

Landgericht Ingolstadt

Az.: 85 O 1810/22



IM NAMEN DES VOLKES

In dem Rechtsstreit

[REDACTED]
- Klägerin -

Prozessbevollmächtigte:

Rechtsanwälte **Wilde Beuger Solmecke**, Rechtsanwälte Partnerschaft mbB, Kaiser-Wilhelm-Ring 27-29, 50672 Köln, Gz.: 3001/22 nek

gegen

Meta Platforms Ireland Limited, vertreten durch d. Geschäftsführer (Director) Gareth Lambe, Merrion Road D04 X2K5, Dublin 4, Irland

- Beklagte -

Prozessbevollmächtigte:

Rechtsanwälte **Freshfields Bruckhaus Deringer**, Rechtsanwälte Steuerberater PartG mbB, Bockenheimer Anlage 44, 60322 Frankfurt, Gz.: 169638 0036 MCM

wegen Persönlichkeitsverletzung

erlässt das Landgericht Ingolstadt - 8. Zivilkammer - durch den Richter [REDACTED] als Einzelrichter aufgrund der mündlichen Verhandlung vom 30.05.2023 folgendes

Endurteil

1. Die Beklagte wird verurteilt, an die Klägerin 1.000,00 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 07.01.2023 zu zahlen.
2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Januar 2019 erfolgte, entstanden sind und/oder noch entstehen werden.

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000 Euro, 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) personenbezogene Daten der Klägerin, namentlich Telefonnummer, Facebook-ID, Familienname, Vorname, Geschlecht, Stadt und Beziehungsstatus, unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern
 - b) die Telefonnummer der Klägerin 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 Contact-Import-Tools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.
4. Die Beklagte wird verurteilt, an die Klägerin vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 07.01.2023 zu zahlen.
5. Im Übrigen wird die Klage abgewiesen.
6. Die Beklagte trägt die Kosten des Rechtsstreits.
7. Das Urteil ist vorläufig vollstreckbar, für den Kläger hinsichtlich Ziff. 1, Ziff. 4 und wegen der Kosten nur gegen Sicherheitsleistung i.H.v. 110 Prozent des jeweils zu vollstreckenden Betrages, ansonsten hinsichtlich Ziff. 2 gegen Sicherheitsleistung i.H.v. 1.000 Euro und hinsichtlich Ziff. 3 gegen Sicherheitsleistung i.H.v. 8.000 Euro.

Beschluss

Der Streitwert wird auf 11.000,00 € festgesetzt.

Tatbestand

Die Klägerin macht gegen die Beklagte Ansprüche auf Schadensersatz, Unterlassung und Auskunft wegen Datenschutzverstößen geltend.

Die Beklagte betreibt für Nutzer in der Europäischen Union die Facebook-Plattform, auf der sie es registrierten Nutzern ermöglicht, auf den Facebook Dienst über die Webseite www.facebook.com oder über Apps für Mobiltelefone und Tablett-PCs zuzugreifen. Im Rahmen der für die Nutzung des Dienstes erforderlichen Registrierung muss der Nutzer persönliche Daten, nämlich Namen und Geschlecht angeben, die als Teil des Nutzerprofils durchgehend öffentlich einsehbar sind. Weiter für die Registrierung erforderlich ist die Angabe entweder einer E-Mail-Adresse oder einer Telefonnummer. Dem Nutzer wird darüber hinaus die Möglichkeit eingeräumt, sei es im Rahmen des Registrierungsprozesses, sei es nach der Registrierung weitere Daten einzugeben.

Die Beklagte stellt ihren Nutzern bezüglich der Daten, welche freiwillig zusätzlich eingegeben werden können, jederzeit abänderbare Einstellungsmöglichkeiten unter anderem in Form einer Zielgruppenauswahl und in Form von Suchbarkeits-Einstellungen zur Verfügung. Der Nutzer kann hierbei im Rahmen der Zielgruppenauswahl festlegen, wer ein bestimmtes Datenelement im Facebook-Profil des Nutzers sehen kann. Mit der Suchbarkeits-Einstellung bestimmt der Nutzer demgegenüber, ob sein Nutzerkonto auf der Facebook-Plattform anhand bestimmter Daten, beispielsweise Telefonnummern gefunden werden kann. Die Suchbarkeits-Einstellungen stellen die Optionen „alle“, „Freunde von Freunden“, „Freunde“ und ab Mai 2019 auch die Option „nur ich“ zur Verfügung. Die von der Beklagten für die Telefonnummer zur Verfügung gestellte Voreinstellung lautet „alle“.

Die Suchbarkeits-Einstellungen befinden sich im Abschnitt "Privatsphäre" des Haupteinstellungs-menüs im Konto eines Nutzers. Zu diesem Menü kann der Nutzer direkt von der Facebook-Startseite aus gelangen, nachdem er sich in seinem Konto angemeldet hat. Die Beklagte stellt dem Eigennutzer eine Vielzahl von Möglichkeiten unter anderem über die Bereiche „Privatsphäre“ und „Hilfe“ auf der Facebook Startseite zur Verfügung, um zu den jeweils maßgeblichen Einstellungen zu gelangen. Auf die Darstellung in der Klageschrift vom 23.11.2022, Seite 10ff wird Bezug genommen. Hinsichtlich der Handynummer stellt die Beklagte den Nutzern gesonderte Hinweise zur Verfügung. Auf die Darstellung der Klageschrift vom 23.11.2022 (Blatt 15/16 der Akte) wird Bezug genommen.

Die Beklagte bot den Nutzern im streitgegenständlichen Zeitraum die Funktion an, die im Smart-

phone eines Nutzers gespeicherten Personenkontakte mit Nutzern auf Facebook zu synchronisieren. Der Nutzer konnte über das sogenannte Contact-Importer-Tool (kurz CIT) seine Kontakte mit Telefonnummern hochladen, um diese mit den auf den Facebook-Konten hinterlegten Telefonnummern abzugleichen und so zu den Facebook-Konten zu gelangen, bei denen Telefonnummern hinterlegt waren, die sich auch in seinen Kontakten befanden.

Die Klägerin ist Sozialversicherungsfachangestellte im öffentlichen Dienst. Sie hat sich im März 2010 bei der Beklagten als Nutzerin registriert und hat hierbei ihre E-Mail-Adresse angegeben. Im Folgenden hat sie auch ihre Handynummer hinterlegt, dabei hat sie die Zielgruppenauswahl so abgeändert, dass die Handynummer für Dritte nicht einsehbar war. Die mit der Handynummer korrespondierende Suchbarkeitseinstellung, bei welcher die von der Beklagten vorgenommene Voreinstellung auf „alle“ lautet. Die Einstellung wurde jedenfalls zum 21.07.2020 von „alle“ auf „nur ich“ geändert. In den letzten vier bis fünf Jahren nutzte sie Facebook jedoch nicht mehr aktiv und hat das Konto nur noch, um mit der Familie im Ausland Kontakt zu halten. Sie hat seit etwa einem bis anderthalb Jahren eine neue Handynummer und hat diese nicht bei Facebook hinterlegt.

Vermutlich zwischen Januar 2018 und September 2019 lasen unbekannt gebliebene Dritte von Millionen von Facebook-Nutzern die von auf Facebook als „öffentlich“ hinterlegten Daten, in Form des so genannten „Scrapings“ aus. Indem - vermutlich über das Contact-Importer-Tool - eine Vielzahl von Kontakten mit automatisch erzeugten Telefonnummern in ein virtuelles Adressbuch eingegeben wurden, gelang es den unbekannten Dritten, diese - selbst generierten - Telefonnummern konkreten Facebook-Profilen zuzuordnen. Wurde mit einer der automatisch generierten „fiktiven“ Telefonnummer eine Übereinstimmung mit einer bei Facebook hinterlegten „realen“ Telefonnummer erzielt, wurde sodann, ohne dass in den entsprechenden Profilen bei den Sichtbarkeitseinstellungen die hinterlegten Telefonnummern öffentlich freigegeben waren, mit Hilfe des Contact-Importer-Tools der jeweils zugehörige Facebook-Nutzer angezeigt. Auf diese Weise konnten die öffentlich einsehbaren Daten des jeweiligen Nutzers abgegriffen und mit dessen Telefonnummer verbunden werden.

