datenschutzrichtlinie der Beklagten hingewiesen. Es liegt aber kein Vortrag dahingehend vor, dass in einer dieser beiden Dokumente die hier streitgegenständliche Funktionalität auch nur Erwähnung findet, sodass dem Registrierungsvorgang insoweit auch kein Erklärungswert zukommen kann. Soweit die Beklagte in diesem Kontext auf Seite 6 der Datenschutzrichtlinie und den dortigen Link verweist („Mehr dazu, wie Du die Informationen über dich kontrollieren kannst, die du mit diesen Apps und Webseiten teilst bzw. die andere teilen.") führt dies nicht weiter. Denn es ist nicht vorgetragen, wohin dieser Link führt und welche Informationen dort aufzufinden sind. Im Übrigen läge eine wirksame Einwilligung selbst dann nicht vor, wenn unter diesem Link Informationen zu der hier streitgegenständlichen Funktionalität abrufbar wären. Denn eine auf einer derartig platzierten Information fingierte Einwilligung wäre nicht „in informierter Weise" erfolgt, wie aber nach den obigen Ausführungen gem. Art. 6 DSGVO erforderlich. In „informierter Weise" ist eine Zustimmung nur dann, wenn die Informationen „leicht zugänglich und deutlich von anderen Sachverhalten klar zu unterscheiden sind. Insbesondere dürfen die Informationen nicht in AGB „versteckt" werden (BeckOK DatenschutzR/Albers/Veit, 42. Ed. 1.11.2021,

DS-GVO Art. 6 Rn. 29-39). Davon könnte hier keine Rede sein, wenn sich die Information (wenn überhaupt) nur unter einem Unterlink finden lässt, der aus der Datenschutzrichtlinie heraus führt und der zudem nach der gewählten Bezeichnung („Mehr dazu, wie Du die Informationen über dich kontrollieren kannst, die du mit diesen Apps und Webseiten teilst bzw. die andere teilen") keinerlei Anhaltspunkte dahingehend enthält, dass dort auch Informationen zur Nutzung der Mobilfunknummer aufzufinden sein könnten, von der zum Zeitpunkt der Registrierung gerade nicht anzunehmen war, dass diese öffentlich geteilt würde.

Nichts Anderes folgt im Übrigen aus dem Umstand, dass den Nutzerinnen und Nutzern auf diversen Unterseiten nach der Registrierung Möglichkeiten angeboten werden, die Voreinstellungen zu ändern. Denn, wie oben dargelegt, erfordert die DSGVO nicht die bloße Möglichkeit, Voreinstellungen nachträglich zu ändern, sondern die aktive und eindeutige Einwilligung von Anfang an. Nachdem eine solche Einwilligung hier aus den dargelegten Gründen nicht gegeben ist, kommt es auch nicht darauf an, ob die angebotenen Möglichkeiten der nachträglichen Änderungen hinreichend einfach und übersichtlich zu finden waren. Soweit hierzu bereits entgegengesetzte Rechtsprechung existiert, überzeugt diese nicht. Die dem Gericht bekannten vorliegenden Entscheidungen prüfen insoweit regelmäßig lediglich pauschal, ob die in der Gesamtbetrachtung vorliegenden Informationen zur Nutzung der Telefonnummer zur Auffindbarkeit hinreichend transparent und klar sind (vgl. etwa LG Ellwangen Urteil vom 25. Januar 2023 - 2 O 198/22 -, GRUR-RS 2023, 1146, Rn. 62; LG Kiel Urteil vom 12. Januar 2023 - 6 O 154/22 -, GRUR-RS 2023, 328, Rn. 38). Dabei wird nicht unterschieden, welche Informationen im Kontext der Registrierung erteilt werden und welche Informationen in anderem Kontext ggf. auf der Seite auffindbar wären. Damit stellen sich diese Entscheidungen im Ergebnis in Widerspruch zu den oben aufgezeigten Anforderungen an eine aktive und eindeutige Zustimmung zu der fraglichen Datenverarbeitung.

Die hier beanstandete Funktion der Suchbarkeit des Profils durch Dritte anhand der Mobilfunknummer war auch – ganz offensichtlich – nicht für die Erfüllung des zwischen den Parteien geschlossenen Vertrags erforderlich, Art. 6 Abs. 1 b DSGVO. Was mit dem Begriff der Erforderlichkeit dabei im Einzelnen gemeint ist, ist allerdings umstritten (vgl. eingehend etwa BeckOK DatenschutzR/Albers/Veit, 43. Ed. 1.2.2023, DS-GVO Art. 6 Rn. 40-47). Klar ist jedoch, dass jedenfalls dann keine Erforderlichkeit im Sinne der DSGVO angenommen werden kann, wenn die konkret in Frage stehende Datenverarbeitung für die Erfüllung des konkreten Vertrages jedenfalls in keiner Weise notwendig, sondern allenfalls irgendwie „nützlich" oder „dienlich" ist

(Ehmann/Selmayr/Heberlein, 2. Aufl. 2018, DS-GVO Art. 6 Rn. 13, 14; BeckOK DatenschutzR/Albers/Veit, 43. Ed. 1.2.2023, DS-GVO Art. 6 Rn. 40-47; Kühling/Buchner/Buchner/Petri, 3. Aufl. 2020, DS-GVO Art. 6 Rn. 42-44). Dies ist hier ersichtlich der Fall, da die Auffindbarkeit der jeweiligen Profile anhand der hinterlegten Mobilfunk-Nummer für die Vertragsabwicklung vorliegend allenfalls nützlich, keinesfalls aber notwendig war. Schon der bloße Umstand, dass die Nutzerinnen und Nutzer die fragliche Funktion in ihren Profileinstellungen deaktivieren konnten ohne dass die Vertragsdurchführung hierdurch von auch nur einer der Parteien als in Frage gestellt gesehen wurde, zeigt, dass es sich um eine möglicherweise praktische aber eben nicht irgendwie notwendige Funktion handelt. Vielmehr erleichtert die Funktion den Nutzerinnen, die dies wünschen, die bessere Vernetzung mit anderen Nutzerinnen und Nutzern, schließt aber eine sinnvolle Nutzung der vielfältigen Nutzungsangebote von Facebook auch bei der Deaktivierung dieser Funktion in keiner Weise aus

Des Weiteren ist auch nicht festzustellen, dass die streitgegenständliche Datenverarbeitung zur Wahrung der berechtigten Interessen der Klägerseite oder Dritten erforderlich war (Art. 82 ABs. 1 f DSGVO). Gleiches gilt für Art. 6 Abs. 1 f DSGVO. Berechtigte Interessen der Beklagten, zu deren Wahrung die Funktion erforderlich wäre, sind nicht festzustellen.

Ferner stellt das Gericht einen unzureichenden Schutz der streitgegenständlichen Daten der Klägerseite durch die Beklagte fest. Die Beklagte hat gegen ihre Pflichten aus Art. 32 DSGVO zur Ergreifung geeigneter technischer und organisatorischer Schutzmaßnahmen verstoßen.

Eine Verletzung von Art. 32 DSGVO ist dabei generell vom Schutzbereich des Art. 82 DSGVO umfasst. Ein Verstoß kann daher die Schadensersatzpflicht nach Art. 82 DSGVO begründen (vgl. nur Kühling/Buchner/Jandt DS-GVO Art. 32 Rn. 40a).

Es liegt auch ein derartiger, haftungsbegründender Verstoß vor.

Nach Art. 32 Abs. 1 Hs. 1 DSGVO haben der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahr-

scheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Das Gebot soll insbesondere personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen davor schützen, dass Dritte diese unbefugt oder unrechtmäßig verarbeiten oder es unbeabsichtigt zu einem Verlust, einer Zerstörung oder Schädigung der Daten kommt (Paal/Pauly/Martini, 3. Aufl. 2021, DSGVO Art. 32 Rn. 2; vgl auch Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DSGVO Art. 32 Rn. 2). Bezüglich der vorzunehmenden Maßnahmen sind der Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung und die jeweilige Eintrittswahrscheinlichkeit sowie das Risiko für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Je höher die drohenden Schäden sind, desto wirksamer müssen die zu ergreifenden Maßnahmen sein (Kühling/Buchner/Jandt DS-GVO Art. 32 Rn. 7-13). Ausweislich des Erwägungsgrunds 76 zur DSGVO sollten dabei die Eintrittswahrscheinlichkeit und Schwere des Risikos anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt (vgl. auch LG Berlin, Urteil vom 14. März 2023 - 56 O 75/22 -, nicht veröffentlicht).

Im vorliegenden Fall ist dabei zur Überzeugung des Gerichts an die vorzunehmenden Maßnahmen und das damit verbundene notwendige Schutzniveau ein hoher Maßstab anzusetzen. Dies ergibt sich zum einen daraus, dass im Falle von Scraping nicht lediglich Daten erhoben werden, die ohnehin öffentlich zugänglich sind. Vielmehr wird durch die Scraping-Angriffe eine Verknüpfung zu dem Konto des Betroffenen und der darin erhaltenen Daten erstellt und somit ein ganzes Datenpaket einschließlich der zuvor nicht öffentlich einsehbaren Telefonnummer zusammengestellt. Die Gefahr, dass diese Daten sodann einschließlich der Telefonnummer massenhaft durch Dritte veröffentlicht werden, ist – wie auch der vorliegende Fall zeigt – besonders hoch (vgl. auch LG Paderborn, Urteil vom 19. Dezember 2022 - 3 O 99/22 -, juris). Gerade bei weltweit genutzten sozialen Netzwerken wie demjenigen der Beklagten ist „Scraping" dabei auch aus einer ex-ante-Sicht zu erwarten gewesen (vgl. LG Berlin, Urteil vom 14. März 2023 - 56 O 75/22 -, nicht veröffentlicht). Der Beklagten war diese Thematik auch bekannt. Bereits in ihrem Artikel vom 6. April 2021 (Anlage B 10) beschäftigte sie sich hiermit und berichtete über das Scraping als „gängige Taktik". Ebenfalls thematisierte sie, dass bereits 2019 darüber berichtet worden war. Darüber hinaus ist gerade bei einem Unternehmen in der Größenordnung der Beklagten davon auszugehen, dass sie grundsätzlich die Möglichkeit hat, geeignete technische Maßnahmen zum Schutz gegen Scraping zu ergreifen. Dies ist ferner sowohl dem oben genannten

Artikel, als auch dem Vortrag der Beklagten zu den Maßnahmen zu entnehmen. Insoweit führt sie beispielsweise selbst aus, dass eine Übertragungsbeschränkung oder das Einrichten von Captcha-Anfragen stattgefunden habe.

