Aktenzeichen:
5 O 185/23

Landgericht Ellwangen (Jagst)

# Im Namen des Volkes

# Urteil

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **WBS.Legal**, Eupener Straße 67, 50933 Köln, Gz.:

gegen

**Meta Platforms Ireland Limited**, vertreten durch d. Geschäftsführer (Director) Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland
- Beklagte -

Prozessbevollmächtigte:
Rechtsanwälte **Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater Partnergesellschaft mbB**, Bockenheimer Anlage 44, 60322 Frankfurt, Gz.:

wegen Schadensersatz u.a.

hat das Landgericht Ellwangen (Jagst) - 5. Zivilkammer - durch den Vizepräsidenten des Landgerichts als Einzelrichter aufgrund der mündlichen Verhandlung vom 03.11.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger 500,00 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 01.08.2023 zu zahlen.

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

3. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 159,94 € zu zahlen zuzüglich Zinsen seit 01.08.2023 in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

4. Im Übrigen wird die Klage abgewiesen.

5. Von den Kosten des Rechtsstreits tragen der Kläger 6/7 und die Beklagte 1/7.

6. Das Urteil ist vorläufig vollstreckbar.

Dem Kläger wird nachgelassen, die Vollstreckung durch die Beklagte gegen Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet.

Der Beklagten wird nachgelassen, die Vollstreckung durch den Kläger gegen Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abzuwenden, wenn nicht der Kläger vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet.

Streitwert: 7.000,00 €.

(Antrag Ziffer 1.: 1.000,00 €;
Antrag Ziffer 2.: 500,00 €;
Antrag Ziffer 3.: 5.000,00 €,
Antrag Ziffer 4.: 500,00 €)

# Tatbestand

Der Kläger macht mit der vorliegenden Klage gegen die Beklagte Ansprüche auf Schadensersatz, Unterlassung und Auskunft wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung geltend.

Der Kläger unterhält ein Nutzerkonto bei der Social Media Platform „facebook.com“. Dieses nutzt er insbesondere, um mit Freunden zu kommunizieren, private Fotos zu teilen und mit anderen Nutzern im Netz zu diskutieren. Die Beklagte betreibt die zuvor benannte Plattform „facebook.com“ (nachfolgend Facebook) und der darauf enthaltenen Dienste. Ihre Dienste ermöglichen es Nutzern, persönliche Profile zu erstellen und mit Freunden zu teilen. Die Nutzer können auf ihren persönlichen Profilen Angaben zu verschiedenen Daten ihrer Person machen und in dem von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können.

Beim Anlegen eines Facebook-Profils wird der künftige Nutzer auf die Datenschutz- und Cookie Richtlinien hingewiesen. Diese sind durch eine Verlinkung getrennt abrufbar. Die Datenschutzeinstellungen enthalten dabei insbesondere Informationen darüber, welche der vom Nutzer erteilten Informationen immer öffentlich zugänglich sind (unter anderem Name, Geschlecht und Facebook-Id) und die Angabe, dass öffentlich zugängliche Informationen jeder, das heißt auch Personen außerhalb der Plattform, sehen kann. Nach der Anmeldung sind zunächst die Vor- bzw. Standardeinstellungen aktiv. Demnach können „alle“ Personen sehen, welche Seiten der Nutzer abonniert oder mit wem er befreundet ist. Ebenso können „alle“ den neuen Nutzer über seine E-Mail-Adresse und - sofern er diese angegeben hat - seine Telefonnummer finden. Der Nutzer kann diese Einstellungen individuell ändern und im Hilfebereich einlesen, wie Facebook insbesondere die Mobilfunknummer verwendet. Die Angabe der Mobilfunknummer ist dabei nicht zwingend. Entscheidet sich ein Nutzer jedoch diese anzugeben, kann er in den Suchfunktionen einstellen, in welchem Umfang er über diese gefunden werden will. Auch insoweit lautet die Grundeinstellung zunächst „alle“.

Die Beklagte betreibt auch eine Messenger-App als Applikation für Smartphones. Nutzer melden sich bei dieser mit ihrem bereits bestehenden Facebook-Profil an, sodass die Messenger-App und die Funktionen von Facebook über denselben Zugang zum Account verknüpft sind.

Anfang April 2021 wurden Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern im Internet öffentlich verbreitet. Bei den Datensätzen handelt es sich um Telefonnummern, FacebookID, Name, Vorname, Geschlecht und weitere korrelierende Daten, wobei streitig ist, ob hierzu auch Bundesland, Land, Stadt und Beziehungsstatus gehörten. Die Beklagte geht davon aus, dass das Contact-Import-Tool zur Bestimmung der Telefonnummern der einzelnen Benutzer genutzt wurde. Indem eine Vielzahl von Kontakten in ein virtuelles Adressbuch eingegeben wurde, gelang es Unbekannten, die Telefonnummern konkreten Facebook-Profilen zuzuordnen. Um die Telefonnummer jeweils zu korrelieren, wurden mit Hilfe des Contact-Import-Tools fiktive Nummern erzeugt und geprüft und die zugehörigen Facebook-Nutzer wurden angezeigt. Auf dem Profil des Nutzers wurde dieser dann besucht und von dort wurden die öffentlichen Daten gescrapt („abgeschöpft“).

Daraus resultierend wurden den Kläger betreffende Daten abgegriffen und im Internet auf Seiten veröffentlicht, die illegale Aktivitäten begünstigen sollen.

Die Einzelheiten hinsichtlich des Ablaufs des Scrapings sind zwischen den Parteien streitig. Dieses Sammeln von Daten mit Hilfe von automatisierten Tools und Methoden war und ist nach den Nutzungsbedingungen der Beklagten untersagt.

Mit E-Mail seiner Prozessbevollmächtigten vom 20.04.2023 (Anlage K 1, AH Kläger) ließ der Kläger die Beklagte zur Auskunft und zur Zahlung eines Schadensersatzes in Höhe von 1.000,00 € mit Fristsetzung auffordern. Weiter wurde die Beklagte in der E-Mail aufgefordert, vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 € binnen 4 Wochen zu zahlen. Mit anwaltlichem Schreiben vom 16.05.2023 (Anlage B 16, AH Beklagte) nahmen die Prozessbevollmächtigten der Beklagten zu der E-Mail vom 20.04.2023 im Einzelnen Stellung. Wegen der Einzelheiten wird auf die genannten Anlagen verwiesen.

Der Kläger ist der Auffassung,

die Beklagte verstoße gegen die DSGVO, indem sie ohne ausreichende Grundlage im Sinne der Art. 6 und 7 DSGVO Informationen im Sinne von Art. 13, 14 DSGVO verarbeite, Daten unbefugten Dritten zugänglich mache und hierbei die Pflichten aus Art. 5 Abs. lit. a, lit. b, lit. c, lit. f, 25 Abs. 1, Abs. 2, 32, 34 Abs. 1, Abs. 2 verletze sowie seine Betroffenenrechte gemäß Art. 15, 17 und 18 DSGVO verletze.

Der Kläger behauptet, das „scrapen“ sei nur möglich gewesen, weil die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten Tools zu verhindern und weil die Einstellungen zur Sicherheit der Telefonnummer auf Facebook so undurchsichtig und kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Nur so hätten auch seine Daten auf sog. Hackerforen wie „raidforums.com“ geraten können.