„Scraping“ war und ist nach den Nutzungsbedingungen von facebook.com untersagt. Das Phänomen war bereits vor dem hier streitgegenständlichen Vorfall bekannt und fand und findet im Internet bekanntermaßen statt. Die auf diese Weise ermittelten Datensätze von Millionen von Facebook-Nutzern wurden Anfang April 2021 im Internet verbreitet.

Auch die Daten der Klägerin wurden in der beschriebenen Art abgeschöpft und verbreitet, wobei zwischen den Parteien streitig ist, in welchem Umfang die Abschöpfung und Verbreitung erfolgte.

Die Beklagte informierte über den Vorfall zunächst von sich aus weder die Klägerin noch die Irish Data Protection Commission als zuständige Datenschutzbehörde. Mit der als Anlage K 1 vorgelegten E-Mail vom 27.07.2022 forderte der Prozessbevollmächtigte der Klägerin die Beklagte vorgerichtlich zur Zahlung von 1.000,- €, Unterlassung künftiger Zugänglichmachung der Daten der Klägerin sowie Erteilung einer Auskunft, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht wurden, auf. Hierbei wurde eine Frist von vier Wochen gesetzt. Die Beklagte wies die von der Klägerin geltend gemachten Ansprüche auf Schadensersatz und Unterlassung mit Schreiben vom 23.08.2021 zurück und erteilte Auskünfte.

Die Klägerin behauptet, in dem Zeitraum 2021 bis 2022 fast täglich belästigende Telefonanrufe erhalten zu haben. Dabei, so trägt die Klägerin vor, habe der Anrufer etwa vorgegeben für Vodafone anzurufen und neue Verträge abschließen zu wollen. Die vielen belästigenden Telefonanrufe seien auch der Grund, weshalb sich die Klägerin eine neue Telefonnummer besorgt habe. Ferner habe sie in diesem Zeitraum vermehrt Spam-Mails erhalten. Die Klägerin behauptet ferner, dass die belästigenden Telefonanrufe und Spam-Mails aufgrund des Scraping-Vorfalles bei Facebook erfolgten. Ferner behauptet die Klägerin, einen erheblichen Kontrollverlust über ihre Daten erlitten zu haben.

Schließlich trägt die Klägerin vor, dass die Beklagte keine hinreichenden technischen und organisatorischen Sicherheitsmaßnahmen ergriffen habe, um die Ausnutzung des von ihr zur Verfügung gestellten Contact-Importer-Tools zu verhindern.

Die Klägerin meint, die Vielzahl der Verstöße der Beklagten und deren datenfeindliches Agieren sei im Rahmen der Bemessung der Höhe des Schadensersatzes ebenso zu berücksichtigen wie das in Art. 83 DSGVO enthaltene Bußgeldregime und rechtfertige einen Schadensersatz in der geltend gemachten Höhe. Der geltend gemachte Feststellungsantrag auf Ersatz künftiger Schäden sei dadurch gerechtfertigt, dass die Wahrscheinlichkeit eines Schadenseintritts durch zukünftige erhebliche Belästigungen und die Gefahr einer missbräuchlichen Nutzung der erworbenen Daten mit einer entsprechenden Schadensverursachung besteht. Sie meint, dem geltend gemachten Unterlassungsanspruch könne weder die fehlende Bestimmtheit noch ein Entfall der

Wiederholungsgefahr entgegengehalten werden. Die Klägerin meint ferner, der ihr zustehende Auskunftsanspruch sei durch die außergerichtlich erteilte Auskunft jedenfalls nicht vollständig erfüllt.

Die Klägerin beantragt:

- 1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 EUR nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.**
- 2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Januar 2019 erfolgte, entstanden sind und/oder noch entstehen werden.**
- 3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,**
 - a. personenbezogenen Daten der Klägerseite, namentlich 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 „pri-**

vat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.

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

Die Beklagte beantragt, die Klage abzuweisen.

Die Beklagte behauptet, im fraglichen Zeitraum ausreichende Sicherheitsmaßnahmen hinsichtlich des Scrapings von Daten ergriffen zu haben. Es habe Übertragungsbeschränkungen und eine Bot-Erkennung durch Captcha-Abfragen gegeben. Darüber hinaus beschäftige die Beklagte ein Team von Datenanalysten und Softwareingenieuren zur Verhinderung von Scraping-Aktivitäten.

Die Beklagte meint, dass es mittlerweile dem allgemeinen Lebensrisiko entspringe, dass Daten abgegriffen werden und Spam Mails und Anrufe eingehen. Sie meint ferner, dass die Klage bereits unzulässig sei, da die Klageanträge Ziffern 1 bis 3 nicht hinreichend bestimmt i.S.d. § 253 Abs.2 Nr. 2 ZPO sei. Darüber hinaus sei in Bezug auf Klageantrag Ziffer 2 das Feststellungsinteresse nach § 256 Abs. 1 ZPO nicht gegeben, da ein künftiger Schadenseintritt bei objektiver Betrachtung nicht ersichtlich sei. Des Weiteren meint die Beklagte, dass ein Schadensersatzanspruch nach Art. 82 daran scheitere, dass die Normen gegen welche die Beklagte verstoßen haben soll, nicht dem Anwendungsbereich des Art. 82 unterfielen. Dem Kläger sei darüber hinaus kein Schaden in Form der erforderlichen spürbaren Beeinträchtigung persönlichkeitsbezogener Belange von einem Gewicht entstanden, der zur Geltendmachung eines Schadensersatzanspruchs berechtige. Die von der Klägerseite gerügten Verstöße gegen einzelne Vorschriften der DSGVO lägen nicht vor. Der von der Klägerseite geltend gemachte Unterlassungsanspruch ver-

folge mit der Implementierung von Sicherheitseinrichtungen ein aktives Tun der Beklagten. Aus der DSGVO ergebe sich kein Unterlassungsanspruch. Ein Unterlassungsanspruch ergebe sich nicht aus nationalen Vorschriften, da die DSGVO insoweit abschließend sei. Der Klägerseite stehe der von ihr geltend gemachte Auskunftsanspruch nicht zu, da dieser durch das außergerichtliche Schreiben vom 17.08.2022 bereits vollumfänglich erfüllt sei.

Das Gericht hat am 30.05.2023 mündlich zur Sache verhandelt. Im Rahmen der mündlichen Verhandlung wurde die Klägerin persönlich angehört.

Zur Ergänzung des Sach- und Streitstandes wird auf die zwischen den Parteien gewechselten Schriftsätze der Parteien nebst Anlagen sowie die Protokolle der mündlichen Verhandlungen vom 30.05.2023 Bezug genommen.

Entscheidungsgründe

Die zulässige Klage ist teilweise begründet.

A. Die Klage ist zulässig.

I. Das Landgericht Ingolstadt ist international, sachlich und örtlich zuständig.

1. Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 Alt. 2. EuGVVO (Brüssel Ia - VO). Gemäß Art. 18 Abs. 1 Alt. 2 EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat.

Die Klägerin ist gemäß Art. 17 Abs. 1 EuGVVO Verbraucher. Sie gibt an, einen Nutzungsvertrag mit der Beklagten geschlossen zu haben über die Nutzung der Social-Media-Plattform Facebook mittels eines Benutzerkontos zu privaten Zwecken. Die Klägerin hat ihren Wohnort in Manching, woraus sich die internationale Zuständigkeit der deutschen Gerichte ergibt.

Die internationale Zuständigkeit deutscher Gerichte ergibt sich ferner aus Art. 79 Abs. 2 DSGVO, deren zeitlicher, sachlicher und räumlicher Anwendungsbereich eröffnet ist.