Die Kammer geht davon aus, dass die Beklagte vorliegend jedoch keine diesen Anforderungen genügenden Schutzmaßnahmen ergriffen hat.

Die Beklagte trifft insoweit eine sekundäre Darlegungslast, zu den von ihr aufgeführten Schutzmaßnahmen konkret vorzutragen (so auch LG Frankfurt am Main, Urteil vom 21. März 2023 - 2-18 O 114/22 -, nicht veröffentlicht; OLG Stuttgart, Urteil vom 31. März 2021 – 9 U 34/21 –, juris). Eine sekundäre Darlegungslast trifft den Prozessgegner der primär darlegungsbelasteten Partei, wenn diese keine nähere Kenntnis der maßgeblichen Umstände und auch keine Möglichkeit zur weiteren Sachaufklärung hat, während der Bestreitende alle wesentlichen Tatsachen kennt und es ihm unschwer möglich und zumutbar ist, nähere Angaben zu machen (BGH, Urteil vom 10. Februar 2015 – VI ZR 343/13 –, juris). So liegt es im hiesigen Fall, da es der Beklagten ohne weiteres möglich ist, darzulegen, welche konkreten Maßnahmen zum Schutz der Daten ergriffen wurden. Demgegenüber hat die Klägerseite als Außenstehende keine Kenntnis über die konkret implementierten Maßnahmen.

Die Beklagte hat zu den notwendigen und ergriffenen Maßnahmen jedoch nicht ausreichend vorgetragen. Sie hat nicht hinreichend dargelegt, welche konkreten Maßnahmen sie überhaupt angewandt hat und wie genau diese ausgestaltet gewesen sein sollen. Insbesondere der pauschale Vortrag, es seien Übertragungsbeschränkungen eingeführt und Captcha-Anfragen genutzt worden, ist einer konkreten Prüfung, ob diese Maßnahmen auch dem erhöhten Maßstab der Sicherungsmaßnahmen genügen, nicht zugänglich, da weder hinreichend zu der Funktionsweise noch zu der konkreten Ausgestaltung vorgetragen wurde. Dieser ungenügende Vortrag wurde auch nach richterlichem Hinweis in der mündlichen Verhandlung nicht weiter präzisiert. Ihrer Darlegungslast wird die Beklagte weder durch einen pauschalen Verweis auf angebliche Geschäftsgeheimnisse bzgl. der Übertragungsbeschränkungen gerecht, noch durch den nicht einlassungsfähigen Vortrag, es seien neben den Übertragungsbeschränkungen noch eine Reihe weiterer, im Einzelnen aber unklar bleibender, Maßnahmen ergriffen worden. Bei einer Berufung auf die Wahrung von Betriebs- und Geschäftsgeheimnissen hat der Betroffene im Prozess nachvollziehbar und substantiiert darzulegen, welche konkreten Nachteile bei der Preisgabe welcher konkre-

ten Geheimnisse zu befürchten seien (OLG Köln, Urteil vom 5. November 2020 – I-7 U 35/20 –, juris). Die Angaben der Beklagten sind aufgrund ihrer Pauschalität und gemessen an diesem Maßstab nicht geeignet, eine konkrete Gefährdung von Geschäftsgeheimnissen zu plausibilisieren.

Soweit die Beklagte darüber hinaus vorträgt, sie gehe nun mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren gegen Scraper vor, handelt es sich bei diesen Maßnahmen augenscheinlich um solche, die erst nach dem erfolgten Scraping-Vorfall ergriffen wurden und die demnach zum hier streitgegenständlichen Zeitpunkt noch nicht im Einsatz waren.

Soweit die Beklagte vorträgt, den „Social Connection Check" eingeführt oder die Kontakt-Importer-Funktion durch die PYMK-Funktion ersetzt zu haben, handelt es sich um solche Maßnahmen, welche nach ihrem Vortrag erst im Nachgang und damit nach dem streitgegenständlichen Vorfall ergriffen wurden. Weiterhin enthält der Vortrag der Beklagten diesbezüglich keine hinreichende Auseinandersetzung damit, aus welchen Gründen diese Maßnahmen nicht bereits vor dem streitgegenständlichen Vorfall ergriffen worden sind. Dies ist insbesondere auch unter dem Gesichtspunkt relevant, dass der Beklagten – wie oben bereits dargelegt – das Problem des Scrapings als „gängige Taktik" bekannt war (vgl. auch LG Frankfurt am Main, Urteil vom 21. März 2023 – 2-18 O 114/22-, nicht veröffentlicht).

Hingegen vermag das Gericht keine Haftung der Beklagten wegen einer etwaigen Verletzung des Grundsatzes „privacy by design" bzw. „privacy by default" zu erkennen. Mit den überzeugenden Argumenten des Landgerichts Paderborn (Urteil vom 19. Dezember 2022 - 3 O 99/22 -, GRUR-RS 2022, 39349) spricht insoweit zwar viel dafür, dass insoweit ein Verstoß gegen Art. 25 DSGVO vorliegen dürfte:

„Art. 25 Abs. 1 DSGVO verpflichtet den Verantwortlichen bereits bei der Entwicklung von Produkten, Diensten und Anwendungen sicherzustellen, dass die Anforderungen der DSGVO erfüllt werden („Privacy by Design"). Abs. 2 konkretisiert diese allgemeine Verpflichtung und verlangt, vorhandene Einstellungsmöglichkeiten standardmäßig auf die „datenschutzfreundlichsten" Voreinstellungen („Privacy by default") zu setzen (Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 3). „Datenschutz durch Voreinstellungen" soll insbesondere diejenigen Nutzer schützen, welche die datenschutztechnischen Implikationen der Verarbeitungsvorgänge entweder nicht zu erfassen in der Lage sind oder sich darüber keine Gedanken machen und sich deshalb auch nicht dazu veranlasst sehen, aus eigenem Antrieb datenschutzfreundliche Einstellungen vorzunehmen, obwohl der Telemediendienst ihnen diese Möglichkeit prinzipiell eröffnet

(Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 25 Rn. 13). Die Nutzer sollen keine Änderungen an den Einstellungen vornehmen müssen, um eine möglichst „datensparsame" Verarbeitung zu erreichen. Vielmehr soll umgekehrt jede Abweichung von den datenminimierenden Voreinstellungen erst durch ein aktives „Eingreifen" der Nutzer möglich werden. Die Regelung soll die Verfügungshoheit der Nutzer über ihre Daten sicherstellen und sie vor einer unbewussten Datenerhebung schützen. Abs. 2 verlangt aber nicht, dass der Verantwortliche stets die jeweils denkbar datenschutzfreundlichste Voreinstellung trifft. Der Verantwortliche entscheidet vielmehr durch die Festlegung eines bestimmten Verarbeitungszweckes auch über den Umfang der dafür erforderlichen Daten. Dem Wortlaut nach ist daher auch eine besonders datenintensive Voreinstellung mit Abs. 2 vereinbar, wenn der Zweck der Verarbeitung dies erfordert. Vor dem Hintergrund der Schutzrichtung des Abs. 2, den Nutzer vor einer Überrumpelung oder dem Ausnutzen seiner Unerfahrenheit zu schützen, muss der Verantwortliche aber stets sicherstellen, dass die geplante Datennutzung auch für einen nicht-technikaffinen Nutzer hinreichend transparent ist. (Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 18 f.).

Gegen diese Regelungen verstößt die Beklagte. Die G-Plattform der Beklagten sah standardmäßig vor, dass neben den verpflichtenden öffentlichen Daten (Name, Geschlecht, Nutzer-ID) auch weitere Angaben des Nutzers öffentlich einsehbar sind. Hier gehören einzelne Informationen auf seinem G-Profil, wie etwa Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse. Allein die Telefonnummer war standardmäßig nur für einen selbst bzw. Freunde einsehbar. Die „Suchbarkeits-Einstellungen" sahen jedoch in ihrer Standard-Voreinstellung unabhängig von der Einsehbarkeit der Telefonnummer vor, dass alle Personen mittels dieser die hinter den Nummern stehenden G-Profile finden konnten. Die Nutzer mussten selbst aktiv werden, um ihre Daten Dritten weniger zugänglich zu machen.

Diese Voreinstellungen entsprechen nicht den Anforderungen, die insbesondere Art. 25 Abs. 2 S. 3 DSGVO normiert. Die Vorschrift ist insbesondere auf soziale Netzwerke ausgerichtet (vgl. Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 20; Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DSGVO Art. 25 Rn. 28, 31; Spindler/Schuster/Spindler/Horváth, 4. Aufl. 2019, DS-GVO Art. 25 Rn. 12). Demnach muss sichergestellt sein, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Der Nutzer muss demnach die Möglichkeit haben, die Veröffentlichung seiner personenbezogenen Daten aktiv zu steuern. Übertragen auf die sozialen Netzwerke folgt daraus, dass der Nutzer selbst festlegen können muss, ob und mit wem er Inhalte innerhalb eines Netzwerks teilt.

Aus Abs. 2 S. 3 folgt in diesem Fall die Verpflichtung für den Betreiber des Netzwerks, die Default-Einstellungen so zu treffen, dass Inhalte der Nutzer nicht standardmäßig mit anderen Nutzern oder Dritten geteilt werden. Als Voreinstellung ist der kleinstmögliche Empfängerkreis vorzusehen (vgl. Ehmann/Selmayr/Baumgartner a.a.O.; Gola/Heckmann/Nolte/Werkmeister a.a.O; Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 25 Rn. 69). Entgegen der Ansicht der Beklagten darf es von den Nutzern nicht erforderlich sein, selbst aktiv individuelle Anpassungen zu machen, die erst dann zu einer geringeren Zugänglichkeit ihrer Daten führt. Es sind vielmehr Voreinstellungen zu treffen, die entgegengesetzt zum Vorgehen der Beklagten den Nutzern die Möglichkeit verschafft, ihre Angaben über den Personenkreis hinaus zugänglich zu machen, der standardmäßig vorgesehen ist. Alternativ ist auch die Gestaltung denkbar, die den Nutzer zu einer Entscheidung für oder gegen die Einsehbarkeit bzw. Suchbarkeit zwingt (Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 25 Rn. 69).