Facebook sei „datenschutzunfreundlich“ eingestellt, es werde unnötig zwischen Datenschutzrichtlinien und Cookie-Verwendung differenziert, obwohl die Verwendung von Cookies ein inhärent datenschutzrechtliches Thema sei. Der gesamte Anmeldevorgang sei intransparent und für den Anwender verwirrend. Dies führe letztlich dazu, dass Nutzer im Vertrauen und mit dem Ziel, mehr persönliche Sicherheit zu erreichen, ihre Telefonnummern auf Facebook preisgäben. Die neben der von der Beklagten betriebene Website noch betriebene Messenger-App als Schnittstelle für die Facebook-Applikation auf Mobilgeräten und die besagte Website seien miteinander verknüpft. Bei erster Anmeldung frage der Messenger-Dienst die Synchronisierung bereits an, ohne über die Risiken der Verwendung aufzuklären. Es könne separat auf der App eingestellt werden, ob eine Synchronisierung erfolgen solle, ohne über Risiken aufzuklären. Insgesamt gebe es drei verschiedene Einstellungsmöglichkeiten zur Verwendung der Telefonnummer, über die ein Nutzer keine transparenten Informationen für eine Gewährleistung einer effektiven digitalen Sicherheit erhalte. Diese Sicherheitslücke werde seit 2019 ausgenutzt, ohne dass die Beklagte etwas dagegen unternehme. Er habe so ungewollt die Kontrolle über seine Daten verloren und werde bis heute wiederholt ungewollt von Unbekannten via SMS und durch Anrufe kontaktiert. Auch nach dem Vorfall 2019 habe die Beklagte nicht adäquat reagiert. Sie habe versäumt, die zuständige Datenschutzbehörde, die „Irish Data Protection Commission“ unverzüglich zu informieren. Auch der Kläger sei nicht informiert worden. Soweit vorgerichtlich Auskünfte über abge-

griffene Daten mitgeteilt worden seien, sei diese Auskunft ungenügend.

Die Datenschutzeinstellungen der Beklagten seien undurchsichtig und kompliziert gestaltet, denn es bestehe eine Flut an Einstellungsmöglichkeiten allein für die Sicherheit der Mobilnummer. Aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte und nicht selbstständig ändere. Dies widerspräche allerdings den Grundsätzen eines nutzerfreundlichen Datenschutzes und dem in der DSGVO niedergelegten Prinzips der „privacy by default“ (=datenschutzfreundliche Voreinstellungen).

Die Auskunft, die er von der Beklagten erhalten habe, sei unzureichend. Das Antwortschreiben der Beklagten enthalte lediglich allgemein gehaltene Informationen zu den auf Facebook verarbeiteten Daten sowie einen Link zur Seite der Beklagten, auf der die Daten über einen individuellen Nutzer gespeicherten Daten eingesehen werden können. Dieses Vorgehen allein sei schon nicht geeignet, dem nach Art. 15 DSGVO umfassenden Auskunftsanspruch gerecht zu werden. Unabhängig davon enthalte das „Auskunftsschreiben“ der Beklagten aber auch keinerlei konkrete Aussagen dazu, welche Daten der Klägerseite im Wege des Scrapings von unbekannten Dritten abgegriffen wurden. So bleibe offen, wann genau die Daten entwendet worden seien oder wie viele verschiedene Beteiligte diese Funktion hinsichtlich seiner Daten ausgenutzt hätten.

Der Kläger 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 Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.

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

a.

personenbezogenen Daten der Klägerseite, namentlich 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-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 trägt vor und ist der Ansicht,

die Wiedergabe des Sachverhalts und des Vorgangs des sog. Scraping seien falsch. Der klägerische Vortrag beruhe auf einem Missverständnis zum Scraping als solchen. Es sei unschlüssig und unsubstantiiert, welche Daten des Klägers genau gescrapt worden sein sollen. Sie bestreitet die Begehung eines Datenschutzverstoßes und eines Unterlassens des Schließens einer technischen Schwachstelle. Vielmehr seien lediglich automatisch gesammelte öffentlich einsehbare Daten entweder von der App oder der Website Facebook gescraped worden. Es seien lediglich öffentlich einsehbare Daten durch Dritte in Form des Scraping abgerufen worden, was nach den Nutzungsbedingungen von Facebook untersagt gewesen sei und noch untersagt sei. Das Abrufen habe im Einklang mit den jeweiligen Privatsphäre-Einstellungen „öffentlich“ auf der Facebook-Plattform gestanden. Es seien allenfalls öffentlich einsehbare Daten abgerufen und an anderer Stelle erneut zugänglich gemacht worden. Sie stelle allen Nutzern, also auch dem Kläger, alle in Art. 13 und 14 DSGVO festgelegten Informationen zur Datenverarbeitung zur Verfügung, die sie zum Zeitpunkt der Datenerhebung im Anwendungsbereich der Datenrichtlinie durchführe. Sie ist daher der Ansicht, nicht gegen die Transparenzpflichten der DSGVO verstoßen zu haben. Es habe zudem eine umfassende und transparente Information über die Möglichkeit der Anpassung ihrer Suchbarkeits-Einstellungen und Zielgruppenauswahl gegeben, woraus sich nachvollziehbar ergebe, wer bestimmte persönliche Informationen, die der Nutzer in seinem Facebook-Profil hinterlegt habe, einsehen könne. Diese Einstellungen habe der Kläger jederzeit anpassen können.

Die Beklagte ist der Ansicht, nicht gegen Art. 24, 32 DSGVO verstoßen zu haben, sondern vielmehr angemessene technische und organisatorische Maßnahmen ergriffen zu haben, das Risiko von Scraping zu unterbinden und Maßnahmen zur Bekämpfung von Scraping zu ergreifen. Es fehle konkreter Vortrag, welche Maßnahmen in welchem Umfang nicht genügen würden. Außerdem müsse eine solche Beurteilung ex ante und nicht ex post erfolgen. Den Anforderungen des Art. 25 DSGVO sei genügt. Es dürfe dabei der zentrale Zweck von Facebook, sich mit Freunden, Familien und Gemeinschaften zu verbinden, nicht außer Be-

tracht bleiben. Es bestehe keine Melde- oder Benachrichtigungspflicht, da es an einer Verletzung der Sicherheit i.S.d. Art. 4 Nr. 12 DSGVO und an einer unbefugten Offenlegung von Daten fehle. Unabhängig davon habe sie wegen der Medienberichterstattung freiwillig eine Vielzahl von Maßnahmen ergriffen, über Scraping und Begrenzungsmöglichkeiten einschließlich einer Änderung von Privatsphäre-Einstellungen zu informieren.

Schließlich fehle es an einem immateriellen Schaden. Art. 82 DSGVO umfasse keine Verstöße gegen Art. 13-15, 24, 25 DSGVO. Zudem fehle es an einem Verstoß gegen Art. 82 DSGVO. Ein kompensationsgeeigneter messbarer Schaden sei auch nicht dargelegt. Selbst bei einem angenommenen vorübergehenden Kontrollverlust über personenbezogene Daten des Klägers wäre dies nicht ihr zuzurechnen, weil die öffentliche Einsehbarkeit den Privatsphäre-Einstellungen des Klägers entsprochen habe. Schließlich fehle es an einer schlüssigen Darlegung der Kausalität.

Mangels Verstoßes gegen die DSGVO sei der ohnehin unzulässige Feststellungsantrag unbegründet. Der Unterlassungsanspruch scheitere an einer Erstbegehungs- und einer Wiederholungsgefahr. Anwaltskosten seien mangels Verzuges unbegründet.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird im Übrigen auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen sowie auf die Sitzungsniederschrift vom 03.11.2023 (Bl. 282 bis 286 d. A.) Bezug genommen.

# Entscheidungsgründe

Die Klage ist zulässig und teilweise begründet.