2. Die sachliche Zuständigkeit des Landgerichts Ingolstadt folgt aus § 1 ZPO i.V.m. §§ 23 Nr. 1, 71 Abs. 1 GVG, wobei das Gericht einen Streitwert von mehr als 5000 € zugrunde legt.

3. Die örtliche Zuständigkeit folgt aus Art. 18 Abs. 1 Alt. 2 EuGVVO. Danach kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat. Das Landgericht ist unabhängig davon nach Art. 79 Abs. 2 S. 2 DSGVO, § 44 Abs. 1 S. 2 BDSG örtlich zuständig (besonderer Gerichtsstand). Die Klägerin hat ihren Wohnsitz in Manching und damit im Bezirk des angerufenen Gerichts.

II. Entgegen dem Vorbringen der Beklagten sind die von der Klägerseite gestellten Anträge hinreichend bestimmt i.S.d. § 253 Abs. 2 Nr. 2 ZPO.

Ein Klageantrag ist hinreichend bestimmt, wenn er den erhobenen Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) absteckt, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennen lässt, das Risiko eines Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeiten auf den Beklagten abwälzt und schließlich eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (s. nur BGH, Urteil vom 21.11.2017 - II ZR 180/15, NJW 2018, 1259 Rn. 8 mwN).

1. Entgegen der Auffassung der Beklagtenseite kann die Bestimmtheit des Klageantrags zu 1) nicht mit der Behauptung, es handele sich um unterschiedliche Lebenssachverhalte, deren Verhältnis zueinander unklar sei und die in einem unzulässigen Alternativverhältnis zueinander stünden, infrage gestellt werden. Nach Auffassung des Gerichts richtet sich der Einwand der Beklagtenseite nicht gegen die Bestimmtheit des Klageantrags i.S.d. § 253 Abs. 2 Nr. 2, Alt. 2. ZPO, sondern gegen die durch § 253 Abs. 2 Nr. 2, Alt. 1 ZPO zwingend vorgeschriebene Bezeichnung

des Gegenstands und Grund des Anspruchs und damit des dem Klageanspruch zugrundegelegten tatsächlichen Sachverhalts.

Soweit die Beklagtenseite ihre Auffassung, es lägen mehrere Lebenssachverhalte vor, auf die von der Klägerseite behauptete Verletzung mehrerer Vorschriften der DSGVO stützt, handelt es sich um rechtliche Qualifizierungen, die nicht zum Lebenssachverhalt gehören. Entgegen der Auffassung der Beklagtenseite wird von der Klägerseite lediglich ein Lebenssachverhalt beschrieben, der den Zeitraum von der Registrierung bis hin zur behaupteten Schädigung in der Gegenwart mit umfasst und durch die bestehenden vertraglichen Beziehungen betreffend die Nutzung der von der Beklagten zur Verfügung gestellten Dienste verbunden wird. Auf Grundlage des vorstehenden Sachverhalts entwickelt die Klägerseite den von ihr geltend gemachten Schadensersatzanspruch. Die von der Beklagtenseite geäußerten Zweifel hinsichtlich des Umfangs der Rechtskraft vermag das Gericht nicht zu teilen. Ebenso wenig überzeugt das Gericht der Einwand, dass das Kostenrisiko in unzulässiger Weise auf die Beklagte abgewälzt wird. Dem Kostenrisiko dürfte angesichts des mit dem Klageantrag zu 1 verfolgten überschaubaren Betrags ohnehin keine gesteigerte Bedeutung zukommen.

2. Der Ansicht der Beklagten, der mit der Ziffer 2) verfolgte Feststellungsantrag entspreche nicht dem Bestimmtheitserfordernis des § 253 Abs. 2 Nr. 2 ZPO, kann nicht gefolgt werden.

Das Erfordernis eines bestimmten Antrags (§ 253 Abs. 2 Nr. 2 ZPO) gilt allerdings als eine die Ordnungsmäßigkeit der Klageerhebung betreffende Prozeßvoraussetzung auch für die Feststellungsklage nach § 256 ZPO. Die Klägerin muss deshalb in seinem Antrag das Rechtsverhältnis, dessen Bestehen oder Nichtbestehen festgestellt werden soll, so genau bezeichnen, dass über dessen Identität und damit über den Umfang der Rechtskraft des begehrten Feststellungsanspruchs keinerlei Ungewissheit herrschen kann (BGH, Urteil vom 4.10.2000 – VIII ZR 289/99, Rn. 35, juris).

Entgegen der Auffassung der Beklagtenseite kann die Bestimmtheit allerdings nicht dadurch infrage gestellt werden, dass der Feststellungsgegenstand im Verhältnis entstandene/künftige Schäden nicht eindeutig festgelegt ist. Das Gericht sieht das festzustellende Rechtsverhältnis mit dem Ersatz künftig entstehender Schäden hinreichend genau bezeichnet. Dies erschließt sich zwar nicht ohne weiteres aus dem Wortlaut des Antrags, wohl aber in Verbindung mit dem Sachvortrag des Klägers, der nach ständiger Rechtsprechung des Bundesgerichtshofs zur streitgegenstandsbestimmenden Auslegung des Antrags heranzuziehen ist (BGH, Urteil vom 4.10.2000

– VIII ZR 289/99, Rn. 36, juris).

Es liegt für den Klageantrag zu 2) auch ein Feststellungsinteresse nach § 256 Abs. 1 ZPO hinsichtlich zukünftiger materieller Schäden vor. Dieses erfordert im Gegensatz zu der von der Beklagtenseite vertretenen Auffassung keinen konkreten Sachvortrag, welche materiellen Schäden ihr noch entstehen könnten. Ausreichend ist die Möglichkeit eines künftigen Schadenseintritts, wobei ein Feststellungsinteresse nur dann zu verneinen ist, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund gegeben ist, mit dem Eintritt eines Schadens wenigstens zu rechnen (BGH, Beschluss vom 09.01.2007 – VI ZR 133/06–, Rn. 5, juris). Mit der Klägerseite hält das Gericht die Gefahr einer missbräuchlichen Nutzung der klägerischen Daten, die zu einem Vermögensschaden auf Klägerseite führen kann, nicht für ausgeschlossen.

Demgegenüber dürfte sich ein Feststellungsinteresse hinsichtlich künftiger immaterieller Schäden wegen des mit dem Antrag zu 1) unbeschränkt geltend gemachten Schmerzensgeldes nach dem Grundsatz der Einheitlichkeit des Schmerzensgeldes, der es gebietet, die Höhe des der Geschädigten zustehenden Schmerzensgeldes aufgrund einer ganzheitlichen Betrachtung der den Schadensfall prägenden Umstände unter Einbeziehung der absehbaren künftigen Entwicklung des Schadensbildes zu bemessen (BGH, Urteil vom 10.07.2018 – VI ZR 259/15, Rn. 6, juris) nicht darstellen lassen.

3. Entgegen der Auffassung der Beklagtenseite ist auch der Klageantrag zu 3a) hinreichend bestimmt.

Soweit die Beklagtenseite den von der Klägerseite im Rahmen des Antrags verwendeten Ausdruck „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ und hierbei insbesondere den Terminus „Stand der Technik“ beanstandet, ist ihr dahingehend recht zu geben, dass der vorgenannte Begriff Wandlungen unterliegt und auslegungsbedürftig ist. Die Verwendung derartiger Begriffe, deren Bedeutung nicht immer gleich sein muss, in Antrags- und Urteilsformel ist nicht grundsätzlich und generell unzulässig (BGH, Urteil vom 05.10.2010 - I ZR 46/09, Rn. 11, juris). Eine auslegungsbedürftige Antragsformulierung kann hinzunehmen sein, wenn dies zur Gewährleistung effektiven Rechtsschutzes erforderlich ist (BGH, Urteil vom 21.05.2015 - I ZR 183/13, Rn. 13, juris).