Die Voreinstellungen auf „Alle" in der Zielgruppenauswahl sowie für die Telefonnummer in den Suchbarkeits-Einstellungen lassen sich auch nicht für alle vom Nutzer angegebenen Daten mit dem von der Beklagten behaupteten Unternehmenszweck rechtfertigen. Der Unternehmenszweck der Beklagten besteht laut ihrer Angabe im hiesigen Verfahren darin, Menschen die Möglichkeit zu geben, Gemeinschaften zu bilden, und die Welt näher zusammenzubringen. Menschen würden die G-Plattform nutzen, um mit Freunden und Familie in Verbindung zu bleiben, um zu erfahren, was in der Welt vor sich geht, sowie um sich mit bedeutsamen Gemeinschaften und Anliegen, die ihnen wichtig sind, zu verknüpfen. Eine öffentliche Einsehbarkeit der persönlichen Daten wie Name, Geburtsdatum, Wohnort, Interessen etc. ließe sich zwar anhand des o.g. Zwecks erklären. Denn Nutzer finden Kontakte in sozialen Netzwerken in der Regel über Namen, geographische Nähe, gemeinsame Lebensabschnitte, z.B. während der Ausbildung oder der Berufsausübung, oder über gemeinsame Interessen.

Dies gilt jedoch nicht hinsichtlich der E-Mail-Adresse sowie die Suchfunktion über die Handynummer. Eine Kontaktaufnahme anhand der öffentlich einsehbaren E-Mail-Adresse erscheint der Kammer nach allgemeiner Lebenserfahrung als zumindest untypisch. Dies gilt ebenfalls über die Suche über die Telefonnummer. Soweit eine Person die Telefonnummer einer anderen Person bereits hat, ist eine Vernetzung dieser durch telefonische Kontaktaufnahme durchführbar. In diesem Rahmen ist es auch möglich, sich gegenseitig auf der G-Plattform zu finden. Eine Suchbarkeit über die Telefonnummer ist dann obsolet. Diese Einstellung sowie das „CIT" unterliegen - wie das „Datenscraping" aufzeigte - vielmehr einer Missbrauchsgefahr durch Dritte.

Nach alledem lässt sich zumindest für die Voreinstellungen der Beklagten über die Einsehbarkeit der E-Mail-Adresse und die Suchbarkeit über die Telefonnummer für „Alle" ein Verstoß ge-

gen Art. 25 DSGVO feststellen."

Jedoch wäre eine derartige Verletzung von Art. 25 DSGVO jedenfalls nicht vom Schutzbereich des Art. 82 DSGVO umfasst und kann daher keine Schadensersatzansprüche auslösen. Systematisch folgt dies bereits aus dem Umstand, dass Art. 82 Abs. 2 DSGVO voraussetzt, dass der Schaden „durch eine Verarbeitung" ausgelöst wurde, während Art. 25 DSGVO Verhaltenspflichten normiert, die vor jeder konkreten Datenverarbeitung liegen und die generellen Voreinstellungen betreffen (Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 25 Rn. 76, 77; so i.E. auch Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DS-GVO Art. 25 Rn. 34). Durch ein derartiges Verständnis der Art. 25, 82 DSGVO wird der Wirkungsbereich des Art. 25 DS-GVO dabei auch nicht in unzulässiger Weise eingeschränkt. Vielmehr werden eventuelle Verstöße gegen Art. 25 DSGVO bei diesem Verständnis auf Verschuldensebene relevant und hindern ggf. eine Entlastung des Normverpflichteten:

„Art. 25 Abs. 1 kommt aber besondere Bedeutung zu, wenn ein Schaden erst einmal eingetreten ist. Denn nach Art. 82 Abs. 3 wird der Verantwortliche (nur) von der Haftung frei, wenn er nachweist, dass er in keinerlei Hinsicht für den Schaden verantwortlich ist. Lässt sich aber ein Verstoß gegen Art. 25 Abs. 1 feststellen, zB weil der Verantwortliche Maßnahmen zur Risikominderung nicht ergriffen, Daten nicht (bzw. nicht rechtzeitig) pseudonymisiert, nicht erforderliche Daten erhoben oder nicht erforderliche Verarbeitungsvorgänge durchgeführt hat, dann ist ein Verschulden des Verantwortlichen allein hierdurch indiziert. Denn jedenfalls wohnt einem Verstoß gegen Art. 25 praktisch immer eine Erhöhung der Gefahr eines Schadens inne. Der Gegenbeweis nach Art. 82 Abs. 3 dürfte sich in einem solchen Fall als noch schwieriger darstellen." (Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 25 Rn. 76, 77).

Das vermag Gericht auch keine weiteren haftungsbegründenden Verstöße der Beklagten gegen die DSGVO im Hinblick auf die vorgetragenen Verletzungen von Informationspflichten zu erkennen. Es kann offenbleiben, ob - was nahe liegt - die Beklagte ihre Meldepflichten aus Art. 33, 34 DSGVO verletzt und weder die Aufsichtsbehörde gemäß Art. 33 DSGVO noch die Klägerseite entsprechend ihrer unverzüglich zu erfüllenden Verpflichtung aus Art. 34 Abs. 1 DSGVO informiert hat. Auf entsprechende Verstöße lässt sich ein immaterieller Schadensersatzanspruch vorliegend jedenfalls nicht stützen, weil nicht zur Überzeugung der Kammer festgestellt werden kann, dass die etwaige Verletzung dieser Pflichten für den geltend gemachten Schaden der Klägerseite überhaupt (mit-)kausal geworden ist und diesen zumindest vertieft hat. Vielmehr ist das streitgegenständliche Scraping der Daten mit der öffentlichen Einstellung der Daten im Internet erstmals offenbar geworden. Dass eine in der Folge unterlassene Information hierüber den da-

mit bereits eingetretenen Schaden in Gestalt der Verletzung des allgemeinen Persönlichkeitsrechtes der Klägerseite konkret weiter vertieft hätte, lässt sich bei dieser Sachlage nicht feststellen. Insbesondere ist nicht ersichtlich, dass der Gefahr, dass die bereits rechtswidrig zirkulierenden Daten auch auf weiteren Seiten angeboten werden, zum Zeitpunkt der unterstellt unterlassenen Information überhaupt noch hätte begegnet werden können (a.A. LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 140: Möglichkeit genommen, geeignete Maßnahmen zu ergreifen, um das Risiko des Missbrauchs seiner Daten zu minimieren).

Soweit nach den obigen Ausführungen haftungsbegründende Verletzungen der DSGVO vorliegen, sind diese auch von der Beklagten zu vertreten.

Dabei kann für das vorliegende Verfahren dahinstehen, ob Art. 82 DSGVO eine verschuldensunabhängige Haftung begründet (BAG, EuGH-Vorlage vom 26. August 2021 - 8 AZR 253/20 (A) -, juris Rn. 40), eine Gefährdungshaftung mit der bloßen Möglichkeit der rechtsvernichtenden Einwendung fehlenden Verschuldens (vgl. hierzu etwa BeckOK DatenschutzR/Quaas DS-GVO Art. 82 Rn. 17-22) oder ob mit der wohl h.M. angenommen werden kann, Art. 82 Abs. 3 DSGVO enthalte ein Verschuldenserfordernis im Sinne der gängigen deutschen Terminologie mit einer entsprechenden Vermutung zu Lasten des Normverletzers und einer bei dem Verpflichteten liegenden Beweislast, dass weder Vorsatz noch Fahrlässigkeit vorlag (vgl. etwa BeckOK DatenschutzR/Quaas DS-GVO Art. 82 Rn. 17-22; Ehmann/Selmayr/Nemitz, 2. Aufl. 2018, DS-GVO Art. 82 Rn. 14, 15; so wohl auch: Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Artikel 82 Haftung und Recht auf Schadenersatz; EuArbRK/Franzen, 4. Aufl. 2022, EU (VO) 2016/679 Art. 82 Rn. 17, 18; Gola/Heckmann/Gola/Piltz, 3. Aufl. 2022, DS-GVO Art. 82 Rn. 24-26).

Denn selbst wenn Art. 82 DSGVO eine Exkulpationsmöglichkeit nach gängiger deutscher Terminologie zukommen würde, wäre der Beklagten eine Exkulpation nicht gelungen. Im Hinblick auf die rechtwidrige Verarbeitung der einschlägigen Daten der Klägerseite ist nichts zu erkennen, was die Beklagte zu Exkulpation vortragen könnte. Die konkrete Konfiguration der Voreinstellungen in den Profilen war ebenso wie die technischen Funktionen zur Nutzung der Mobilfunkdaten von der Beklagten im Rahmen ihres Geschäftsbetriebes offenkundig bewusst so verfasst wie oben beschrieben. Insoweit liegt entsprechend zumindest Fährlässigkeit vor. Dies gilt auch für die fehlende Erfüllung der Sorgfaltsanforderungen. Auch insoweit ist jedenfalls Fahrlässigkeit zu vermuten. Einlassungsfähiger Vortrag, der dem Fahrlässigkeitsvorwurf entkräften könnte, setzte zumindest voraus, dass dargelegt wird, aufgrund welcher konkreter Erkenntnisse man ex ante davon hätte ausgehen dürfen, dass die – nicht einlassungsfähig vorgetragenen (vgl. oben) – Maß-

nahmen zur Erfüllung des Art. 32 DSGVO ausreichend sein könnten. Derartiges hat die Beklagte nicht vorgetragen.

Des Weiteren liegt auch ein ersatzfähiger Schaden im Sinne von Art. 82 Abs. 1 DSGVO vor.