**I.**

Die Klage ist zulässig. Das Landgericht Ellwangen (Jagst) ist sowohl international als auch sachlich und örtlich zuständig (1.). Die Klageanträge Ziff. 1) - 3) sind hinreichend bestimmt, es besteht ein Feststellungsinteresse (2.).

1.

a)
Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1, Alt. 2 EuGVVO.

aa)
Gemäß Art. 1 Abs. 1 EuGVVO ist diese sachlich anwendbar auf Zivilsachen, wie vorliegend gegeben.

bb)
Die Zuständigkeit der deutschen Gerichtsbarkeit folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 Alt. 2 EuGVVO. Ein ausschließlicher Gerichtstand gemäß Art. 24 EuGVVO ist hier nicht ersichtlich. 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.

Der Kläger ist gemäß Art. 17 Abs. 1 EuGVVO Verbraucher. Er gibt an, einen Nutzungsvertrag mit der Beklagten über die Nutzung der Social-Media-Plattform Facebook mittels eines Benutzerkontos zu privaten Zwecken geschlossen zu haben. Als doppelrelevante Tatsache reicht in der Zulässigkeit das Behaupten von Tatsachen, aus denen sich ein solcher vertraglicher Anspruchs ergeben kann.

cc)
Der Kläger hat seinen Wohnort in in Deutschland, sodass die deutsche Gerichtsbarkeit zuständig ist.

b)
Die internationale Zuständigkeit deutscher Gerichte ergibt sich ferner aus Art. 79 Abs. 2 DSGVO. Danach können Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

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 selbst erklärt, dass sie in den meisten Fälle die Rolle als Verantwortliche bekleide. Lediglich, wenn sie Werbekunden bediene, könne sie ausnahmsweise als Auftragsverarbeitende fungieren.

Der Kläger hat als Betroffener seinen Wohnsitz in Deutschland, weshalb die deutsche Gerichtsbarkeit international zuständig ist.

c)

Das Landgericht Ellwangen (Jagst) ist ferner sachlich gemäß §§ 23 Nr. 1, 71 Abs. 1 GVG sachlich zuständig, da der Streitwert vorliegend bei 7.000,00 € liegt. Es wird insofern auf die Ausführungen zum Streitwert unter III. 2. verwiesen.

d)

Darüber hinaus ist das Landgericht Ellwangen (Jagst) auch örtlich zuständig. 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 Ellwangen (Jagst) ist unabhängig davon nach Art. 79 Abs. 2 Satz 2 DS-GVO, § 44 Abs. 1 S. 2 BDSG örtlich zuständig (besonderer Gerichtsstand). Der Kläger hat seinen Wohnsitz in und damit im Bezirk des angerufenen Gerichts.

2.

Die Klageanträge Ziff. 1) und 3) sind hinreichend bestimmt (a), c)). Für den Feststellungsantrag Ziff. 2) besteht darüber hinaus ein Feststellungsinteresse (b)).

a)

Der Klageantrag Ziff. 1) ist hinreichend bestimmt iSv § 253 Abs. 2 Nr. 2 ZPO.

Grundsätzlich kann eine hinreichende Bestimmtheit des Antrags im Sinne des § 253 Abs. 2 Nr. 2 ZPO angenommen werden, wenn er den Anspruch konkret bezeichnet, den Rahmen der gerichtlichen Entscheidungsbefugnis erkennbar abgrenzt, den Inhalt und Umfang der materiellen Rechtskraft erkennen lässt, das Risiko des Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abwälzt und wenn er die Zwangsvollstreckung aus dem beantragten Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (BGH, Urteil vom 21. November 2017 - II ZR 180/15 -, juris, Rn. 8 m.w.N.). Der Klageantrag ist dabei der Auslegung zugänglich, wobei auch die Klagebegründung heranzuziehen ist (Zöller/Greger, ZPO, 34. Auflage, § 253 Rn. 13 m.w.N.).

Die Bemessung des Schmerzensgeldes in das Ermessen des Gerichts gestellt, weshalb die Stellung eines unbezifferten Antrags ausnahmsweise zulässig ist. Ein Verstoß gegen den in § 253 Abs. 2 Nr. 2 ZPO normierten Bestimmtheitsgrundsatz liegt dann nicht vor, wenn die Bestimmung des Betrages von einer gerichtlichen Schätzung nach § 287 ZPO oder vom billigen Ermessen des Gerichts abhängig ist (BGH, Urteil vom 1. Februar 1966 – VI ZR 196/64, juris Rn. 12). Die nötige Bestimmtheit wird durch umfassende Darlegung der Berechnungs- bzw. Schätzgrundlagen des Klägers im Rahmen der Klagebegründung sowie durch Nennung einer Größenordnung erreicht (Zöller/Greger, ZPO, 34. Aufl., § 253 ZPO Rn. 14).

Diese Voraussetzungen liegen vor. Sowohl in der Klagebegründung als auch im Klageantrag Ziff. 1) selbst, hat der Kläger einen Mindestbetrag in Höhe von 1.000,00 € angegeben.

b)
Der Klageantrag Ziff. 2) ist ebenso hinreichend bestimmt. Überdies liegt das notwendige Feststellungsinteresse vor.

Gemessen an vorstehenden Erwägungen genügt auch der Klageantrag Ziff. 2) dem vorbenannten Bestimmtheitserfordernis des § 253 Abs. 2 Nr. 2 ZPO. Denn dem Klageantrag Ziff. 2) lässt sich hinreichend bestimmt entnehmen, dass der Kläger festgestellt wissen will, dass die Beklagte verpflichtet ist, dem Kläger sämtliche künftige Schäden zu ersetzen, die dem Kläger aufgrund der missbräuchlichen Datenabgreifung entstanden sind bzw. noch entstehen werden. Die Verwendung der Vergangenheitsform „entstanden sind“ mag missverständlich sein und einer Auslegung offen stehen, führt aber nicht zur Unbestimmtheit des Klageantrags. Der Kläger hat ebenfalls die Zukunftsform „noch entstehen werden“ verwendet, die offensichtlich mit dem Ersatz „künftiger“ Schäden vereinbar ist.

Das notwendige Feststellungsinteresse gemäß § 256 ZPO hat der Kläger hinreichend dargetan. Denn das Feststellungsinteresse nach § 256 Abs. 1 ZPO liegt bei einer Verletzung eines absoluten Rechts oder eines vergleichbaren Rechtsguts bereits dann vor, wenn künftige Schadensfolgen möglich sind, auch wenn der Eintritt eines Schadens noch ungewiss ist. Dies wäre nur dann nicht der Fall, wenn aus Sicht des Klägers bei verständiger Würdi-

gung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (BGH, Beschluss vom 9. Januar 2007 - VI ZR 133/06, juris; BGH, Urteil vom 16. Januar 2001 - VI ZR 381/99, juris).

Bei den behaupteten Verstößen gegen die DSGVO mit der behauptet dargelegten unkontrollierten Nutzung gescrapter Daten ist bei verständiger Würdigung zumindest nicht ausgeschlossen, dass irgendein materieller oder immaterieller Schaden entstehen könnte. Denn der Kläger gibt an, ein solches Feststellungsinteresse wegen der behauptet einmal gescrapten Daten und damit behauptet einhergehenden unbefugten und unkontrollierten Datenverwendung zu haben, die auch zu künftigen Schäden führen könne, deren Art und Umfang noch unbekannt sind. Es ist daher nicht völlig ausgeschlossen, dass der Kläger infolge der Veröffentlichung seiner Daten einen irgendwie gearteten Schaden erleidet.

c)
Auch der Klageantrag Ziff. 3) ist hinreichend bestimmt.

Soweit die Beklagte rügt, dass die Formulierung „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ im Klageantrag Ziff. 3) zu unbestimmt sei, führt dies nicht zur Unzulässigkeit des Antrags.