So liegt der Fall hier. Die Beschreibung von konkreten Sicherheitsmaßnahmen anstelle des verwendeten Begriffs würde einerseits die Befugnisse der Beklagten zur Entscheidung, welche Si-

cherheitsmaßnahmen sie implementieren möchte, einschränken, andererseits wäre die Klägerin verpflichtet, sich über den aktuellen Stand der Technik zu erkundigen, um diese der Klage zugrunde zu legen und bei Änderungen jeweils eine neue Klage gegen die Beklagte anzustrengen. Diese Vorgehensweise würde einem effektiven Rechtsschutz widersprechen (so auch LG Essen, Urteil vom 10.11.2022 - 6 O 111/22, Rn. 55, juris, LG Bielefeld, Urteil vom 19.12.2022 - 8 O 182/22, Rn. 31, juris).

Entgegen der Auffassung der Beklagtenseite kann den Anträgen 3) die Bestimmtheit auch nicht deswegen abgesprochen werden, weil hier lediglich der Gesetzeswortlaut wiedergegeben wird. Über den Gesetzeswortlaut hinaus hat die Klägerseite aber mit der Einbeziehung des von der Beklagten zur Verfügung gestellten Contact- Importer-Tools hinreichend deutlich macht, dass er kein Verbot im Umfang des Gesetzeswortlauts beansprucht, sondern sich mit seinem Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert (BGH, Urteil vom 21.05.2015 - I ZR 183/13, Rn. 13, juris).

Der von der Klägerseite verwendete Begriff der unübersichtlichen und unvollständigen Information hat in der Antragstellung über die Aufnahme der konkreten Verletzungshandlung eine hinreichende Konkretisierung gefunden.

B. Die Klage ist ferner teilweise begründet.

I. Die Klägerin hat einen Anspruch auf Ersatz ihres immateriellen Schadens in Höhe von 1.000,00 € aus Art. 82 Abs. 1, Abs. 2 S. 1 DSGVO.

1. Zur Überzeugung des Gerichts hat die Beklagte als Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO gegen mehrere Vorschriften aus der DSGVO verstoßen.

Nach Art. 82 Abs. 1 DSGVO ist für eine Schadensersatzpflicht ein Verstoß gegen die DSGVO erforderlich. Da der sachliche Anwendungsbereich der DSGVO nach deren Art. 2 Abs. 1 jedoch nur für die Datenverarbeitung eröffnet ist, ist ein Verstoß in Form einer gegen die Vorschriften der DSGVO erfolgten Datenverarbeitung erforderlich. Art. 82 Abs. 1, Abs. 2 S. 1 und S. 2 DSGVO beinhalten daher lediglich die Klarstellung, dass der Verantwortliche für alle - durch entsprechende Verstöße verursachte - Schäden haftet, während der Auftragsverwalter nur unter weiteren Voraussetzungen für Schäden haftet. Eine Einschränkung hinsichtlich der - eine Haftung nach Art. 82

Abs. 1 DSGVO begründenden - Verstöße liegt hierin jedoch nicht.

a) Die Beklagte hat gegen die Verpflichtung aus Art. 25 Abs. 2 DSGVO verstoßen ("privacy by default").

aa) Ein Verstoß gegen Art. 25 Abs. 2 DSGVO kann einen Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO begründen, Art. 25 DSGVO ist mithin vom Schutzbereich des Art. 82 DSGVO umfasst. (Martini in: Paal/Pauly, DSGVO, BDSG, Art. 25 DSGVO, Rn. 6; a.A. Nolte/Werkmeister in: Gola/Heckmann, DSGVO, BDSG, Art. 25 DSGVO, Rn. 34; LG Lübeck, Urteil vom 25.05.2023 - 15 O 74/22, Rn. 94, juris). Die entgegengesetzte Auffassung erklärt ihre ablehnende Haltung damit, dass es sich bei Art. 25 um eine organisatorische Verpflichtung handle und sich Schadensersatzansprüche erst mit einer rechtswidrigen Verarbeitung ergeben (Nolte/Werkmeister in: Gola/Heckmann, DSGVO, BDSG, Art. 25 DSGVO, Rn. 34). Es wird mithin darauf abgestellt, dass es sich bei Art. 25 DSGVO um eine Art Vorfeldverpflichtung zur Datenverarbeitung handle und die Schadensersatzpflicht des Verantwortlichen nach Art. 82 Abs. 1, Abs. 2 S. 1 DSGVO einen Verstoß durch eine nicht der Verordnung entsprechende Verarbeitung voraussetzt (LG Lübeck, Urteil vom 25.05.2023 - 15 O 74/22, Rn. 94, juris). Dies kann jedoch nicht überzeugen. Vielmehr ist der sachliche Anwendungsbereich der Verordnung nach Art. 2 Abs. 1 DSGVO doch nur bei der Datenverarbeitung eröffnet. Die Anwendbarkeit der DSGVO setzt also die tatsächliche Datenverarbeitung voraus. Aus diesem Grund ist Art. 25 DSGVO so zu verstehen, dass der Verantwortliche verpflichtet wird, nur diejenigen Datenverarbeitungen tatsächlich einzusetzen, welche die Grundsätze des Art. 25 DSGVO beachten. Mithin stellt die Inbetriebnahme einer unter Missachtung der Vorgaben des Art. 25 DSGVO entwickelten Verarbeitung einen Verstoß dar (Baumgartner in: Ehmann/Selmayr, DSGVO, Art. 25 Rn. 7; Martini in: Paal/Pauly, DSGVO, BDSG, Art. 25 DSGVO, Rn. 6).

bb) Nach Art. 25 Abs. 2 S. 1 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Art. 25 Abs. 2 S. 2 DSGVO konkretisiert, dass solche Maßnahmen insbesondere sicherstellen müssen, dass personenbezogene Daten durch Vorein-

stellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Mithin besteht eine Verpflichtung zu datenschutzfreundlichen Voreinstellungen ("privacy by default"). Diese Vorschrift ist gerade auf soziale Netzwerke zugeschnitten und soll es den Nutzern ermöglichen, den Kreis der Empfänger der betroffenen Daten selbst zu steuern, weshalb auch der kleinstmögliche Empfängerkreis als Voreinstellung vorzusehen ist (Nolte/Werkmeister in: Gola/Heckmann, DSGVO, BDSG, Art. 25 DSGVO, Rn. 31).

cc) Für die Registrierung bei dem Sozialen Netzwerk der Beklagten ist unstreitig die Angabe des Namens und eine E-Mail-Adresse oder eine Handynummer erforderlich. Die Hinterlegung einer Telefonnummer ist nicht erforderlich, wenn eine E-Mail-Adresse angegeben wird. Sie kann jedoch vorgenommen werden, um etwa leichter gefunden zu werden oder den Zugriff auf das Konto zu ermöglichen (Authentifizierungsfunktion). Wird die Telefonnummer hinterlegt, ist die Einstellung zunächst auf "everyone" "by phone number" gestellt. Ändert man diese Einstellung nicht, so kann der jeweilige Nutzer über seine Mobilnummer gefunden werden. Die Standard-Voreinstellung sah mithin vor, dass alle Personen - unabhängig von der Einsehbarkeit der Telefonnummer - das Profil mit der Telefonnummer finden können. Die Nutzer mussten selbst aktiv werden, um ihre Daten weniger zugänglich zu machen. Ebenso verhält es sich mit der E-Mail-Adresse. Auch in Bezug auf diese ist die Standardeinstellung die, dass jedermann den Nutzer mit der E-Mail-Adresse finden kann.

dd) Hierin liegt jedoch bereits der Verstoß gegen Art. 25 Abs. 2 DSGVO. Mithin wurde nicht der kleinstmögliche Empfängerkreis - die Einstellung „nur ich“ - als Voreinstellung vorgenommen. Vielmehr wurde die Telefonnummer der Klägerin durch die Voreinstellung einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht. Mithin konnte jeder durch Eingabe der Telefonnummer diese mit dem Profil der Klägerin in Verbindung bringen. Dieser Verstoß erfolgte auch im Rahmen der Verarbeitung personenbezogener Daten, worunter nach Art. 4 Nr. 2 DSGVO auch die Speicherung von Daten fällt. Als die Telefonnummer der Klägerin gespeichert wurde, geschah das auf die Weise, dass ein jeder ihr Profil durch Eingabe der Telefonnummer finden konnte und so die Telefonnummer mit dem Namen der Klägerin und deren weiteren Daten verbinden konnte.