Grundsätzlich ermöglicht Art. 82 Abs. 1 DSGVO den Ersatz materieller und immaterieller Schäden. Ein materieller Vermögensschaden i.S.v. § 249 BGB wurde von der Klägerseite nicht vorgetragen. Sie beruft sich jedoch erfolgreich auf das Vorliegen eines immateriellen Schadens. Ein immaterieller Schaden liegt dabei zwar nicht schon in der bloßen Verletzung einer Norm der DSGVO (EuGH, Urteil vom 4. Mai 2023 - C-300/21 -, juris). Jedoch liegt ein immaterieller Schaden vor, wenn infolge der Verletzung der Norm der DSGVO ein absolut geschütztes Rechtsgut der geschädigten Person verletzt wurde. In Betracht kommt insoweit etwa eine Verletzung des Rechts auf körperliche Unversehrtheit ebenso wie eine Verletzung des Rechts auf informationelle Selbstbestimmung als besondere und ebenfalls absolut geschützte Ausprägung des allgemeinen Persönlichkeitsrechts (vgl. zur Bejahung eines Schadens im Sinne des Art. 82 DSGVO bei Verletzung des allgemeinen Persönlichkeitsrechts etwa EuArbRK/Franzen, 4. Aufl. 2022, EU (VO) 2016/679 Art. 82 Rn. 19ff.). Entsprechend ist insbesondere auch in der deutschen Rechtsprechung anerkannt, dass eine Verletzung des allgemeinen Persönlichkeitsrechts einen Schaden im Sinne des Art. 82 DSGVO darstellen kann. Streitig war bis zuletzt nur, ob diese Verletzung eine gewisse Erheblichkeitsschwelle überschreiten muss (für eine Erheblichkeitsschwelle etwa OLG Dresden, Hinweisbeschluss vom 11. Juni 2019 - 4 U 760/19 (LG Görlitz) -, ZD 2019, 567; gegen eine Erheblichkeitsprüfung etwa EuArbRK/Franzen, 4. Aufl. 2022, EU (VO) 2016/679 Art. 82 Rn. 19ff.; BeckOK DatenschutzR/Quaas DS-GVO Art. 82 Rn. 31-36; LAG Baden-Württemberg, Urteil vom 25. Februar 2021 - 17 Sa 37/20 -, BeckRS 2021, 5529) oder ob zumindest „ganz unerhebliche" Verletzungen im Sinne einer Bagatelle ausscheiden sollten (EuArbRK/Franzen, 4. Aufl. 2022, EU (VO) 2016/679 Art. 82 Rn. 19-22; Paal, MMR 2020, 14, 16, mit weiterer Rspr. auch Wybitul, NJW 2021, 1190; OLG Dresden, Hinweisbeschluss vom 11. Juni 2019 - 4 U 760/19 (LG Görlitz) -, ZD 2019, 567) – wobei diese Frage nunmehr durch den Europäischen Gerichtshof dahingehend beantwortet wurde, dass keine Erheblichkeitsprüfung durchzuführen ist (EuGH, a.a.O.).

Eine für die Bejahung eines Schadens damit ausreichende Verletzung des allgemeinen Persönlichkeitsrechts in der Ausprägung des Rechts auf informationelle Selbstbestimmung liegt hier vor. Das auch im Zivilrecht deliktrechtlich über § 823 BGB und im Datenschutzrecht durch Art.

82 DSGVO geschützte Recht auf informationelle Selbstbestimmung enthält die „Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden" (vgl. hierzu im Einzelnen BeckOGK/Specht-Riemenschneider, 1.2.2023, BGB § 823 Rn. 1365-1383). Dieses Recht der Klägerseite wurde und wird bis heute fortlaufend verletzt. Infolge der obigen Verstöße gegen die einschlägigen Bestimmungen der DSGVO gelangten die streitgegenständlichen Daten inzwischen unstreitig auf jedenfalls eine online betriebene Seite, auf der sie öffentlich gemacht worden sind und damit fortgesetzt das geschützte Recht der Klägerseite verletzen, selbst zu entscheiden, wo und ob sie diese Daten offenbaren möchte. Dieser Verletzung misst das Gericht dabei auch ein erhebliches Gewicht zu, da die Daten der Klägerseite im „Paket" mit den Daten Millionen anderer Nutzer und Nutzerinnen angeboten werden, was den derart generierten „Datenpaketen" einen entsprechend höheren Nutzwert für kriminell handelnde Dritte zukommen lässt und was entsprechend die Intensität der Persönlichkeitsrechtsverletzung und die Gefahr von Weiterungen steigert.

Wie sich die Klägerseite dabei fühlt, ist nach der Auffassung des Gerichts für das Vorliegen eines Schadens unerheblich, da ein solcher bereits in der tatsächlich stattfindenden (und nicht nur befürchteten) Persönlichkeitsrechtsverletzung durch Dritte liegt. Ein Abstellen auf die emotionale Befindlichkeit der Klägerseite wäre nur dann erheblich, wenn die Rechtsgutverletzung maßgeblich in einer Verletzung des Rechts auf körperliche Unversehrtheit zu sehen wäre. Dies ist jedoch nicht der Fall, da – wie dargelegt – bereits eine haftungsbegründende Verletzung des Rechts auf informationelle Selbstbestimmung vorliegt, neben der der begleitenden Befindlichkeit der Klägerseite keine weitere haftungssteigernde Relevanz zukommt.

Der Schaden beruht kausal (vgl. zu der str. Erforderlichkeit dieses Tatbestandsmerkmals nur BeckOK DatenschutzR/Quaas, 42. Ed. 1.8.2022, DS-GVO Art. 82 Rn. 26-27) auf den oben festgestellten Verstößen.

Im Hinblick auf die rechtswidrige Verarbeitung der klägerischen Daten liegt die erforderliche Kausalität vor. Der von der Klägerseite bemühten Überlegungen zur Beweislastverteilung analog der Rechtsprechung zum hinweisgerechten Verhalten bedarf es dafür nicht. Anknüpfungspunkt für die Kausalität ist insoweit – anders als in den Fällen aus der Rechtsprechung zum hinweisgerechten Verhalten – nicht die fehlende Aufklärung, sondern die wegen der fehlenden Einwilligung rechtswidrige Datenverarbeitung in Form des Betreibens der streitgegenständlichen Funktion. Hieraus folgt, dass die Kausalität zwischen DSGVO-Verletzung und Schaden gegeben ist: Hätte

es die Beklagte unterlassen, die mangels Einwilligung rechtswidrige Funktion der Profilidentifikation anhand Telefonnummer Dritten zur Verfügung zu stellen, wäre es nicht zu dem Schaden gekommen (so auch überzeugend das LG Paderborn (LG Paderborn Urteil vom 19. Dezember 2022 - 3 O 99/22 -, GRUR-RS 2022, 39349, Rn. 127 ff.):

„Die gemäß den vorstehenden Ausführungen festgestellten Gesetzesverletzungen sind kausal für den bei dem Kläger entstandenen Schaden. Der Verantwortliche haftet lediglich für kausal durch die rechtswidrige Verarbeitung verursachte Schäden (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 41). Eine Mitursächlichkeit des Verstoßes genügt (OLG Stuttgart ZD 2021, 375; LG Köln ZD 2022, 52 Rn. 21). Die Verletzung der Informations- und Aufklärungspflichten des Art. 13 Abs. 1 lit. c) DSGVO ist kausal für den bei dem Kläger entstandenen Schaden. Gemäß vorstehender Erwägungen hat die Beklagte den Kläger bereits bei Erhebung seiner Mobilfunknummer nur unzureichend über die Verwendung seiner Mobilfunknummer im Hinblick auf das CIT aufgeklärt, sodass bezogen auf die Mobilfunknummer eine rechtswidrige Verarbeitung vorliegt. Diese ist auch kausal für den beim Kläger entstandenen Schaden, da es durch die Verwendung des CIT zu einem Kontrollverlust auf Seiten des Klägers kam."

Gleiches gilt für die Kausalität zwischen dem unzureichenden Schutz der streitgegenständlichen Daten und dem Schaden. Durch die unzureichenden Maßnahmen wurde das Scraping ermöglicht bzw. zumindest erleichtert. Dies hat zu einem Kontrollverlust im Hinblick auf die Daten und letztlich zu dem festgestellten Schaden geführt. Es liegt daher zumindest Mitursächlichkeit vor.

Soweit die Beklagte im Übrigen vorträgt, die Mobilfunknummer der Klägerseite sei bereits zuvor im Internet öffentlich zugänglich gewesen, ändert dies nichts daran, dass die hier streitgegenständlichen Daten aufgrund des Scraping-Vorfalls veröffentlicht wurden. Dass bestimmte Daten der Klägerseite bereits öffentlich zugänglich waren, lässt diesen kausalen Zusammenhang nicht entfallen.

Die Höhe des Schadensersatzes beziffert das Gericht mit 500,00 €, wobei es diesen Betrag für angemessen, aber auch für ausreichend hält, um den immateriellen Schaden auszugleichen und gleichzeitig der erforderlichen Abschreckungswirkung Rechnung zu tragen sowie dabei die besonderen Umstände des Falles zu würdigen. Dem Gericht steht insoweit gemäß § 287 ZPO ein Ermessen zu.

Es gelten für die Bemessung der Höhe des immateriellen Schadens die Grundsätze des § 253 BGB. Auch herangezogen werden können dabei die Kriterien des Art. 83 Abs. 2 DSGVO. Darunter zählen bspw. die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung, der Grad des Verschuldens, Maßnahmen zur Minderung des entstandenen Schadens, frühere Verstöße sowie die Kategorien der betroffenen personenbezogenen Daten, die betroffenen Kategorien personenbezogener Daten zur Ermittlung (BeckOK DatenschutzR/Quaas DS-GVO Art. 82 Rn. 31-36).

Im vorliegenden Fall war insbesondere zu berücksichtigen, dass die Beklagte mehrere Verstöße gegen die DSGVO begangen hat, in welchem Umfang die Daten der Klägerseite „gescrapt" wurden, und dass diese veröffentlicht wurden. Auf der anderen Seite war heranzuziehen, dass es sich mit Ausnahme der Mobilfunknummer um bereits öffentlich zugängliche Daten der Klägerseite handelte, die weder besonders schutzwürdig noch intimen waren. Ebenfalls ist es (bislang) nicht zu einer konkreten Vermögensgefährdung oder -schädigung gekommen.

Der Antrag zu 1., soweit er immateriellen Schadensersatz im Zusammenhang mit der etwaigen Verletzung des Auskunftsanspruchs der Klägerseite gemäß Art. 15 DSGVO betrifft, ist unbegründet. Die Klägerseite kann von der Beklagten aus § 82 DSGVO insoweit keine Zahlung immateriellen Schadensersatzes verlangen. Es lässt sich bereits eine Verletzung des Auskunftsanspruches durch die Beklagte nicht feststellen.