Zwar darf ein Unterlassungsantrag nicht derart undeutlich gefasst sein, dass der Streitgegenstand und der Umfang der Prüfungs- und Entscheidungsbefugnis des Gerichts (§ 308 Absatz 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. Doch ist eine auslegungsbedürftige Antragsformulierung dann hinzunehmen, wenn eine weitergehende Konkretisierung nicht möglich und die gewählte Antragsformulierung zu Gewährleistung eines effektiven Rechtsschutzes erforderlich ist (BGH GRUR 2017, 422).

Gemessen an diesen Maßstäben ist der Klageantrag Ziff. 3) hinreichend bestimmt. Denn selbst bei einer Benennung derzeitiger möglicher Sicherheitsmaßnahmen würde dies in Anbetracht der technischen Weiterentwicklung alsbald dazu führen, dass die aktuellen Vorkehrungen veralten, sodass der Kläger erneut klagen müsste. Dies stünde einem effektiven

Rechtsschutz im Sinne des Art. 19 GG entgegen. Zudem wird aus der Klagebegründung deutlich, dass der Kläger Sicherheitsstandards verlangt, die möglichen (weiteren) Scraping-Angriffen vorbeugen. Die gesetzlich vorgeschrieben Sicherheitsstandards einzurichten ist jedoch zuvorderst die Aufgabe der Beklagten. Insoweit kann diese nicht von ihren Nutzern die konkrete Benennung der Sicherheitsmaßnahmen verlangen (LG Bielefeld GRUR-RS 2022, 38375).

**II.**

Der Kläger hat gegen die Beklagte einen Anspruch auf Ersatz immateriellen Schadens in Höhe von 500,00 € nebst Zinsen sowie auf Zahlung außergerichtlicher Rechtsanwaltskosten nebst Zinsen. Weiter kann er die Feststellung verlangen, dass die Beklagte für etwaige zukünftig eintretende Schäden haftet. Hinsichtlich weitergehender Ansprüche ist die Klage abzuweisen.

1.

Der Kläger hat gegen die Beklagte gemäß Art. 82 Abs. 1 DSGVO einen Anspruch auf immateriellen Schadensersatz in Höhe von 500,00 € aufgrund der Verletzungen von Vorschriften der DSGVO.

a)

Der zeitliche Anwendungsbereich der am 25.05.2018 in Kraft getretenen DSGVO (Art. 99 Abs. 2 DSGVO) ist eröffnet, da das „Scraping“ im Jahre 2021 erfolgte (OLG Stuttgart , Urteil vom 22.10.2023, Az. 4 U 20/23).

Soweit angenommen wird, dass die Weiterverarbeitung der Daten ab dem 25.05.2018 in Einklang mit der DSGVO zu bringen war (so OLG Hamm GRUR-RS 22505), ist eine

differenziertere Sichtweise erforderlich. Satz 2 des Erwägungsgrundes 171 zur DSGVO bestimmt ausdrücklich, dass Verarbeitungen, die zum Zeitpunkt der Anwendung der Verordnung bereits begonnen haben, innerhalb von zwei Jahren nach dem Inkrafttreten mit ihr in Einklang gebracht werden sollen, bestimmt also gerade keine Umsetzung bis zum 25.05.2018. Nach Erwägungsgrund 171 Satz 3 sind neue Einwilligungen nur erforderlich, wenn die bestehenden Einwilligungen nicht mehr den Anforderungen der DS-GVO entsprechen. Da insoweit eine Übergangsfrist eingeräumt worden ist, der Abgriff aber gerade innerhalb dieser Frist passiert ist, kann nicht auf Art. 13, 14 DSGVO abgestellt werden. Die Frage hinreichender Informationen ist entscheidend ist für die Reichweite, Wirksamkeit und Fortgeltung einer Einwilligung über den 25.05.2018 hinaus (OLG Stuttgart a.a.O.).

Der Beklagten kann für die Zeit vor dem 25.05.2018 auch kein Verstoß gegen die Verpflichtung zur Datenschutz-Folgenabschätzung aus Art. 35 DSGVO zur Last gelegt werden, denn Art. 35 Abs. 1 Satz 1 DSGVO verlangt, dass diese „vorab“, also vor dem Beginn des allgemein vorgesehenen Datenverarbeitungsvorgangs zu erfolgen hat, also vor der Zurverfügungstellung des KIT, beziehungsweise des Facebookdienstes und damit vor dem 25.05.2018. Allerdings bestimmt Art. 35 Abs. 11 DSGVO, dass der Verantwortliche erforderlichenfalls eine Überprüfung durchführt, um zu bewerten, ob die Verarbeitung weiter gemäß der Datenschutz-Folgenabschätzung durchgeführt wird. Dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind. Da der Datenabgriff als eine solche Änderung des Risikos anzusehen ist, war mit dem Bekanntwerden des Vorfalls eine Überprüfung vorzunehmen (OLG Stuttgart a.a.O.).

b)

Der sachliche Anwendungsbereich der DSGVO ist eröffnet, denn der Betrieb eines sozialen Netzwerks mit der Sammlung und Speicherung von Nutzerdaten (Name, ID. Geschlecht, Telefonnummer etc.), die Vernetzung der Mitglieder und die Beschickung mit individualisierter Werbung ist Verarbeitung und Speicherung von personenbezogenen Daten gemäß Art. 2 Abs. 1 DSGVO. Bei den genannten Daten handelt es sich um personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO (OLG Stuttgart a.a.O.).

c)

Die DSGVO ist auch räumlich anwendbar, da die Beklagte für ihre Tätigkeit eine Niederlassung innerhalb der Union in Irland betreibt (OLG Stuttgart a.a.O.).

d)

Der Kläger ist durch den Datenabgriff betroffen.

e)

Der Beklagten sind mehrere Verstöße gegen die DSGVO vorzuwerfen:

aa. Der Anspruch auf Schadenersatz nach Art. 82 Abs. 1 DSGVO setzt nicht voraus, dass eine Schutznorm verletzt wird oder eine rechtswidrige Datenverarbeitung vorliegt, es genügt jede Verletzung materieller oder formeller Bestimmungen der DS-GVO (OLG Stuttgart a.a.O.). Diese Auslegung ergib sich im Hinblick auf den weitern Wortlaut der Vorschrift und die Ausführungen im Erwägungsgrund 146 Satz 5 DS-GVO (OLG Stuttgart a.a.O.).

bb. Es kann letzten Endes offenbleiben, wer die Beweislast für das Vorliegen eines Verstoßes trägt, denn nach dem nicht bestrittenen Klägervortrag und den Einräumungen der Beklagten sind entsprechende Verstöße festzustellen, jedenfalls hat die Beklagte der sie treffenden sekundären Darlegungslast nicht genügt. Diese obliegt der Beklagten, da der Kläger keinen Einblick in die Datenverarbeitungsvorgänge der Beklagten hat.

Es ist jedoch nach den Ausführungen des EuGH im Urteil von 24.02.2022 (C-175/20), dem OLG Hamm (a.a.O.) und dem Schlussantrag des Generalanwalts im Verfahren C-340/21 (BGH GRUR RS 2023, 8707) davon auszugehen, dass die jeweilige Nachweispflicht für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten gem. Art. 5 DSGVO bei der Beklagten liegt. Für eine Beweislast bei der Beklagten spricht insoweit auch Art. 24 Abs. 1 Satz 1 DSGVO, wonach der Verantwortliche den Nachweis führen muss, dass die Verarbeitung im Einklang mit der DSGVO erfolgt. Da Art. 5 Abs. 1 DSGVO allgemeine Grundsätze enthält, die in den folgenden Vorschriften spezifiziert werden, erstreckt sich die Beweislast auch auf diese speziellen Vorschriften (OLG Stuttgart a.a.O.).

cc. Der Kläger hat hinreichend vorgetragen, den Abgriff welcher Daten er rügt (v.a. der Telefonnummer).

dd. Der Beklagten sind folgende Verstöße vorzuwerfen:

(1)

Verstoß gegen das Transparenzgebot (Art. 5 Abs. 1 lit. a) DSGVO).