ee) Nachdem die Beklagte die aufgezeigten Voreinstellungen trifft und hiermit nach Auffassung des Gerichts gegen Art. 25 Abs. 2 DSGVO verstoßen hat, ist es an dieser Stelle unerheblich, ob den Nutzern ein Hinweis auf die vorgenommene Einstellung und über Einstellungsmöglichkeiten erteilt wurde. Auch etwaige Gepflogenheiten auf sozialen Netzwerken können nicht berücksichtigt werden (a.A. LG Bielefeld Urteil vom 10.03.2023 - 19 O 147/22, Rn. 45, juris; LG Fulda, Urteil vom 14.03.2023 - 3 O 73/22, Rn. 46, juris). Art. 25 Abs. 2 S. 2 DSGVO ist insofern eindeutig. Personenbezogene Daten dürfen nicht ohne Eingreifen der betroffenen Person durch Voreinstellungen einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Hiermit ist klar zum Ausdruck gebracht, dass die Zugänglichmachung besagter Daten lediglich mit der Möglichkeit dies durch Einstellungen für die Zukunft zu ändern nicht ausreicht. Vielmehr verlangt Art. 25 Abs. 2 S. 2 DSGVO genau das Gegenteil. Ebenso wenig kann an dieser Stelle berücksichtigt werden, ob und gegebenenfalls in welchem Umfang die Beklagte technische Maßnahmen ergriffen hat, um Scraping zu erschweren (a.A. LG Bielefeld Urteil vom 10.03.2023 - 19 O 147/22, Rn. 46, juris). Hierbei handelt es sich um Erwägungen, welche lediglich im Rahmen der Frage des Verschuldens der Beklagten und damit am Maßstab des Art. 82 Abs. 3 DSGVO zu berücksichtigen sind.

b) Darüber hinaus ist die Beklagte auch ihrer Informations- und Aufklärungspflicht gemäß Art. 13 DSGVO jedenfalls nicht in vollem Umfang nachgekommen. Mithin ist das Gericht zu der Überzeugung gelangt, dass die Beklagte die Klägerin im Zeitpunkt der Datenerhebung ihrer Handynummer nicht ausreichend über die Zwecke der Verarbeitung besagter Handynummer aufgeklärt hat.

aa) Ein Verstoß gegen Art. 13 DSGVO kann einen Schadensersatzanspruch nach Art. 82 DSGVO begründen, auch Art. 13 DSGVO fällt unter den Schutzbereich des Art. 82 DSGVO (Franck in: Gola/Heckmann, DSGVO, BDSG, Art. 13 DSGVO, Rn. 64; Schmidt-Wudy in: BeckOK Datenschutzrecht, Art. 13 DSGVO, Rn. 18; LG Stuttgart, Urteil vom 26.01.2023 - 53 O 95/22, Rn. 72, juris; a.A. LG Essen, Urteil vom 10.11.2022 - 6 O 111/22, Rn. 62, 65, 72, juris).

bb) Art. 13 Abs. 1 lit. c DSGVO legt die Verpflichtung fest, die betroffene Person über die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung anzugeben. Entsprechend der Legaldefinition der (Daten-) Verarbeitung in Art. 4

Nr. 2 DSGVO entstehen die Informations- und Aufklärungspflichten des Art. 13 DSGVO bereits mit der Erhebung personenbezogener Daten. Bereits zu diesem Zeitpunkt hat der Verantwortliche gegenüber dem Betroffenen umfangreiche Informationspflichten zu erfüllen.

cc) Dieser Verpflichtung hat die Beklagte jedenfalls in Bezug auf die Verwendung der Handynummer im Rahmen des „Contact-Import-Tool“ nicht genügt. Durch diese Funktion kann ein Nutzer einen Abgleich der in seinem Smartphone gespeicherten Kontakte mit den auf Facebook registrierten Nutzerprofilen, die ihr Profil mit einer Mobilfunknummer verknüpft haben, durchführen. So können diese Kontakte auf der Facebook-Plattform gefunden, und es kann mit ihnen in Verbindung getreten werden.

Aus dem Vortrag der Beklagtenseite ist nicht ersichtlich, dass insoweit durch die Beklagte eine irgendwie geartete Aufklärung erfolgt wäre. Derlei vermag die Beklagte insbesondere im Rahmen der Klageerwiderung vom 13.04.2023 (dort Rn. 38 ff.) nicht aufzuzeigen. Vielmehr wird durch die Information „Möglicherweise verwenden wir deine Mobilnummer für diese Zwecke: Um dir Personen, die du kennen könntest, vorzuschlagen, damit du dich mit ihnen auf Facebook verbinden kannst“ (Rn. 45 der Klageerwiderung) gerade ein gegenteiliger Eindruck erweckt. Es wird nicht darüber informiert, dass andere den Kläger als Nutzer finden können, sondern darüber, dass dem Kläger seine Telefonnummer nützlich sein kann, andere Facebook-Nutzer zu finden. Das eine mag zwar mit dem anderen unmittelbar zusammenhängen, indes gestaltet sich die Information der Beklagten selektiv und damit unvollständig. Das wird auch nicht durch den anschließenden Hinweis, dass man kontrollieren könne, wer die eigene Telefonnummer sehen könne, geheilt.

Auch in der vorgelegten Datenrichtlinie aus dem Jahr 2018 der Anlage B 9 wird in der Rubrik „Wie werden diese Informationen geteilt?“ noch nicht einmal im Ansatz auf die Verwendung der Handynummer im Rahmen des „Contact-Import-Tool“ hingewiesen. Dort wird lediglich erläutert, dass die von einem Benutzer bereitgestellten Informationen zur Bereitstellung, Verbesserung und Entwicklung der Dienste, zur Kommunikation mit dem die Informationen bereitstellenden Benutzer, zum Anzeigen und Messen von Werbeanzeigen und Diensten sowie zur Förderung der Sicherheit verwendet werden. Ein Hinweis auf die Verwendung der Mobilfunknummer für das „Contact-Import-Tool“ erfolgt dagegen nicht.

dd) Angesichts des Vorstehenden kann hier auch nicht von einer wirksamen Einwilligung der Klä-

gerin i.S.d. Art. 6 Abs. 1 lit. a DSGVO ausgegangen werden. Eine Einwilligung kann mithin keinen Bestand haben, wenn dem Betroffenen nicht schon bei der Datenerhebung sämtliche gemäß Art. 13 DSGVO erforderlichen Informationen mitgeteilt werden. Ebenso wenig ist das Auffinden über das „Contact-Import-Tool“ für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich (Art. 6 Abs. 1 Satz 1 lit. c DSGVO).

c) Schließlich hat die Beklagte noch gegen Art. 32, 24, 5 Abs. 1 lit. f DSGVO verstoßen, da sie keine zureichenden Sicherheitsmaßnahmen hinsichtlich der Nutzung des „Contact-Importer-Tools“ getroffen hat.

aa) Nach Art. 32 Abs. 1 DSGVO hat der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Art. 32 DSGVO konkretisiert damit die als Generalauftrag gestalteten Datensicherheitsmaßnahmen des Art. 24 DSGVO und dient u.a. der Gewährleistung der Absicherung der Datenschutzgrundsätze der Vertraulichkeit und Integrität nach Art. 5 Abs. 1 f) DSGVO. Zielrichtung ist ein umfassender Schutz der für die Verarbeitung von personenbezogenen Daten genutzten Systeme, also im Kern die Datensicherheit (Mantz in: Sydow/Marsch DSGVO/BDSG, Art. 32 DSGVO Rn. 1). 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 (Martini in: Paal/Pauly, DSGVO, BDSG, Art. 32 DSGVO Rn. 2).