Nach Art. 15 DSGVO kann die betroffene Person Auskunft über personenbezogenen Daten verlangen, wenn der Verantwortliche sie betreffende personenbezogene Daten verarbeitet. Art. 15 DSGVO enthält dabei vier Anspruchsinhalte. Nach Art. 15 Abs. 1 Hs. 1 DSGVO besteht ein Anspruch auf Auskunft bzw. eine Bestätigung, ob der Verantwortliche personenbezogene Daten der betroffenen Person verarbeitet. Gemäß Art. 15 Abs. 1 Hs. 2 Teil 1 DSGVO besteht Anspruch auf Auskunft über die personenbezogenen Daten, die in Bezug auf die betroffene Person vom Verantwortlichen verarbeitet werden. Art. 15 Abs. 2 DSGVO sieht einen Anspruch auf die in Art. 15 Abs. 1 Hs. 2 Teil 2 Buchst. a bis h DSGVO im Einzelnen genannten Meta-Informationen (Verarbeitungszwecke, Datenkategorien, Empfänger(kategorien), Speicherdauer, Herkunft der Daten etc.) und auf Unterrichtung über geeignete Garantien gem. Art. 46 DSGVO bei Übermittlung in ein Drittland vor. Zuletzt besteht gemäß Art. 15 Abs. 3 S. 1 DSGVO ein Anspruch auf Zurverfügungstellung einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind.

Gemessen hieran hatte die Klägerseite bereits dem Umfange nach überwiegend keinen Anspruch auf die vorgerichtlich begehrten Informationen. Die begehrten Informationen werden weit überwiegend nicht vom Anwendungsbereich Art. 15 DSGVO erfasst. Im Einzelnen:

Soweit Information darüber begehrt wurden, ob personenbezogene Informationen durch die Beklagte verarbeitet werden und zu welchem Zweck bzw. welchen Zwecken, lässt sich dieser Anspruch auf Art. 15 Abs. 1 Hs. 2 vor lit. a) sowie Art 15 Abs. 1 Hs. 2 lit. a) DSGVO stützen.

Soweit die Klägerseite wissen wollte, ob die „Sicherheitslücke durch mehrere Unbefugte ausgenutzt [wurde], [s]ofern ja, von wem?", kann im Ausgangspunkt ein Anspruch gemäß Art 15 Abs. 1 Hs. 2 lit. c) bestehen.

Danach besteht ein Auskunftsrecht der betroffenen Person auch hinsichtlich der Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen. Dabei ist Art. 15 Abs. 1 Hs. 2 lit. c) DSGVO dahin auszulegen, dass das in dieser Bestimmung vorgesehene Recht der betroffenen Person auf Auskunft über die sie betreffenden personenbezogenen Daten bedingt, dass der Verantwortliche, wenn diese Daten gegenüber Empfängern offengelegt worden sind oder noch offengelegt werden, verpflichtet ist, der betroffenen Person die Identität der Empfänger mitzuteilen, es sei denn, dass es nicht möglich ist, die Empfänger zu identifizieren, oder dass der Verantwortliche nachweist, dass die Anträge auf Auskunft der betroffenen Person offenkundig unbegründet oder exzessiv im Sinne von Art. 12 Abs. 5 DSGVO sind; in diesem Fall kann der Verantwortliche der betroffenen Person lediglich die Kategorien der betreffenden Empfänger mitteilen (EuGH, Urteil vom 12.01.2023, C-154/21, Celex-Nr. 62021CJ0154, Rz. 51).

Soweit der Anspruch nach den obigen Ausführungen bestehen kann, ist er durch Erfüllung erloschen, § 362 Abs. 1 BGB.

Mit Schreiben vom 23.08.2021 (Anlage K 2) hat die Beklagte in angemessener Weise mitgeteilt, welche personenbezogenen Daten verarbeitet werden, indem sie die Klägerseite auf die Selbstbedienungstools verwiesen hat. Diese Erfüllungshandlung war ausreichend um den Erfüllungserfolg zu gewährleisten. Auch hat sie ausführlich auf die Zwecke der Datenverarbeitung hingewiesen. Hinsichtlich der begehrten Information zu den „unbefugten" Empfängern der auf dem Nutzerprofil im Internet bereitgestellten Daten hat sich die Beklagte zulässigerweise auf die Mitteilung ei-

ner Kategorie von potentiellen Empfängern beschränkt. In dem Schreiben hat sie hinsichtlich des Personenkreises mitgeteilt, dass jedermann auf die allein betroffenen öffentlich zugänglichen Informationen Zugriff hatte bzw. hätte haben können, und, dass das „Scraping" durch unbekannte Dritte erfolgt sei. Ferner hat sie ausgeführt, dass die Informationen durch sog. Scraping öffentlich abrufbarer Profilinformationen von Facebook-Nutzerprofilen im Zeitraum bis September 2019 erlangt wurden, wobei Funktionen verwendet worden seien, die es ordnungsgemäßen Nutzern ermöglichen sollen, diese Informationen einzusehen. Die Beschränkung auf Kategorien von Empfängern (jedermann) ist bei dieser Sachlage, zumal dem unbekannten genauen Zeitpunkt auch gemessen an den durch den EuGH aufgestellten Anforderungen zulässig, nachdem es bereits tatsächlich unmöglich ist, die „unbefugten" Empfänger der personenbezogenen Daten zu identifizieren. Vor dem Hintergrund, dass die Daten unstreitig auch bei einer befugten Nutzung eingesehen werden konnten, vermag eine Auskunft dahingehend nicht zu erfolgen, welcher Nutzer im Einklang und welcher Nutzer unter Verstoß gegen die Nutzungsbedingungen handelte. Entsprechendes lässt sich entgegen der Auffassung der Klägerseite ersichtlich auch etwaigen Log-Dateien nicht entnehmen, nachdem – selbst unterstellt diese enthielten Informationen über „Telefonabgleiche" – auch daraus nicht darauf geschlossen werden könnte, ob der jeweilige Empfänger „unbefugt" handelt. Die Beklagte hat mithin, indem sie mitteilte, dass jedermann Zugriff hätte haben können, hinreichend Auskunft zu der Kategorie der möglichen unbefugten Empfänger erteilt.

Der Klageantrag zu 2. ist begründet. Die Klägerseite hat Anspruch auf Feststellung der Eintrittspflicht für künftige materielle Schäden.

Begründet ist ein Feststellungsantrag, wenn die sachlichen und rechtlichen Voraussetzungen eines Schadensersatzanspruchs vorliegen, also ein haftungsrechtlich relevanter Eingriff gegeben ist, der zu möglichen künftigen Schäden führen kann.

Diese Voraussetzungen liegen vor.

Eine gewisse Wahrscheinlichkeit des Schadenseinstritts ist darüber hinaus nicht erforderlich.

Ob im Rahmen der Begründetheit zusätzlich eine gewisse Wahrscheinlichkeit des Schadenseintritts zu verlangen ist, hat der Bundesgerichtshof bislang weitgehend offengelassen. Er hat für die vorliegende Konstellation der Verletzung eines absoluten Rechtes – hier betroffen in Gestalt des allgemeinen Persönlichkeitsrechtes in der Ausprägung des Rechtes auf informationelle

Selbstbestimmung - klargestellt, dass jedenfalls in Fällen, in denen die Verletzung eines u.a. durch § 823 Abs. 1 BGB geschützten absoluten Rechtsguts und darüber hinaus ein daraus resultierender Vermögensschaden bereits eingetreten sind, die Begründetheit einer Klage, die auf die Feststellung der Ersatzpflicht für weitere, künftige Schäden gerichtet ist, nicht von der Wahrscheinlichkeit des Eintritts dieser Schäden abhängig ist (BGH, Urteil vom 17.10.2017 – VI ZR 423/16 -, NJW 2018, 1242 Rz. 49).

Auch im vorliegenden Fall ist eine gewisse Wahrscheinlichkeit nicht zu fordern.

Zur Begründung hat der BGH für die von ihm entschiedene Konstellation angeführt, es gebe keinen Grund, die Feststellung der Ersatzpflicht für weitere, künftige Schäden von der Wahrscheinlichkeit ihres Eintritts abhängig zu machen. Materiell-rechtlich würde es den Anspruch auf Ersatz dieser Schäden ohnehin nicht geben, solange diese nicht eingetreten seien; von der Wahrscheinlichkeit des Schadenseintritts hänge die Entstehung des Anspruchs also nicht ab. Die Leistungspflicht solle bei künftige Schäden erfassenden Feststellungsklagen deshalb nur für den Fall festgestellt werden, dass die befürchtete Schadensfolge wirklich eintritt. Da dementsprechend der Feststellungsausspruch nichts darüber aussage, ob ein künftiger Schaden eintreten werde, sei es unbedenklich, die Ersatzpflicht des Schädigers für den Fall, dass der Schaden eintreten sollte, bereits jetzt festzustellen (BGH, Urteil vom 17.10.2017 - VI ZR 423/16 -, NJW 2018, 1242 Rz. 49).

Diese Ausführungen sind auf den vorliegenden Fall übertragbar, in dem die Verletzung eines absoluten Rechtes feststeht, und zwar ein Nichtvermögensschaden aber (noch) kein Vermögensschaden eingetreten ist. Auch bei dieser Fallgestaltung würde es den Anspruch auf Ersatz von Vermögensschäden nicht geben, solange diese nicht eingetreten sind, sodass die Entstehung des Anspruchs nicht von der Wahrscheinlichkeit des Schadenseintritts abhängt. Auch insofern bedarf es einer einschränkenden Voraussetzung in Gestalt einer gewissen Wahrscheinlichkeit nicht, und es ist auch insoweit unbedenklich, die Ersatzpflicht des Schädigers für den Fall, dass der Schaden eintreten sollte, bereits jetzt festzustellen, zumal immerhin ein immaterieller Schaden feststeht. Abweichend von Sachverhalten, in denen es infolge von Verletzungen von Normen zum Schutz des Vermögens im Allgemeinen ausschließlich um befürchtete künftige Vermögensschäden geht, ist in der vorliegenden Fallgestaltung überdies eine Verletzung des absoluten Rechtes bereits eingetreten.

Der unter dem Antrag zu 3. b. geltend gemachten Unterlassungsantrag hat keinen Erfolg.

Es kann insoweit offenbleiben, ob – was zutreffen dürfte – entgegen der Auffassung der Beklagten auch unter Geltung der DSGVO Unterlassungsansprüche in Betracht kommen und ob diese auf Art 17, 21 DSGVO oder §§ 823, 1004 BGB zu stützen wären (Überblick zum Meinungsstand bei Leibold/Laoutoumai, ZD-Aktuell 2021, 05583).