Da die neue Datenrichtlinie und die Nutzungsbedingungen vom 19.04.2018 nicht den Anforderungen des DSGVO genügen, konnte die vorher erklärte Einwilligung keine Wirkung mehr entfalten, weshalb die Beklagte mit dem Inkrafttreten der DSGVO gegen das Transparenzgebot aus Art. 5 Abs. 1 lit. a) DSGVO verstoßen hat.

Da die neue Datenrichtlinie und die Nutzungsbedingungen vom 19.04.2018 nicht den Anforderungen des DSGVO genügen, konnte die vorher erklärte Einwilligung keine Wirkung mehr entfalten, weshalb die Beklagte mit dem Inkrafttreten der DSGVO gegen das Transparenzgebot aus Art. 5 Abs. 1 lit. a) DSGVO verstoßen hat.

Art. 5 Abs. 1 lit. a) DSGVO verlangt, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“). Art. 5 Abs. 1 DSGVO regelt diverse Grundsätze für die Verarbeitung personenbezogener Daten und enthält insoweit (neben Zielsetzungen und Zielvorstellungen) auch verbindliche Regelungen. Jede Verarbeitung personenbezogener Daten muss mit den in Art. 6 der Richtlinie 95/46 also der Vorgängerregelung zur DSGVO beziehungsweise Art. 5 der Verordnung 2016/679 aufgestellten Grundsätzen in Bezug auf die Qualität der Daten und mit einem der in Art. 7 der Richtlinie bzw. Art. 6 der Verordnung aufgeführten Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten im Einklang stehen (OLG Stuttgart a.a.O.).

Die Grundsätze der Nachvollziehbarkeit und der Transparenz bedeuten neben dem in Art. 13 DSGVO normierten Pflichtenkatalog, dass neben der Kenntnis über den Verantwortlichen und die Zwecke der Verarbeitung insoweit auch über die Risiken der Verarbeitung zu informieren ist, welche die betroffene Person kennen muss, um die Auswirkungen einer Verarbeitung auf sich einzuschätzen (Erwägungsgrund 39 Satz 5 DSGVO). Dazu gehören auch die Konsequenzen einer Verarbeitung. Wenn eine Verletzung bezüglich der Transparenzvorgaben festzustellen ist, liegt gleichzeitig eine rechtswidrige Verarbeitung vor.

Der Kläger hat Verstöße hinreichend substanziiert dargelegt: keine ausreichend transparente Hinweise für die Nutzung der Telefonnummer, es werde nur darauf hingewiesen, dass nur der Nutzer seine Telefonnummer einsehen könne, auf andere Möglichkeiten werde nicht hingewiesen; es sei nicht ausreichend über die Privatsphäreneinstellung informiert worden; die Verwendung der Telefonnummer im Rahmen der Anwendung des Kontakt-Import-Tools sei nicht erklärt worden; keine ausreichenden Sicherheitsmaßnahmen bzgl. des Kontakt-Import-Tools; die Einstellungen zur Sicherheit der Telefonnummer seien derart undurchsichtig, dass eine Nutzer tatsächlich keine sicheren Einstellungen erreichen kann.

In den von den Parteien vorgelegten Anlagen wird nicht darauf hingewiesen, dass bei einer Nutzung des Kontakt-Import-Tools auch bei einer Beschränkung der Telefoneinstellungen die Möglichkeit eines Zugriffs auf das Konto gegeben ist, weshalb objektiv keine ausreichende Information über diese Verarbeitungsmöglichkeit erfolgte. Da zur Verarbeitung auch jede andere Form der Bereitstellung von Daten gehört (Art. 4 Nr. 2 DSGVO), liegt insoweit eine rechtswidrige Verarbeitung vor. Der Kläger hat in diesem Zusammenhang zutreffend ausgeführt, dass insgesamt nicht ausreichend transparent und vor allem übersichtlich dargestellt wird, unter welchen Bedingungen die Nummer von der Beklagten überhaupt verarbeitet wird. Da die Beklagte jedoch nach dem übereinstimmenden Vortrag der Parteien bis zu dem Scraping-Vorfall keine Kenntnis davon hatte, dass in ihrem Kontakt-Import-Tool eine Schwachstelle bestand, über die ein Auslesen und Verknüpfen der Daten möglich war, ist zwar objektiv ein Transparenzverstoß anzunehmen. Allerdings kann der für die Datenverarbeitung Verantwortliche nur über das informieren, was ihm tatsächlich positiv bekannt ist, weshalb im Ergebnis bezüglich der fehlenden Information über die Verarbeitungsmöglichkeit kein vorwerfbarer Verstoß festgestellt werden kann.

Allerdings ist mit dem OLG Hamm (a.a.O.) und dem OLG Stuttgart (a.a.O.) davon auszugehen, dass die Einwilligung vor dem 25.05.2018 ohne Relevanz bleibt und das spätere Schweigen des Klägers auf die unveränderte bloße opt-out-Möglichkeit bezüglich der Suchbarkeit unwirksam war (Art. 5 Abs. 1 lit a), 6 Abs. 1 Unterabs. 1 lit a) DSGVO). Nach Art. 6 Abs. 1 Unterabs. 1 lit. a) DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn und soweit die betroffene Person ihre Einwilligung freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich im Sinne von Art. 4

Nr. 11 DSGVO für einen oder mehrere bestimmte Zwecke erteilt hat (EuGH GRUR-RS 2023, 15772; OLG Hamm a.a.O.). Insoweit ist auch der Transparenzgrundsatz zu berücksichtigen (OLG Hamm a.a.O.). In den von den Parteien vorgelegten Anlagen wird nicht darauf hingewiesen, dass bei einer Nutzung des Kontakt-Import-Tools auch bei einer Beschränkung der Telefoneinstellungen die Möglichkeit eines Zugriffs auf das Konto gegeben ist, weshalb die Einwilligung unwirksam ist (OLG Hamm a.a.O.; OLG Stuttgart a.a.O.). Der Europäische Gerichtshof hat zudem entschieden, dass bei Voreinstellungen mit einer sogenannten Abwahlmöglichkeit (Opt-out-Voreinstellung) nicht von einer wirksamen Einwilligung in die Datenverarbeitung ausgegangen werden kann, weil die Einwilligung ein aktives Verhalten erfordert (Art 4 Nr. 11 DSGVO), bei einer entsprechenden Voreinstellung die tatsächliche Einwilligung objektiv nicht geklärt werden kann, jedenfalls unklar bleibt, ob die Einwilligung in Kenntnis der Sachlage abgegeben wurde (EuGH MMR 2019, 732). Deshalb ergibt sich auch aus der Tatsache, dass die Suchbarkeit im Zeitpunkt der Änderung der AGB weiter aus „alle“ eingestellt war und nur eine opt-out-Lösung vorgesehen war, dass keine wirksame Einwilligung vorlag (OLG Hamm a.a.O., OLG Stuttgart a.a.O.).