Bei der Implementierung von geeigneten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DSGVO sind dabei der Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen als Faktoren zu berücksichtigen. Je höher die drohenden Schäden sind, desto wirksamer müssen die zu ergreifenden Maßnahmen sein (Jandt in: Kühling/Buchner, DS-GVO, BDSG, Art. 32 DSGVO Rn. 7-13). Ausweislich des Erwägungsgrundes 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 (so auch LG Lübeck, Urteil vom 25.05.2023 - 15 O 74/22, Rn. 84, juris).

bb) 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 Lübeck, Urteil vom 25.05.2023 - 15 O 74/22, Rn. 85, juris). Der Beklagten war diese Thematik auch bekannt. Bereits in ihrem Artikel vom 06.04.2021 (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 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.

cc) Das Gericht geht jedoch davon aus, dass die Beklagte vorliegend keine diesen Anforderungen genügenden Schutzmaßnahmen ergriffen hat.

Die Beklagte trifft insoweit eine sekundäre Darlegungslast, zu den von ihr aufgeführten Schutzmaßnahmen konkret vorzutragen (OLG Stuttgart, Urteil vom 31.03.2021 – 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 10.02.2015 – 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 Sicherheitsmaßnahmen genügen, nicht zugänglich, da weder hinreichend zu der Funktionsweise noch zu der konkreten Ausgestaltung vorgetragen wurde. Dieser ungenügende Vortrag erfolgte, obgleich in der Klageschrift (Blatt 32 ff. d.A.) das Fehlen technischer Schutzmaßnahmen vorgetragen wurde.

Soweit die Beklagte darüber hinaus vorträgt, auf andere Art gegen Scraper vorzugehen, 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.

d) Ob die Beklagte schließlich auch gegen ihre Meldepflichten aus Art. 33, 34 DSGVO verstoßen hat, kann hier offen bleiben. Selbst wenn dem so wäre, wäre ein Verstoß im Rahmen des Art. 82 Abs. 1 DSGVO doch nur dann relevant, wenn der Pflichtverstoß für den eingetretenen Schaden kausal war (EuGH, Urt. v. 04.05.2023 – C-300/21, NZA 2023, 621 Rn. 32). Davon, dass ein Pflichtverstoß kausal für den Schaden war oder diesen zumindest vertieft hätte, konnte sich das Gericht die nach § 286 ZPO erforderliche Überzeugung jedoch nicht bilden. 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 damit bereits eingetretenen Schaden in Gestalt der Verletzung des allgemeinen Persönlichkeitsrechtes der Klägerseite konkret weiter vertieft hätte, lässt sich bei dieser Sachlage nicht feststellen (vgl. auch LG Lübeck, Urteil vom 25.05.2023 - 15 O 74/22, Rn. 96, juris). Selbiges gilt auch für den behaupteten Verstoß gegen Art. 15 DSGVO. Das Auskunftsverlangen wurde mit E-Mail vom 27.07.2022 (Anlage K 1) der Beklagten übermittelt. Zu diesem Zeitpunkt war der Schaden längst

eingetreten und konnte auch nicht mehr intensiviert werden. Insbesondere hatte sich die Klägerin bis zu diesem Zeitpunkt bereit eine neue Handynummer besorgt.

2. Ferner liegt auch ein ersatzfähiger Schaden i.S.v. Art. 82 Abs. 1 DSGVO vor.

a) Der Begriff des Schadens ist ein autonomer Begriff des Unionsrechts, welcher in allen Mitgliedstaaten einheitlich auszulegen ist (vgl. EuGH, Urt. v. 04.05.2023 – C-300/21, NZA 2023, 621 Rn. 30). Er ist nach dem Erwägungsgrund 146 S. 3 im Lichte der Rechtsprechung des Europäischen Gerichtshofs weit und auf eine Art und Weise auszulegen, die den Zielen der Verordnung in vollem Umfang entspricht. Grundsätzlich ermöglicht Art. 82 Abs. 1 DSGVO den Ersatz materieller und immaterieller Schäden. Dabei genügt ein Verstoß gegen die DSGVO allein jedoch noch nicht für die Annahme eines Schadens (vgl. EuGH, Urt. v. 04.05.2023 – C-300/21, NZA 2023, 621 Rn. 42). Vielmehr ist der Schaden als ein neben dem Verstoß gegen die DSGVO eigenständiges Kriterium gesondert festzustellen. Es bedarf mithin des Nachweises eines konkret entstandenen Schadens (OLG Frankfurt, Urteil vom 02.03.2022 - 13 U 206/20, Rn. 70, juris). In den Erwägungsgründen 75 und 85 wird der Kontrollverlust über die personenbezogenen Daten als Beispiel für das Vorliegen eines solchen Schadens aufgeführt. Schließlich darf der Schadensersatz nicht davon abhängig gemacht werden, dass der entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat (vgl. EuGH, Urt. v. 04.05.2023 – C-300/21, NZA 2023, 621 Rn. 51). Der Schadensbegriff des Art. 82 Abs. 1 DSGVO umfasst mithin auch „Bagatellschäden“.

b) Unter Anwendung der vorstehenden Grundsätze, ist das Gericht, nach der am 30.05.2023 durchgeführten mündlichen Verhandlung und der in diesem Rahmen erfolgten Anhörung der Klägerin, i.S.d. § 286 Abs. 1 S. 1 ZPO davon überzeugt, dass auf Seiten der Klägerin ein Schaden vorliegt. Dieser in Form von belästigenden Anrufen und von Spam-Mails in ganz erheblichem Umfang. Dabei gingen die belästigenden Anrufe so weit, dass die Klägerin sich eine neue Handynummer besorgt hat. Hinsichtlich der belästigenden E-Mails hat die Klägerin mittlerweile ihren Spam-Filter so eingestellt, dass diese überwiegend im Spam-Ordner landen. Gleichwohl ist dies für sie immer noch problematisch, da sie E-Mails mit vermeintlichen Postlieferungsscheinen erhält. Diese von echten Bestellungen abzugrenzen gestaltet sich schwierig.

Aufgrund des in der mündlichen Verhandlung gewonnenen Eindrucks von der Klägerin, hält das

Gericht diese für insgesamt glaubwürdig und ihre Aussage für glaubhaft. Sie war keineswegs bemüht, die floskelhaften und letztlich nichtssagenden Formulierungen der Klage zu wiederholen. Vielmehr schilderte sie das, was sie gestört hat, ohne Übertreibungen und ohne erkennbaren Blick auf das, was ihrem Begehren vermeintlich dienlicher sein könnte. So gab sie auch ohne Weitere zu, wenn sie sich an etwas nicht erinnern konnte. Gab etwa an, dass ihr nicht mehr bekannt sei, wann genau sie ihre Handynummer eingepflegt hat.

3. Die oben bezeichneten Verstöße der Beklagten gegen die DSGVO waren zur Überzeugung des Gerichts auch kausal für den Schaden der Klägerin.

a) Der Schadensersatzanspruch aus Art. 82 Abs. 1 DSGVO erfordert neben einem Verstoß gegen die DSGVO und einem Schaden auch die Kausalität zwischen beiden (vgl. EuGH, Urt. v. 04.05.2023 – C-300/21, NZA 2023, 621 Rn. 32).

b) Das Gericht ist davon überzeugt, dass die Klägerin - wie auch in der Klageschrift vorgetragen - ihre Telefonnummer nicht angegeben hätte, wenn sie über die Folgen der Hinterlegung der Telefonnummer angemessen informiert worden wäre. Auch ist das Gericht davon überzeugt, dass die Klägerin keine Änderung der Datenschutzeinstellungen hinsichtlich der Telefonnummer vorgenommen hätte, wenn eine datenschutzfreundliche Voreinstellung wie sie Art. 25 Abs. 2 DSGVO verlangt erfolgt wäre. Dies wird auch dadurch verdeutlicht, dass die Klägerin ihre neue Telefonnummer nicht bei Facebook hinterlegt hat. Schließlich sind auch die unzureichenden Sicherheitsmaßnahmen nach Auffassung des Gerichts kausal dafür, dass die Daten durch Scraping abgegriffen wurden. Insgesamt sind somit alle aufgezeigten Verstöße gegen die DSGVO kausal dafür, dass die Daten der Klägerin durch Scraping abgegriffen werden konnten..