Jedenfalls steht der Klägerseite kein Unterlassungsanspruch dahin zu, eine Datenverarbeitung ohne Erfüllung der Informationspflichten hinsichtlich der Funktionsweise des CIT und der Verwendung von Telefonnummern zu unterlassen.

Die Beklagte hat zwar gegen die DSGVO verstoßen, indem sie im Kontext der Registrierung nicht ausreichend nach Art. 13, 14 DSGVO über die Nutzung der mitgeteilten Mobilfunknummer im Zusammenhang mit dem CIT informiert und die Klägerseite damit in seinen Rechten verletzt hat, diese Pflichtverletzung löst aber für die Zukunft keine Folgen mehr aus, da die Klägerseite zumindest im Verlauf des Rechtsstreits sämtliche Informationen erhalten hat, die die fragliche Art und Weise der Datenverarbeitung betreffen. Die von der Klägerseite begehrte Information, dass die Telefonnummer auch bei Einstellung auf „privat" noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert werde und, im Falle der Nutzung der Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird, ist der Klägerseite jedenfalls nunmehr bekannt. Die geforderte Information, von der sie die weitere Datenverarbeitung abhängig machen will, hat die Klägerseite damit bereits. Es besteht mithin weder eine Fortwirkung noch eine Wiederholungsgefahr. Vielmehr würde sich die Klägerseite in Selbstwiderspruch setzten, so sie in Kenntnis die von der Beklagten angebotene Plattform weiter nutzen und gleichzeitig die Unterlassung der Datenverarbeitung ohne Erfüllung der Informationspflichten hinsichtlich der Funktionsweise des CIT und der Verwendung der Telefonnummer fordern würde.

Der Klageantrag zu 4. ist unbegründet.

Der Klägerseite steht kein auf Art 15. DSGVO oder auf dem Nutzungsvertrag i.V.m. § 242 BGB gestützter (weitergehender) Auskunftsanspruch gegenüber der Beklagten zu.

Ein Auskunftsanspruch nach Art. 15 DSGVO besteht nicht.

Nach Art. 15 DSGVO kann – wie bereits ausgeführt - die betroffene Person Auskunft über personenbezogenen Daten verlangen, wenn der Verantwortliche sie betreffende personenbezogene Daten verarbeitet. Art. 15 DSGVO enthält dabei vier Anspruchsinhalte. Nach Art. 15 Abs. 1 Hs. 1 DSGVO besteht ein Anspruch auf Auskunft bzw. eine Bestätigung, ob der Verantwortliche personenbezogene Daten der betroffenen Person verarbeitet. Gemäß Art. 15 Abs. 1 Hs. 2 Teil 1 DS-GVO besteht Anspruch auf Auskunft über die personenbezogenen Daten, die in Bezug auf die betroffene Person vom Verantwortlichen verarbeitet werden. Art. 15 Abs. 2 DSGVO sieht einen Anspruch auf die in Art. 15 Abs. 1 Hs. 2 Teil 2 Buchst. a bis h DS-GVO im Einzelnen genannten Meta-Informationen (Verarbeitungszwecke, Datenkategorien, Empfänger(kategorien), Speicherdauer, Herkunft der Daten etc.) und auf Unterrichtung über geeignete Garantien gem. Art. 46 DS-GVO bei Übermittlung in ein Drittland vor. Letztlich besteht gemäß Art. 15 Abs. 3 S. 1 DS-GVO ein Anspruch auf Zurverfügungstellung einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind.

Zweck der Vorschrift ist es, den Betroffenen durch den Auskunftsanspruch in die Lage zu versetzten, von einer Verarbeitung der ihn betreffenden Daten Kenntnis zu erhalten und diese auf ihre Rechtmäßigkeit hin zu überprüfen (BeckOK DatenschutzR/Schmidt-Wudy, 43. Ed. 1.2.2023, DS-GVO Art. 15 Rn. 2). Art. 15 DSGVO gewährt dabei aber keine Auskunftsrechte im Hinblick auf einen Datenabfluss und im Nachgang eines solchen bezüglich der wirtschaftlichen Verwertung der Daten (vgl. Dickmann, r+s 2018, 345 [351]).

Gemessen hieran ist die seitens der Klägerseite mit dem Klageantrag zu 4. begehrte

„Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet, [...] namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten",

teilweise bereits nicht von Art. 15 DSGVO erfasst. Soweit die Klägerseite Auskunft dahin verlangt,

„welche Daten zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten", ist diese Auskunft nicht von Art. 15 DS-GVO erfasst. Es handelt sich weder um eine Information über die durch die Beklagte verarbeiteten personenbezogenen Daten der Klägerseite noch handelt es sich um Meta-Informationen zu diesen Daten gemäß Art 15 Abs. 1 Hs. 2 Teil 2 DSGVO. In der Sache begehrt die Klägerseite vielmehr Informationen zu der (unbefugten) Datenerhebung durch unbekannte Dritte, die sie gemäß Art 15 DSGVO nicht von der Beklagten verlangen kann.

Soweit der Anspruch besteht, ist er durch Erfüllung erloschen, § 362 Abs. 1 BGB.

Es besteht gemäß Art. 15 Abs. 1 Hs. 2 Teil 1 DSGVO zum einen Anspruch auf Auskunft zu den durch die Beklagte verarbeiteten personenbezogenen Daten der Klägerseite. Der Verantwortliche muss die betroffene Person darüber informieren, welche Daten er über sie verarbeitet. Gemäß Art. 4 Ziff. 7 DSGVO ist „Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden. „Verarbeitung" umfasst gemäß Art. 4 Ziff. 2 DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; das Auskunftsrecht umfasst alle Daten, die bei dem Verantwortlichen vorhanden sind (Bäcker in: Kühling/Buchner, DS-GVO, BDSG, 3. Aufl. 2020, Art. 15 DS-GVO Rn. 8).

Es besteht ferner - wie bereits ausgeführt - im Ausgangspunkt ein Auskunftsrecht der betroffenen Person auch hinsichtlich der Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen gemäß Art. 15 Abs. 1 Hs. 2 lit. c) DSGVO.

Soweit ein Anspruch danach in Betracht kommt, hat die Beklagte ihn erfüllt, sodass er gemäß § 362 BGB erloschen ist.

Mit Schreiben vom 23.08.2021 hat die Beklagte in angemessener Weise mitgeteilt, welche personenbezogenen Daten verarbeitet werden, indem sie die Klägerseite auf die Selbstbedienungstools verwiesen hat. Diese Erfüllungshandlung war ausreichend um den Erfüllungserfolg zu gewährleisten. Soweit der Antrag der Klägerseite im Sinne eines neuen Auskunftsbegehrens nach Art. 15 Abs. 1 DSGVO gerichtet auf die Auskunft betreffend (sämtliche) die Klagepartei betreffende personenbezogene Daten, welche die Beklagte verarbeitet, auszulegen sein sollte, hat die Be-

klagte die Klägerseite mit der Klageerwiderung wiederum auf ihre Selbstbedienungstools („Access Your Information" und „Download Your Information") verwiesen, die der Klagepartei einen Zugriff auf die personenbezogenen Daten gemäß Art. 15 DSGVO erlauben.

Hinsichtlich der begehrten Information zu den Empfängern, die „Daten durch Scraping" erlangen konnten, gelten die obigen Ausführungen entsprechend. Die Beklagte hat sich insoweit zulässigerweise auf die Mitteilung einer Kategorie von potentiellen Empfängern („jedermann") beschränkt. Vor dem Hintergrund, dass die Daten unstreitig auch bei einer - im Sinne der Nutzungsbedingungen - befugten Nutzung eingesehen werden konnten, ist eine Auskunft dahingehend, wer genau schließlich im Wege von „Scraping" Daten erlangt hat, nicht möglich.

Ein Auskunftsanspruch lässt sich auch nicht auf ein gesetzliches Schuldverhältnis oder den Nutzungsvertrag i.V.m. § 242 BGB stützen.

Allerdings kann aus dem gesetzlichen Schuldverhältnis, das durch die Verletzung der DSGVO begründet wird, und aus dem vertraglichen Schuldverhältnis in Gestalt des Nutzungsvertrages jeweils i.V.m. § 242 BGB ein (unselbstständiger) Auskunftsanspruch bestehen, welcher neben dem Bestehen eines Rechtsverhältnisses zwischen den Parteien zur Voraussetzung hat, dass die Klägerseite in entschuldbarer Weise über das Bestehen und den Umfang seines Rechts im Ungewissen und der Verpflichtete unschwer zur Auskunftserteilung in der Lage ist.

Diese Voraussetzungen liegen hier nicht vor.

Soweit die Klägerseite Auskunft begehrt, welche Daten [...] erlangt werden konnten, ist sie insoweit allerdings in entschuldbarer Weise über das Bestehen und den Umfang ihrer Rechte im Ungewissen und die Beklagte unschwer zur Auskunftserteilung in der Lage. Die Beklagte hat aber bereits in dem Schreiben vom 23.08.2022 (Anlage K2, Anlagenband I der Klägerseite) hierzu Auskünfte wie folgt erteilt:

„Im Gegenteil ist anzunehmen, dass die in den durch Scraping abgerufenen Daten enthaltenen Informationen durch sog. Scraping öffentlich abrufbarer Profilinformationen von Facebook-Nutzerprofilen im Zeitraum bis September 2019 erlangt wurden, wobei Funktionen verwendet wurden, die es ordnungsgemäßen Nutzern ermöglichen sollen, diese Informationen einzusehen, um ihnen zu helfen, mit anderen in Kontakt zu treten. Soweit die in den durch Scraping abgerufenen Daten enthaltenen Informationen vom Facebook-Nutzerprofil Ihres Mandanten stammen, waren sie öffentlich auf Facebook zugänglich (wie unten weiter erläutert wird). [...]