(2)

Keine ausreichenden Sicherungsmaßnahmen (Art. 5 Abs. 1 lit. f) DSGVO)

Da eine Datenverarbeitung schon dann vorliegt, wenn ein automatisierter Zugriff auf Daten möglich ist, nach dem Schutzzweck der DSGVO insoweit auch kein willensgesteuertes Verhalten erforderlich ist (unbeabsichtigte Beeinträchtigungen genügen), hat die Beklagte keine ausreichenden Sicherungsmaßnahmen ergriffen. Der Datenschutzverstoß liegt insoweit in der ungeschützten Bereitstellung der Daten.

Art. 5 Abs. 1 lit. f) DSGVO verlangt, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit”). Der Begriff der Vertraulichkeit zielt auf den Schutz der Daten vor unbefugter Kenntnisnahme und damit unbefugter Verarbeitung. Die Daten sollen vor ge-

planten Zugriffen und unbeabsichtigten Beeinträchtigungen geschützt werden. Hierzu gehört nach Erwägungsgrund 39 Satz 12 DSGVO, dass unbefugte Personen weder Zugang zu den Daten, noch zu den Geräten haben, mit denen sie verarbeitet werden. Welche Maßnahmen zum Schutz der Daten ergriffen werden müssen, hängt insbesondere vom Risiko eines unberechtigten Zugriffs und der Art der Verarbeitung ab (EuGH NJW 2014, 2169).

Art. 32 Abs. 1 DSGVO konkretisiert, dass 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 hat, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zur danach geforderten Datensicherheit gehört auch der Schutz der Daten vor Verlust, Schädigung und Missbrauch, also auch davor, dass Dritte die Daten unbefugt oder unrechtmäßig verarbeiten. Verantwortliche und Auftragsverarbeiter müssen die Risiken ihrer jeweiligen Verarbeitung reflektieren und risikoadäquate Maßnahmen ergreifen, um ein möglichst hohes Maß an Verarbeitungssicherheit zu erreichen (OLG Stuttgart a.a.O.).

Der Begriff „Verarbeitung“, wie er in Art. 4 Nr. 2 DSGVO definiert wird, ist nach dem Willen des Unionsgesetzgebers mit der Formulierung „jede[r] Vorgang“ weit zu fassen und stellt keine erschöpfende Aufzählung von Vorgängen im Zusammenhang mit personenbezogenen Daten oder Sätzen solcher Daten – wie etwa Erheben, Erfassen, Speicherung und Abfragen – dar (EuGH BeckRS 2023, 14515). Verarbeitung von Daten ist danach jede Form der Bereitstellung, weshalb der Vortrag der Beklagten, der Abgriff sei keine Folge eines Datenverarbeitungsvorgangs in dieser Form nicht zutrifft.

Durch die Möglichkeit eines Zugriffs auf die persönlichen Daten des Klägers im Kontakt-Import-Tool hat die Beklagte gegen Art. 5 Abs. 1 lit. f) DSGVO verstoßen, denn zur Verarbeitung von Daten zählt auch jede Form der gegebenenfalls auch nicht beabsichtigten Bereitstellung von Daten (Art. 4 Nr. 2 DSGVO), zumal nach der englischen Sprachfassung (otherwise making available) die bloße Zugriffsmöglichkeit genügt. Die Beklagte hat durch die standardmäßige Voreinstellung, dass die Telefonnummer von „jedermann“ aufgefunden werden kann, nicht den Vorgaben aus Art. 5 Abs. 1 lit. f) und 25 Abs. 2 DSGVO genügt (OLG Hamm a.a.O., OLG Stuttgart a.a.O.).

Durch die eingeräumte Möglichkeit des Hochladens von Telefonnummern für eine Verknüpfung der Kontakte wurden die persönlichen Daten des Klägers (Name, Facebook-ID etc.) für eine Verknüpfung bereitgestellt beziehungsweise zur Verfügung gestellt, weshalb eine Zugriffsmöglichkeit vorhanden war, die nach den Nutzungsbedingungen der Beklagten untersagt ist (OLG Hamm a.a.O., OLG Stuttgart a.a.O.). Insoweit ist kein ausreichender Schutz der persönlichen Daten des Klägers vorhanden gewesen.

Soweit die Beklagte auf dem Standpunkt steht, es fehle an einem Verstoß, da die Telefonnummern von den Scrapern bereitgestellt worden seien und nur Informationen eingesammelt wurden, die ohnehin öffentlich einsehbar waren, kann der Senat dieser Auffassung nicht folgen. Die Beklagte hat selbst ausdrücklich eingeräumt, dass nach ihren Nutzungsbedingungen der Abgriff untersagt war, weshalb sie selbst von einer Rechtswidrigkeit des Verhaltens ausgeht. Angesichts des Schutzzwecks der DSGVO, den Schutz personenbezogener Daten zu gewährleisten, kommt es nicht darauf an, dass die (fingierten) Telefonnummern von den Scrapern stammten, zumal ein Zugriff auf die übrigen Daten und eine Verknüpfung ermöglicht wurde, die gerade nicht erwünscht war. Die personenbezogenen Daten (Name etc.) hätten nicht abgefragt und zugeordnet werden können, wenn nicht diese Schwachstelle vorhanden gewesen wäre (OLG Hamm a.a.O., OLG Stuttgart a.a.O.).

Die Beklagte verneint das Vorliegen einer Schwachstelle, legt aber jedenfalls im Rahmen der sie treffenden sekundären Darlegungslast nicht ausreichend dar, warum dann dennoch ein Zugriff und die Verknüpfung möglich waren.

(3)

Keine geeigneten Maßnahmen zur Umsetzung der Datenschutzgrundsätze (Art. 25 Abs. 1 DSGVO)

Nach Art. 25 Abs. 1 DSGVO ist der Verantwortliche verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Datenschutzgrundsätze (z.B. Datenminimierung) wirksam umzusetzen, die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. Aus den obigen Ausführungen ergibt sich außerdem ein Verstoß gegen Art. 5 Abs. 1 lit. b), 25 Abs. 1 DSGVO (ebenso OLG

Hamm GRUR-RS 2023, 22505 Rn. 130).

(4)

Keine ausreichenden datenschutzfreundlichen Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Die Voreinstellung einer Zugriffsmöglichkeit auf die Telefonnummer für jedermann hat gegen die Vorgaben aus Art. 25 Abs. 2 DSGVO verstoßen.

Art. 25 Abs. 2 DSGVO die Verpflichtung des Verantwortlichen, datenschutzfreundliche Voreinstellungen vorzunehmen. Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch die Voreinstellung nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist (Art. 25 Abs. 2 Satz 1 DSGVO). Die Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit (Art. 25 Abs. 2 Satz 2 DS-GVO). Diese Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Anzahl von natürlichen Personen zugänglich gemacht werden (Art. 25 Abs. 2 Satz 3 DS-GVO).