Durch den von der Klägerin geschilderten engen zeitlichen Zusammenhang zwischen dem Scraping-Vorfall und dem Beginn der belästigenden Anrufe und E-Mails ist das Gericht ferner davon überzeugt, dass letztere kausal auf den Scraping-Vorfall zurückzuführen sind.

4. Eine Exkulpation der Beklagten nach Art. 82 Abs. 3 DSGVO gelingt nicht. Hierfür müsste die Beklagte nachweisen, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden ein-

getreten ist, verantwortlich ist. Die Beklagte hat jedoch keinerlei Umstände angeführt, die sie hinsichtlich der unzureichend erteilten Informationen in Bezug auf die Verarbeitung der Telefonnummer, die fehlenden Sicherheitsmaßnahmen zur Vermeidung des automatisierten Abgreifens von Daten über das „Contact-Importer-Tool mittels Telefonnummern und die datenschutzunfreundliche Standardeinstellung bei der Suchbarkeit über die Telefonnummer entlasten könnte.

5. Die Höhe des Schadens wird von Seiten des Gerichts mit 1.000, - € beziffert. Diesen Betrag hält das Gericht für angemessen, aber auch für ausreichend, um den immateriellen Schaden der Klägerin auszugleichen, also der Ausgleichs- und Genugtuungsfunktion des immateriellen Schadensersatzes zu genügen. Darüber hinaus wird hiermit auch der generalpräventiven Funktion des immateriellen Schadensersatzes hinreichend Rechnung getragen. Das Gericht hat hierbei die Höhe des Schadens unter Zugrundelegung dessen, worin sich der oben geschilderte Schaden auf Seiten der Klägerin manifestiert, gemäß § 287 Abs. 1 S. 1 ZPO nach seiner freien Überzeugung bestimmt.

a) Hinsichtlich der Höhe des Schadensersatzes ist zunächst zu berücksichtigen, dass die betroffene Person nach Erwägungsgrund 146 S. 6 einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten soll. Ferner soll dem Schadensersatzanspruch unter Berücksichtigung der Erwägungsgründe 75 und 85 eine abschreckende Wirkung zukommen und der Datenschutzgrundverordnung durch eine empfindliche Anspruchshöhe zu einer effektiven Geltung verhelfen werden (EuGH, Urteil vom 17.12.2015 - C-407/14, NJW 2016, 1080; Quaas in BeckOK, DSGVO, Art. 82 Rn. 31b). Kommt es jedoch zu einer großen Anzahl von Rechtsverstößen durch den gleichen Verantwortlichen, so ist die hohe abschreckende Wirkung ebenso in der Breite der Schadensersatzpflicht zu sehen, d.h. in der Summe aller immateriellen Ersatzansprüche (OLG Koblenz, Urteil vom 18.05.2022 - 5 U 2141/21, Rn. 93, juris). Im Übrigen sind innerstaatlichen Vorschriften heranzuziehen, solange die Grundsätze der Äquivalenz und der Effektivität beachtet werden (EuGH, Urteil vom 04.05.2023 - C-300/21, NZA 2023, S. 621 Rn. 59). Die Grundsätze des § 253 BGB sind mithin zu beachten. Die konkreten Umstände des Einzelfalles sind wesentlich.

b) Im streitgegenständlichen Fall hält das Gericht einen Betrag in Höhe von 1.000,00 € für erfor-

derlich, aber auch ausreichend.

Das Gericht verkennt hierbei nicht, dass es über die Beträge hinausgegangen ist, welche von der Rechtsprechung bisher in den Fällen im Zusammenhang mit dem Scraping-Vorfall bei Facebook zuerkannt wurden (vgl. LG Paderborn, 19.12.2022 - 3 O 99/22; LG Stuttgart, Urteil vom 26.01.2023 - 53 O 95/22; LG Heidelberg, Urteil vom 17.01.2023 - 7 O 10/22, Anlage K 4; LG Heidelberg, Urteil vom 17.01.2023 - 7 O 12/22, Anlage K 4; LG Heidelberg, Urteil vom 17.01.2023 - 7 O 14/22, Anlage K 4; LG Frankfurt a.M., Urteil vom 21.03.2023 - 2-18 O 114/22, Anlage K 4; LG Lüneburg, Urteil vom 25.05.2023 - 15 O 74/22). Der vorliegende Fall weicht jedoch in zwei entscheidenden Punkten von den besagten Entscheidungen ab, namentlich in den zur Überzeugung des Gerichts festgestellten Auswirkungen des Scraping-Vorfalles auf Seiten der Klägerin und deren Verhalten im Nachgang. Während in den aufgeführten Entscheidungen keine besondere persönliche Betroffenheit des Klägers vom Gericht festgestellt werden konnte (LG Paderborn, 19.12.2022 - 3 O 99/22, Rn. 146, juris; LG Heidelberg, Urteil vom 17.01.2023 - 7 O 12/22, Anlage K 4; LG Frankfurt a.M., Urteil vom 21.03.2023 - 2-18 O 114/22, Anlage K 4), die persönliche Betroffenheit sich auf etwa 3 Ping-Anrufe pro Monat über etwa 9 Monate erstreckte (LG Stuttgart, Urteil vom 26.01.2023 - 53 O 95/22, Rn. 106, juris) oder der Kläger im Nachgang nichts zu seinem Schutz unternommen hat (wie etwa die Handynummer zu wechseln oder die Datenschutzvorschriften zu ändern, LG Heidelberg, Urteil vom 17.01.2023 - 7 O 10/22, Anlage K 4; LG Heidelberg, Urteil vom 17.01.2023 - 7 O 14/22, Anlage K 4), sind die vorliegend festgestellten Auswirkungen deutlich gravierender. Die Klägerin erhielt im Zeitraum zwischen 2021 und 2022 teilweise fast täglich belästigende Telefonanrufe. Hinzu kamen die belästigenden E-Mails. Diese Belästigungen gingen tatsächlich so weit, dass sich die Klägerin eine neue Telefonnummer besorgt hat, um zukünftig keine dieser unerwünschten Anrufe mehr zu erhalten. Jedenfalls zum 21.07.2020 wurde die Suchbarkeitseinstellung hinsichtlich der Handynummer geändert und die Klägerin hat ihren Spam-Filter in Bezug auf die belästigenden E-Mails angepasst. Das Verhalten der Klägerin im Nachgang an den Scraping-Vorfall kann vorliegend daher keinesfalls Anspruchsmindernd berücksichtigt werden. Vielmehr ist insbesondere die Anschaffung einer neuen Handynummer und die damit verbundenen Unannehmlichkeiten Anspruchserhöhend zu berücksichtigen.

Schließlich hat das Gericht vorliegend berücksichtigt, dass der Beklagten mehrere schadensursächliche Verstöße gegen die DSGVO vorzuwerfen sind, welche einen sehr weitgehenden Kontrollverlust der personenbezogenen Daten der Klägerin ermöglicht und begünstigt haben.

6. Der geltend gemachte Zinsanspruch folgt aus §§ 288, 291 BGB.

II. Nachdem der Klägerin ein Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO zusteht, ist auch auf den Klageantrag zu 2 zu erkennen. Es ist nicht ausgeschlossen, dass die Klägerin künftig infolge der Verstöße der Beklagten gegen die DSGVO - auch - materielle Schäden erleidet. Dies zumal ein unkontrollierter Datenverlust eingetreten ist. Zwar hat sie mittlerweile eine andere als die „abgegriffene“ Handynummer. Ihre E-Mail-Adresse hat sie jedoch nicht gewechselt.

III. Darüber hinaus kann der Kläger die mit dem Klageantrag zu 3 beanspruchte Unterlassung - in weiten Teilen - erfolgreich gegenüber der Beklagten geltend machen.