Wie in unserem Schreiben vom 21. Juni 2021 erläutert, wurden die durch Scraping abgerufenen Daten nach unserem Verständnis durch den Prozess der sogenannten Telefonnummernaufzäh-

lung abgerufen. Es ist insofern anzunehmen, dass die in den durch Scraping abgerufenen Daten enthaltenen Telefonnummern von den Scrapern unter Anwendung der Methode der Telefonnummernaufzählung bereitgestellt und gerade nicht von Facebook-Nutzerprofilen abgerufen wurden. Zu diesem Zweck haben die Scraper nach unserem Verständnis Listen mit möglichen Telefonnummern von Nutzern hochgeladen, um so zu versuchen festzustellen, ob diese Telefonnummern mit einem Facebook-Konto verbunden sind. Wurde eine Übereinstimmung festgestellt, haben die Scraper bestimmte öffentlich zugängliche Informationen (d. h. Informationen, die öffentlich waren oder bei denen die Zielgruppenauswahl auf "öffentlich" eingestellt war) von dem jeweiligen Nutzerkonto abgerufen. [...]

Facebook Irland hält keine Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten enthalten. Auf Grundlage der bislang vorgenommenen Analysen ist es Facebook Ireland jedoch gelungen, der Nutzer ID Ihres Mandanten die folgenden Datenkategorien zuzuordnen, die nach unserem Verständnis in den durch Scraping abgerufenen Daten erscheinen und mit den auf dem Facebook-Profil Ihres Mandanten verfügbaren Informationen übereinstimmen (die "Datenpunkte"):

· Nutzer ID

· Vorname

· Nachname

· Land

· Geschlecht

Darüber hinaus ist nach unserem Verständnis auch die Telefonnummer Ihres Mandanten in den durch Scraping abgerufenen Daten enthalten, wobei diese nach unserem Verständnis, wie oben beschrieben, von den Scrapern unter Anwendung der Methode der Telefonnummernaufzählung bereitgestellt und gerade nicht vom Facebook-Nutzerprofil Ihres Mandanten abgerufen wurde.

Wie oben beschrieben waren jegliche Daten, die im Rahmen der relevanten Scraping Aktivitäten von Facebook abgerufen wurden, auf Facebook öffentlich zugänglich. In diesem Zusammenhang weisen wir darauf hin, dass bestimmte Nutzerinformationen auf dem Profil eines Nutzers, darunter Vorname, Nachname, Geschlecht und Nutzer-ID, immer öffentlich zugänglich sind. Andere Daten sind ebenfalls öffentlich, wenn die Zielgruppenauswahl des Nutzers für diese Daten auf "öffentlich" eingestellt ist."

Damit hat die Beklagte den Anspruch vorliegend jedenfalls gemäß § 362 BGB erfüllt, nachdem sie dargestellt hat, auf welcher Weise die unbekannten Dritten nach ihren Erkenntnissen vorgingen und welche Daten bei dieser Vorgehensweise eingesehen werden konnten, nämlich die – nach den jeweiligen Einstellungen - „öffentlich" einsehbaren Daten der Klägerseite, sowie die von unbekannten Dritten generierte Telefonnummer.

Soweit die Klägerseite Auskunft begehrt,

„durch welche Empfänger Daten [...] erlangt werden konnten" und „zu welchem Zeitpunkt Daten [...] erlangt werden konnten",

hat die Beklagte in ihrem außergerichtlichen Schreiben, erklärt, dass Dritte öffentlich zugängliche Informationen im Wege des sog. „Scrapings" zusammengetragen hätten. Ferner hat sie ausgeführt, dass diese Daten „bis September 2019" erlangt worden seien. Weitere Auskünfte vermag die Klägerseite vorliegend nicht zu verlangen, nachdem das Scraping von außen erfolgt ist. Die von der Klagepartei begehrte Auskunftserteilung ist daher aufgrund des Vorganges des Scrapings unter Ausnutzung von Daten, die auf „öffentlich" gestellt sind, auch für die Beklagte unmöglich. Das gilt gleichermaßen für die Auskunft, wann die Daten gescrapt wurden. Die Beklagte hat der Klägerseite im Ergebnis also alle Informationen mitgeteilt, die ihr im Zuge des Scraping-Vorfalls zur Verfügung standen. Weitere Angaben kann sie nicht machen. Sie ist entsprechend hierzu auch nicht verpflichtet.

Der Klägerseite steht ein Anspruch auf Ersatz vorgerichtlicher Rechtsanwaltsgebühren lediglich in Höhe von 159,94 € zu.

Die vorgerichtlichen Rechtsanwaltskosten sind Teil des gemäß Art. 82 Abs. 1 DSGVO zu erset-

zenden Schadens. Die Hinzuziehung eines Rechtsanwalts zur Durchsetzung der klägerischen Ansprüche hält die Kammer angesichts der Komplexität der Materie für erforderlich. Ausgehend von einem Wert des berechtigten Verlangens der Klägerseite von bis zu 1.000,00 € zum Zeitpunkt der außergerichtlichen Tätigkeit ergibt dies Kosten in Höhe von 159,94 € (1,3 Geschäftsgebühr Nr. 2300, 1008 VV RVG: 114,40 €; Auslagen Nr. 7001 u. 7002 VV RVG: 20,00 €; 19 % MwSt: 25,54 €).

Der Zinsanspruch folgt aus §§ 288, 291 BGB.

Die Kostenentscheidung folgt aus § 92 Abs. 2 Nr. 1 ZPO.

Danach kann das Gericht der einen Partei die gesamten Prozesskosten auferlegen, wenn die Zuvielforderung der anderen Partei verhältnismäßig geringfügig war und keine oder nur geringfügig höhere Kosten veranlasst hat. Dabei müssen beide Voraussetzungen, die „verhältnismäßig geringfügige Zuvielforderung" und die „Veranlassung keiner oder nur geringfügig höherer Kosten" kumulativ zusammentreffen. Die Geringfügigkeitsgrenze liegt bei 10 % des Streitwertes bzw. hinsichtlich der Mehrkosten der Verfahrenskosten (vgl. Herget in: Zöller, Zivilprozessordnung, 34. Aufl. 2022, § 92 Kosten bei teilweisem Obsiegen, Rn. 10). Zuvielforderung meint über den engeren Begriffssinn hinaus nicht nur den auf Verurteilung gerichteten Antrag der Klägerseite, sondern auch den auf Anspruchsabwehr gerichteten Antrag der Beklagten, wenn dieser bezogen auf die Klageforderung in geringfügigem Umfang verurteilt und die Klage im Übrigen abgewiesen wird (Schulz in: Münchener Kommentar zur ZPO, 6. Aufl. 2020, ZPO § 92 Rn. 19).

Diese Voraussetzungen liegen hier vor. Die Beklagte wurde bezogen auf die Klageforderung nur in geringfügigem Umfange verurteilt und die Klage weit überwiegend abgewiesen. Zu Mehrkosten hat die Rechtsverteidigung nicht geführt.

Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt aus § 709 ZPO.

Den Gebührenstreitwert hat die Kammer mit 8.500,00 € festgesetzt.

Der Bemessung des Gebührenstreitwertes hat die Kammer im Ausgangspunkt gemäß § 48 Abs. 1 S. 1 GKG die für die Zuständigkeit des Prozessgerichts oder die Zulässigkeit des Rechtsmittels geltenden Vorschriften der §§ 3, 6-9 ZPO über den Wert des Streitgegenstands zu Grun-

de gelegt. In der konkreten Streitsache ist ferner zu berücksichtigen, dass verfahrensgegenständlich eine Mehrzahl von Anträgen ist und die Streitigkeiten je nach Antrag zum Teil als vermögensrechtlich und zum Teil als nichtvermögensrechtlich zu qualifizieren sind.

Ob ein Rechtsstreit vermögens- oder nichtvermögensrechtlicher Natur ist, bestimmt sich nach dem Zweck des jeweiligen Klageantrages. Ist der Klageantrag unmittelbar auf eine vermögenswerte Leistung gerichtet, handelt es sich stets um einen vermögensrechtlichen Streit. Ferner sind Ansprüche als vermögensrechtlich zu qualifizieren, die auf vermögensrechtlichen Beziehungen beruhen bzw. ihnen entstammen, sowie solche Ansprüche, die im Wesentlichen der Wahrung wirtschaftlicher Belange dienen. In allen anderen Fällen ist das Rechtsverhältnis entscheidend, aus dem der geltend gemachte Anspruch hergeleitet wird (vgl. Elzer in: Toussaint, Kostenrecht, 53. Aufl. 2023, GKG § 48 Rn. 7 m.w.N.).

Für die Fälle nichtvermögensrechtlicher Streitigkeiten bestimmt § 48 Abs. 2 S. 1 GKG, dass der Streitwert 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 ist, wobei die Grenzen gemäß §§ 34 Abs. 1, 48 Abs. 2 S. 2 GKG bei 500 € und 1 Mio. € liegen. Im Grundsatz kann in Anlehnung an § 23 Abs. 3 Satz 2 RVG bei einer nichtvermögensrechtlichen Streitigkeit und mangelnden genügenden Anhaltspunkten für ein höheres oder geringeres Interesse von einem Wert von 5.000 € ausgegangen werden (vgl. etwa BGH, Beschluss vom 17. November 2015 – II ZB 8/14 –, Rn. 13, juris). Bei der Bemessung darf ferner das Gesamtgefüge der Bewertung nichtvermögensrechtlicher Streitgegenstände nicht aus den Augen verloren werden (vgl. BGH Beschluss vom 28.1.2021 – III ZR 162/20 -, GRUR-RS 2021, 2286 Rn. 9 m.w.N.).

Hieran gemessen hat die Kammer den Streitwert auf insgesamt 8.500,00 € festgesetzt. Im Einzelnen:

Der Antrag zu 1. betrifft eine vermögensrechtliche Streitigkeit; der Streitwert ergibt sich aus dem von der Klägerseite vorgestellten immateriellen (Mindest-)Ersatzbetrag in Höhe von 1.000,00 €.

Der Antrag zu 2. auf Feststellung der Ersatzpflicht hinsichtlich künftiger Schäden betrifft eine vermögensrechtliche Streitigkeit. Ihm ist ein eigener wirtschaftlicher Wert beizumessen, wobei das

Interesse der Klägerseite gemäß § 3 ZPO zu schätzen ist. Die Kammer schätzt dieses Interesse unter Berücksichtigung der hinsichtlich etwaiger künftiger Vermögensschäden ersichtlich schwierig nachzuweisenden Kausalität auf lediglich 250,00 €.

Die in dem Antrag zu 3. unter lit. a. und b. zusammengefassten Unterlassungsanträge betreffen jeweils nichtvermögensrechtliche Streitigkeiten; die Kammer hat für die Unterlassungsanträge insgesamt einen Gebührenstreitwert von 7.000,00 € festgesetzt.