Der Europäische Gerichtshof hat in diesem Zusammenhang entschieden, dass bei Voreinstellungen mit einer sogenannten Abwahlmöglichkeit (Opt-out-Voreinstellung) nicht von einer wirksamen Einwilligung in die Datenverarbeitung ausgegangen werden kann, weil die Einwilligung ein aktives Verhalten erfordert (Art 4 Nr. 11 DSGVO), bei einer entsprechenden Voreinstellung die tatsächliche Einwilligung objektiv nicht geklärt werden kann, jedenfalls unklar bleibt, ob die Einwilligung in Kenntnis der Sachlage abgegeben wurde (EuGH MMR 2019, 732). Art. 25 Abs. 2 DSGVO enthält damit nach Wortlaut und Systematik ein sogenanntes Opt-out-Verbot für nicht erforderliche Daten. Erforderlich sind Daten, wenn der Verarbeitungszweck ohne sie nicht zu erreichen ist. Diese Voraussetzung ist restriktiv auszulegen; Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten müssen sich auf das absolut Notwendige beschränken (EuGH GRUR 2021, 1067 Rn. 110; BGH Urteil vom 12.10.2021, VI ZR 488/19 Rn. 30). In der Wahl des Verarbeitungszwecks ist der Verantwortliche allerdings

weitgehend frei. Art. 5 Abs. 1 lit. b) DSGVO gebietet es lediglich, einen eindeutigen und legitimen, rechtlich zulässigen Zweck zu wählen. Nicht erforderliche Daten sind demnach solche, die der Verantwortliche nicht notwendig verarbeiten muss. Hinsichtlich der Voreinstellungen ist die bloße Abwahlmöglichkeit insoweit dann nicht ausreichend. Danach ist durch die standardmäßige Konfiguration von (Privatsphäre-) Einstellungen zu gewährleisten, dass Nutzer eines sozialen Netzwerks die nicht erforderlichen Daten nur den Personenkreisen und nur in dem Umfang zugänglich machen, den sie vorab selbst festgelegt haben. Die Verpflichtung gilt nach Art. 25 Abs. 2 Satz 3 DSGVO insbesondere auch für die Zugänglichkeit der Daten, also die tatsächliche Möglichkeit, auf die Daten zuzugreifen. Die auf soziale Netzwerke zugeschnittene Regelung soll es den betroffenen Nutzern ermöglichen, den Kreis der Empfänger ihrer Nachrichten oder sonstigen Aktivitäten selbst zu steuern. Als Voreinstellung ist der kleinstmögliche Empfängerkreis vorzusehen. Deshalb kann der Auffassung der Beklagten nicht gefolgt werden, dass Art. 25 DSGVO keine Vorgaben für konkrete Datenverarbeitungsvorgänge macht – die Frage der möglichst engen Voreinstellungen betrifft konkret die Verarbeitung von Daten.

Die Bejahung dieses Verstoßes führt auch zu einer nicht rechtmäßigen Verarbeitung nach Art. 5 Abs. 1 lit. a) DSGVO.

Die DSGVO geht zudem im Ausgangspunkt davon aus, dass jede Verarbeitung personenbezogener Daten zunächst einmal unzulässig ist, wenn nicht ein Erlaubnistatbestand vorliegt. Art. 6 Abs. 1 Satz 1 DSGVO (soweit einschlägig) knüpft die Rechtmäßigkeit der Verarbeitung an verschiedene Voraussetzungen, u.a. an eine wirksame Einwilligung.

Die Einwilligung muss nach dem Erwägungsgrund 32 DSGVO durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Eine wirksame Einwilligung liegt insbesondere nicht vor, wenn die Speicherung oder der Zugriff durch Voreinstellungen erlaubt wird, die der Nutzer abwählen muss (also keine opt-out-Einwilligung; EuGH MMR 2019, 732, OLG Stuttgart a.a.O.). Eine Einwilligung in die Möglichkeit eines Datenabgriffs wurde nicht erklärt.

Mittels einer Telefonnummernaufzählung konnten über die Kontakt-Import-Funktion die

Nummern in Abhängigkeit von den Suchbarkeits-Einstellungen mit den dazugehörigen Facebookkonten verbunden werden.

Es mag zwar zutreffen, dass angesichts des Zwecks der Plattform die (weitere) Möglichkeit des Auffindens des Nutzerkontos über die Handynummer wünschenswert oder nützlich gewesen ist, diese diente aber nicht der Wahrung berechtigter Interessen und war auch nicht erforderlich (Art. 6 Abs. 1 Satz 1 lit. b) und f) DSGVO).

Auch wenn hinsichtlich der Zwecke eine weitgehende Freiheit des Verantwortlichen bestehen mag, muss insbesondere sichergestellt sein, dass die Daten nicht ohne eine ausdrückliche Einwilligung des Betroffenen einer unbestimmten Anzahl von Person zugänglich gemacht werden, es sei denn, der Betroffene hat dies ausdrücklich so voreingestellt. Die Erfassung der Telefonnummer war und ist für die Nutzung der Plattform und für den Betrieb jedoch nicht unabdingbar notwendig, weil der Nutzer unter seinem Namen aufgefunden werden kann, auch wenn es dann gegebenenfalls mehrere Treffer geben mag. Das zeigt sich insbesondere auch daran, dass sämtliche Voreinstellungen, um die es hier geht, ohne weiteres abgewählt werden können, ohne dass dies ersichtlich der weiteren Vertragsdurchführung entgegensteht, weil sie ansonsten nicht für eine Abwahl vorgesehen wären (OLG Stuttgart a.a.O.).

Die Bereitstellung der Daten im Kontakt-Import-Tool war nicht zur Vertragserfüllung erforderlich, da diese nicht dazu diente, Gemeinschaften zu bilden und die Welt näher zusammenzubringen (so der von der Beklagten vorgetragene Unternehmenszweck), auch nicht dazu diente für den Kläger neue Kontakte und andere Nutzer zu finden. Jedenfalls erfolgte die Bereitstellung insoweit nicht auf ausdrückliche Anfrage des Klägers. Soweit die Beklagte insoweit auf den Zweck der Bereitstellung eines sozialen Netzwerks abstellen mag, mag der Verarbeitungszweck die Öffentlichkeit des Namens erfordert haben, weil nur so eine Auffindbarkeit möglich ist, dies gilt aber gerade nicht für weitere Daten, insbesondere die Telefonnummer. Die fehlende Erforderlichkeit ergibt sich auch daraus, dass die Suchbarkeit seit 06.06.2019 vollständig deaktiviert worden ist (OLG Hamm a.a.O., OLG Stuttgart a.a.O.).

Die von der Beklagten vorgetragenen Zwecke – Ermöglichung der Verbindung von Menschen, Unterstützung bei der Suche und Auffindbarkeit anderer Nutzer – erlauben es der Beklagten nicht, den Umfang der zulässigen Datenverarbeitung auszuweiten. Der

durch das Recht auf informationelle Selbstbestimmung gewährleistete Schutz würde ebenso wie die Bindung der Datenverarbeitung an die Erforderlichkeit zur Vertragserfüllung durch Art. 6 Abs. 1 lit. b) DSGVO erheblich beeinträchtigt, wenn ein marktbeherrschendes Unternehmen wie die Beklagte die Bedeutung des Zugangs zu seinem sozialen Netzwerk uneingeschränkt dazu ausnutzen könnte, durch die Definition seines Leistungsangebots den Umfang der zulässigen Datenverarbeitung unter Hintanstellung der Nutzerinteressen allein an seinem Interesse an der Vermarktung eines durch die Internetnutzung innerhalb und außerhalb von Facebook generierten Bestandes personenbezogener Daten seiner Nutzer auszurichten und über das für die Benutzung des sozialen Netzwerks erforderliche Maß auszuweiten (BGH GRUR-RS 2020, 20737 Rn. 110; OLG Stuttgart a.a.O.).

(5)

Verstoß gegen die erforderliche Datenschutz-Folgenabschätzung (Art 35 DSGVO).

Die Beklagte hat nicht ausreichend sekundär vorgetragen, welche Schutzmaßnahmen bezüglich des Kontakt-Import-Tools seit Mai 2018 vorgesehen waren, weshalb im Grundsatz von einem Verstoß auszugehen ist.

Art 35 Abs. 1 DSGVO verlangt vom Verantwortlichen eine sogenannte Datenschutz-Folgenabschätzung, wenn eine Form der Datenverarbeitung aufgrund Art, Umfang, Umständen und Zwecken der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der natürlichen Personen zur Folge haben kann.