1. Soweit es für den vorbeugenden Unterlassungsschutz eine gesonderte Anspruchsgrundlage in der DSGVO nicht gibt, bleibt im Hinblick auf die Vorgaben des Art. 79 DSGVO entweder ein Rückgriff auf § 823 Abs. 2, § 1004 BGB analog möglich, um Schutzlücken zu vermeiden (vgl. nur OLG München, Urteil vom 19.01.2021 - 18 U 7243/19, juris Rn. 62), oder ein solcher Anspruch folgt mit Blick auf die unrechtmäßige Datenverarbeitung seitens der Beklagten aus Art. 17 Abs. 1 lit. d DSGVO, falls man annimmt, aus dem dort normierten Lösungsrecht lasse sich auch ein Unterlassungsanspruch herleiten (vgl. BGH, Urteil vom 13.12.2022 - VI ZR 60/21 Rn. 10; zum Ganzen auch: OLG Frankfurt, Urteil vom 14.04.2022 - 3 U 21/20, GRUR-RS 2022, 10537

2. Die Beklagte hat - wie oben festgestellt - jedenfalls gegen Art. 13, Art. 25 Abs. 2 und Art. 32, 24, 5 Abs. 1 lit. f DSGVO verstoßen. Diese Rechtsverstöße geben dem Kläger einen darauf bezogenen Anspruch auf Beseitigung und künftige Unterlassung.

a) Daher kann der Kläger verlangen, dass die Beklagte es unterlässt, personenbezogenen Daten (Telefonnummer, Facebook-ID, Familienname, Vorname, Geschlecht, Stadt, Beziehungsstatus) unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen. In gleicher Weise kann der Kläger beanspruchen, dass die Beklagte es unterlässt, dass seine Mobilfunknummer trotz einer Einstellung auf „privat“ noch durch Verwendung des Contact-Im-

port-Tools verwendet werden kann, es sei denn, es wird ausdrücklich die Einwilligung hierzu erteilt.

b) Ausgenommen davon sind indes die Daten „Land“ und „Bundesland“, die - nach dem vom Kläger unbestritten gebliebenen Vorbringen der Beklagten - nicht Gegenstand der Angaben auf der Facebook-Plattform sind. Insoweit ist der Unterlassungsanspruch teilweise nicht begründet und daher abzuweisen.

c) Soweit die Beklagte darauf verweist, dass der Kläger durch eine Änderung der Einstellungen auf der Facebook-Plattform die von ihm gewünschte Rechtsfolge erreichen kann, steht dies Unterlassungsansprüchen der Klägerin nicht entgegen.

Durch mögliche, von der Klägerin selbst vorzunehmende Änderungen von Einstellungen in ihrem Facebook-Profil ist eine Wiederholungsgefahr nicht entfallen, und die Klägerin kann grundsätzlich Unterlassung jeder einmal getätigten rechtswidrigen Datenverarbeitung verlangen. Denn im Fall eines rechtswidrigen Eingriffs in ein geschütztes Rechtsgut des Betroffenen besteht nach ständiger Rechtsprechung des Bundesgerichtshofs eine tatsächliche Vermutung für das Vorliegen der Wiederholungsgefahr. An eine Entkräftung der Vermutung sind strenge Anforderungen zu stellen, im Regelfall bedarf es hierfür der Abgabe einer strafbewehrten Unterlassungsverpflichtungserklärung gegenüber dem Gläubiger des Unterlassungsanspruchs. Eine solche hat die Beklagte hier nicht abgegeben, sie geht vielmehr von der Wirksamkeit der von ihr angenommenen Einwilligung aus.

3. Die Ordnungsmittellandrohung folgt aus § 890 ZPO.

IV. Das im Klageantrag Ziffer 4 geltend gemachte Auskunftsverlangen kann keinen Erfolg haben. Insbesondere besteht kein Auskunftsanspruch aus Art. 15 DSGVO.

1. Art. 15 Abs. 1 Hs. 1, 2 DSGVO enthält zunächst einen Anspruch der betroffenen Person gegen

den Verantwortlichen, ihm zu bestätigen, ob ihn betreffende personenbezogene Daten verarbeitet werden. Verarbeitet der Verantwortliche personenbezogene Daten der betroffenen Person, so hat die betroffene Person gem. Art. 15 Abs. 1 Hs. 1, 2 DSGVO ein Recht auf Auskunft über diese personenbezogenen Daten. Der Klägerin steht daher grundsätzlich ein Auskunftsanspruch gegen die Beklagte als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO über die bei dieser verarbeiteten sie betreffenden personenbezogenen Daten zu.

2. Dieser Anspruch ist jedoch gemäß § 362 Abs. 1 BGB durch Erfüllung erloschen.

a) Den Auskunftsanspruch erfüllt der Verantwortliche indem er die verlangten Informationen nach Maßgabe des Art. 15 erteilt. Außerdem muss der Verantwortliche gem. Art. 15 Abs. 3 DSGVO eine Kopie der personenbezogenen Daten, die er verarbeitet, zur Verfügung stellen. Erfüllt im Sinne des § 362 Abs.1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die - gegebenenfalls konkludente - Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (vgl. BGH, Urteil vom 03.09.2020 - III ZR 136/18 = GRUR 2021,110). Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll.

b) So liegt es auch im vorliegenden Fall. Mit Schreiben vom 23.08.2021 hat die Beklagte in angemessener Weise mitgeteilt, welche personenbezogenen Daten verarbeitet werden, indem sie die Klägerin auf die Selbstbedienungstools verwiesen hat. Diese Erfüllungshandlung war ausreichend um den Erfüllungserfolg zu gewährleisten. Dem ist die Klägerin in der Replik auch nicht mehr entgegen getreten, sodass das Auskunftsbegehren hinsichtlich dieses Teilaspekts des Auskunftsanspruchs durch Erfüllung erloschen ist.

c) Soweit die Klägerin darüber hinaus Auskunft verlangt, "welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten" besteht ein Anspruch nicht.

Der Anspruch ist (ebenfalls) durch Erfüllung untergegangen, § 362 BGB. Die Beklagte hat mit der Klageerwiderung vorgetragen, über die Verarbeitungstätigkeiten Dritter (hier: "Scraper"), keine Angaben machen zu können. Unabhängig davon, ob die erteilte Auskunft unrichtig oder unvollständig ist, begründet die erteilte Auskunft jedenfalls keinen (weiteren) Auskunftsanspruch, da die Beklagte zum Ausdruck gebracht hat, das Auskunftsbegehren der Klägerin vollständig erfüllt zu haben.

3. Weitere Anspruchsgrundlagen für das Auskunftsverlangen der Klägerin sind nicht ersichtlich.

V. Im Rahmen des ihr zustehenden materiellen Schadensersatzanspruchs nach Art. 82 Abs. 1 DSGVO kann die Klägerin auch die Erstattung vorgerichtlich angefallener Rechtsanwaltsgebühren beanspruchen. Ausgehend von dem in Ansatz zu bringenden Gegenstandswert in Höhe von 11.000,00 € unterliegt die Klägerin lediglich im Hinblick auf Begehren, welchen das Gericht einen Wert von 800,00 € zumisst. Erfolgreich war die Klägerin damit mit 10.200,00 €. Insgesamt ergeben sich daher Gebühren nach Ziff. 2300, 7002, 7008 VV RVG i.H.v. 1.054,10 €. Beantragt wurden jedoch lediglich 887,03 €, so dass diese zuzusprechen sind. Sie sind nach §§ 288, 291 BGB zu verzinsen.

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

D. Die Entscheidung zur vorläufigen Vollstreckbarkeit beruht auf §§ 709 S. 1, 2 ZPO.

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 Ingolstadt
Auf der Schanz 37
85049 Ingolstadt

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.


Richter

Verkündet am 16.06.2023

gez.

Urkundsbeamtin der Geschäftsstelle



Für die Richtigkeit der Abschrift
Ingolstadt, 19.06.2023

Urkundsbeamtin der Geschäftsstelle