Für den Antrag zu 3. a. hat die Kammer den Gebührenstreitwert unter Berücksichtigung aller Umstände des Einzelfalls, insbesondere des Umfangs und der Bedeutung der Sache und der Vermögens- und Einkommensverhältnisse der Parteien, und in Anlehnung an § 23 Abs. 3 S. 2 RVG auf 5.000,00 € festgesetzt. Konkrete Umstände für eine geringere oder höhere Wertfestsetzung sind nicht ersichtlich. Der Antrag 3. a. ist darauf gerichtet, künftig zu verhindern, dass im Rahmen des Nutzungsverhältnisses der Beklagten bekannt gegebene personenbezogene Daten unbefugten Dritten zugänglich gemacht werden. Das Interesse besteht in der beabsichtigten Sicherstellung, dass etwaige (weitere) Rechtsverletzungen künftig unterbleiben, durch Veranlassung der Beklagten zur Gewährleistung eines höheren Schutzniveaus im Rahmen ihrer Datenverarbeitung. Für die Klägerseite ist dieses Interesse durchaus bedeutsam angesichts der von einem möglichen Scraping regelmäßig betroffenen hohen Personenzahl und der damit verbundenen Gefahr, dass die Daten der Klägerseite mit den Daten anderer Betroffener zu Datenpaketen von ungleich größerem Wert bzw. Interesse missbräuchlicher Verwendung zusammengeführt werden.

Für den Antrag zu 3. b. hat die Kammer den Gebührenstreitwert unter Berücksichtigung aller Umstände des Einzelfalls, insbesondere des Umfangs und der Bedeutung der Sache und der Vermögens- und Einkommensverhältnisse der Parteien auf 2.000,00 € festgesetzt. Mit dem Antrag Ziffer 3. b. wird Unterlassung dahingehend begehrt, die Telefonnummer der Klägerseite auf der Grundlage der erteilten Einwilligung zu verarbeiten. Das Interesse der Klägerseite besteht hier in der Abstellung (etwaig) unberechtigter Verarbeitung ihres personenbezogenen Datums in Gestalt der Telefonnummer. Die Kammer hat bei der Bemessung berücksichtigt, dass es sich zwar lediglich um ein Datum der Klägerseite in Gestalt der Telefonnummer handelt. Bei der Bedeutung der Sache war insoweit zwar einzustellen, dass gerade dieses Datum in der heutigen Gesellschaft von erheblicher Bedeutung ist. Es war aber gleichwohl zu berücksichtigen, dass es der Klägerseite ausweislich der Antragsformulierung im Kern um die Beanstandung geht, dass die Beklagte nicht eindeutig darüber informiert habe, dass die Telefonnummer auch bei Ein-

stellung auf „privat" noch durch Verwendung des Kontaktimporttools verwendet werden könne, wenn nicht explizit hierfür die Berechtigung verweigert werde und im Falle der Nutzung der Facebook-Messenger App dort ebenfalls explizit die Berechtigung verweigert werde.

Die Unterlassungsanträge sind vorliegend zusammenzurechnen, ein Additionsverbot nach dem GKG besteht nicht.

Gemäß § 39 Abs. 1 RVG werden in derselben Angelegenheit grundsätzlich die Werte mehrerer Streitgegenstände zusammengerechnet, soweit nichts Anderes bestimmt ist. Eine Ausnahme ist vorliegend nicht ersichtlich. Im Einzelnen:

Die gesetzliche Ausnahme des § 48 Abs. 3 GKG ist nicht einschlägig. Danach ist nur ein Anspruch, und zwar der höhere, maßgebend, wenn mit einem nichtvermögensrechtlichen Anspruch ein aus ihm hergeleiteter vermögensrechtlicher Anspruch verbunden ist. Vorliegend macht die Klägerseite sowohl immateriellen Schadensersatz als auch Unterlassungsansprüche im Zusammenhang mit einer Verletzung ihres Rechts auf informationelle Selbstbestimmung geltend. Allerdings leitet sich der Anspruch auf immateriellen Schadensersatz nicht i.S.d. § 48 Abs. 3 GKG aus dem nichtvermögensrechtlichen Anspruch her, sondern beide Ansprüche haben lediglich ihre Grundlage in demselben Sachverhalt bzw. derselben Verletzung des Rechtes auf informationelle Selbstbestimmung (vgl. Toussaint in: Dörndorfer/Wendtland/Gerlach/Diehn, BeckOK KostR, 41. Ed. 1.4.2023, GKG § 48 Rn. 50.3).

Darüber hinaus gilt ein allgemeines ungeschriebenes Additionsverbot, wenn mehrere Streitgegenstände wirtschaftlich identisch sind, also keine wirtschaftliche Werthäufung vorliegt. Eine solche wirtschaftliche Identität hat zur Voraussetzung, dass ein Anspruch aus dem anderen folgt oder auf dasselbe Interesse ausgerichtet ist, sodass die klagende Partei mit den Ansprüchen letztlich jeweils nur dasselbe Ziel verfolgt oder der Kläger die Klageforderung nur einmal verlangen kann. In Anlehnung an § 45 Abs. 1 S. 3 GKG ist für diese Fälle nur der höchste Einzelwert maßgebend. Das gilt auch in nichtvermögensrechtlichen Angelegenheiten (vgl. nur Elzer in: Toussaint, Kostenrecht, 53. Aufl. 2023, GKG § 39 Rn. 17 m.w.N.).

Auch diese Voraussetzungen liegen nicht vor, nachdem beide Unterlassungsanträge sowohl kumulativ als auch unabhängig voneinander verfolgt werden können und werden und die Klägersei-

te im Übrigen auch die dargestellt unterschiedlichen Interessen verfolgt (augenscheinlich insoweit a.A. OLG Stuttgart, Beschluss vom 3. Januar 2023 – 4 AR 4/22 –, Rn. 28, juris: Anträge seien letztlich auf dasselbe Ziel gerichtet, die Beklagte zu einem besseren Schutz der überlassenen Daten zu verpflichten).

Die Kammer hat den Streitwert für den Klageantrag zu 4. auf 250,00 € festgesetzt. Dabei hat die Kammer berücksichtigt, dass ein Interesse der Klägerseite vorliegend sowohl - zumal das Auskunftsbegehren anders als das vorprozessuale Begehren gefasst ist - in der Auskunft an sich liegen als auch dem Zweck dienen kann, Voraussetzungen für den Grund und die Höhe eines Schadenersatzanspruchs nach Art. 82 Abs. 1 DSGVO zu schaffen. Nachdem Letzteres in immaterieller Hinsicht bereits mit dem Klageantrag zu Ziffer 1. geltend macht wird und zudem hinsichtlich etwaiger künftiger Vermögensschäden mit dem Klagantrag zu 2 die Feststellung der künftigen Einstandspflicht begehrt wird, kommt dem Antrag zur Schaffung der Voraussetzungen für einen Schadensersatzanspruch gegenwärtig allenfalls hinsichtlich künftiger Vermögensschäden etwaige Bedeutung zu, wobei die Kammer das Interesse insoweit angesichts der ersichtlich problematisch nachzuweisenden Kausalität als gering einschätzt. Die Kammer hält auch unter Berücksichtigung des Interesses der Klägerseite an der Auskunft selbst einen Wert des Antrages von 250,00 € für angemessen.

gez.

Apel
Vorsitzender Richter am Landgericht

Beschluss

Der Streitwert wird auf 8.500,00 € festgesetzt.

Rechtsbehelfsbelehrung:

Gegen die Entscheidung, mit der der Streitwert festgesetzt worden ist, kann Beschwerde eingelegt werden, wenn der Wert des Beschwerdegegenstands 200 Euro übersteigt oder das Gericht die Beschwerde zugelassen hat.

Die Beschwerde ist binnen **sechs Monaten** bei dem

Landgericht Erfurt
Juri-Gagarin-Ring 105 – 107
99084 Erfurt

einzulegen.

Die Frist beginnt mit Eintreten der Rechtskraft der Entscheidung in der Hauptsache oder der anderweitigen Erledigung des Verfahrens. Ist der Streitwert später als einen Monat vor Ablauf der sechsmonatigen Frist festgesetzt worden, kann die Beschwerde noch innerhalb eines Monats nach Zustellung oder formloser Mitteilung des Festsetzungsbeschlusses eingelegt werden. Im Fall der formlosen Mitteilung gilt der Beschluss mit dem dritten Tage nach Aufgabe zur Post als bekannt gemacht.

Die Beschwerde ist schriftlich einzulegen oder durch Erklärung zu Protokoll der Geschäftsstelle des genannten Gerichts. Sie kann auch vor der Geschäftsstelle jedes Amtsgerichts zu Protokoll erklärt werden; die Frist ist jedoch nur gewahrt, wenn das Protokoll rechtzeitig bei dem oben genannten Gericht eingeht. Eine anwaltliche Mitwirkung ist nicht vorgeschrieben.

Rechtsbehelfe können auch als **elektronisches Dokument** eingereicht werden. Eine einfache E-Mail genügt den gesetzlichen Anforderungen nicht.

Rechtsbehelfe, die durch eine Rechtsanwältin, einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind **als elektronisches Dokument** einzureichen, es sei denn, dass dies aus technischen Gründen vorübergehend nicht möglich ist. In diesem Fall bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig, wobei die vorübergehende Unmöglichkeit bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen ist. Auf Anforderung ist das elektronische Dokument nachzureichen.

Elektronische Dokumente müssen
- mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder
- von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.

Ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen ist, darf wie folgt übermittelt werden:
- auf einem sicheren Übermittlungsweg oder
- an das für den Empfang elektronischer Dokumente eingerichtete Elektronische Gerichts- und Verwaltungspostfach (EGVP) des Gerichts.

Wegen der sicheren Übermittlungswege wird auf § 130a Absatz 4 der Zivilprozessordnung verwiesen. Hinsichtlich der weiteren Voraussetzungen zur elektronischen Kommunikation mit den Gerichten wird auf die Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung - ERVV) in der jeweils geltenden Fassung sowie auf die Internetseite www.justiz.de verwiesen.

gez.

[redacted]
Vorsitzender Richter am Landgericht

Verkündet am 09.06.2023

gez.
[redacted], JHSin
als Urkundsbeamtin der Geschäftsstelle