Die Risikobewertung verlangt eine Prognose, mit welch hoher Wahrscheinlichkeit ein hoher oder im Ausmaß unbekannter physischer, materieller oder immaterieller Schaden eintritt oder ein erwarteter Vorteil ausbleibt. Der Verantwortliche soll die Datenschutz-Folgenabschätzung vor der Verarbeitung durchführen, mit der die spezifische Eintrittswahrscheinlichkeit und die Schwere dieses hohen Risikos unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Ursachen des Risikos bewertet werden. Diese Folgenabschätzung sollte sich insbesondere mit den Maßnahmen, Garantien und Verfahren befassen, durch die dieses Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen der DSGVO nachgewiesen werden soll (Erwägungsgrund 90).

Hinsichtlich der Schäden stellt Erwägungsgrund 85 der DSGVO ab auf den Verlust der Kontrolle über die personenbezogenen Daten, die Einschränkung von Rechten, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.

Gegenstand der Abschätzung ist die Rechtmäßigkeit des geplanten Datenverarbeitungsverfahrens, weil nur so das Ziel der Abschätzung erreicht werden kann.

Für langfristig angelegte Datenverarbeitungsvorgänge, die bereits vor der Geltung der DSGVO begonnen haben – also vor dem 25.05.2018 (Art. 99 Abs. 2 DSGVO), besteht grundsätzlich keine Pflicht zur Folgenabschätzung, soweit es sich um den gleichen Vorgang handelt.

Der Kläger hat bestritten, dass die Beklagte überhaupt eine Datenschutzfolgenabschätzung vorgenommen hat, die Beklagte stellt insoweit auf die von ihr ergriffenen Sicherheitsmaßnahmen ab, um Scraping zu verhindern.

Da auch insoweit zumindest die Grundsätze der sekundären Darlegungs- und Behauptungslast gelten, weil der Kläger keinen Einblick in diese internen Vorgänge der Beklagten hat, der ein substantiierter Gegenvortrag unschwer möglich und zumutbar ist, genügt die pauschale Behauptung des Klägers, die insoweit gemäß § 138 Abs. 3 ZPO als unstreitig zu behandeln ist. Danach hat die Beklagte die notwendige Folgenabschätzung nicht vorgenommen.

(6)

Verstöße gegen Informationspflichten (Art. 13, 14 DSGVO) liegen nicht vor, da das Nutzerkonto bereits vor dem Inkrafttreten der DSGVO eingerichtet wurde und die Beklagte bis zum Scraping-Vorfall keine Kenntnis von der Schwachstelle im Kontakt-Import-Tool bestand. Eine Information kann nur über positiv bekanntes erfolgen (OLG Stuttgart a.a.O.).

(7)

Ein Verstoß gegen Melde- und Benachrichtigungspflichten (Art. 33, 34 DSGVO) ist nicht kausal für den geltend gemachten Schaden, da der (unterstellte) Verstoß keinen weiteren Schaden ausgelöst hat (OLG Stuttgart a.a.O.).

f)

Dem Kläger ist durch die Verstöße der Beklagten gegen die genannten Vorschriften der DSGVO ein immaterieller Schaden im Sinne des Art. 82 Abs. 1 DSGO entstanden.

aa)

Der Begriff des Schadens ist gemäß Erwägungsgrund 146 S. 3 DSGVO weit auf eine Art und Weise auszulegen, die den Zielen dieser Verordnung in vollem Umfang entspricht. Für einen Schadensersatzanspruch nach Art. 82 DSGVO reicht allerdings der bloße Verstoß gegen die Bestimmungen der DSGVO nicht aus. Es muss ein Schaden vorliegen (EuGH, Urteil vom 4. Mai 2023 - C-300/21 -, juris Rn. 33 ff.). Der Ersatz eines immateriellen Schadens nach Art. 82 DSGVO ist aber nicht davon abhängig, dass der entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht (EuGH, aaO, Rn. 45), so dass auch Bagatellschäden einen Schadensersatzanspruch begründen. Zu berücksichtigen ist weiter, dass der Unionsgesetzgeber unter dem Begriff „Schaden“ insbesondere auch den bloßen „Verlust der Kontrolle“ über eigene Daten infolge eines Verstoßes gegen die DSGVO fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte (EuGH, Urteil vom 14. Dezember 2023, C-340/21 Rn. 82, juris). Das Gericht hat deshalb zu prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann (EuGH, aaO, Rn. 85) Art. 82 Abs. 1 DSGVO ist mithin so auszulegen, dass allein der Umstand, dass eine betroffene Person infolge eines Verstoßes gegen die DSGVO befürchtet, dass ihre personenbezogenen Daten durch Dritte missbräuchlich verwendet werden könnten, einen „immateriellen Schaden“ im Sinne dieser Bestimmung darstellen kann (EuGH, aaO, Rn. 86).

bb)

Ein Schaden kann deshalb auch bereits in einem unguten Gefühl, in der Angst und Besorgnis liegen, dass personenbezogene Daten Unbefugten bekannt geworden sind, wenn die Gefahr besteht, dass die Daten unbefugt weiterverwendet werden (vgl. LG Freiburg, Urteil vom 15.09.2023 - 8 O 184/22 Rn. 102, juris).

cc)

Im vorliegenden Fall trat der immaterielle Schaden durch die aufgrund des Scrapings bei dem Kläger nachvollziehbar ausgelöste Besorgnis bezüglich des weiteren Schicksals seiner persönlichen Daten ein, die damit - als ein mit seiner Telefonnummer verknüpfter Datensatz - im Netz kursierten. Denn dadurch erlitt dieser einen Kontrollverlust über seine Daten, der vorliegend mit dem Subjektiv besorgniserregenden Risiko einherging, dass diese Daten etwa durch Identitätsdiebstahl unbefugt und schadensträchtig genutzt werden. Zu dieser allgemeinen Besorgnis treten die in der informatorischen Anhörung glaubhaft vom Kläger geschilderten Anrufe und Nachrichten. Der Kläger hat glaubhaft geschildert, dass er den Eindruck hat, dass sich das in der weiteren Zeit immer mehr verstärkt hat, dass das mehr geworden sei (Sitzungsniederschrift, Bl. 283 d. A.). Es sei so, dass er mindestens fünf- bis sechsmal in der Woche Anrufe bekomme, die er auf solche Undichtigkeiten zurückführe. Das sei auch mit der Zeit immer mehr geworden. Weiter hat er angegeben, dass er ein Nebengewerbe als Trockenbauer betreibe und es so sei, dass er dann schon ans Telefon ran müsse, weil es ja sein könne, dass ein Kunde sich melde oder dass es etwa Lieferschwierigkeiten gibt, was in letzter Zeit öfter vorgekommen sei und dann gehe er ans Telefon und dann kriege er solche Schwachsinnsanrufe. Er werde dann jedes Mal gestört, wenn er arbeite und werde da unterbrochen.

dd)

Die erforderliche Kausalität zwischen den Verstößen der Beklagten gegen die DSGVO und dem Schaden des Klägers liegt vor. Aus der persönlichen Anhörung des Klägers ergibt sich deutlich, dass er über seine Telefonnummer jedenfalls auf diese Weise nicht gefunden

werden wollte. Entsprechend hat die gegen Art. 25 Abs. 2 DSGVO verstoßene datenschutzunfreundliche Standardvoreinstellung der Suchbarkeit über die Telefonnummer auf „für alle“ zur Schadensentstehung beigetragen. Schließlich ist der Schaden auch kausal auf den Verstoß der Beklagten gegen Art. 24, 32, 5 Abs. 1 f DSGVO zurückzuführen, denn durch die unzureichenden Schutzmaßnahmen ermöglichte die Beklagte das missbräuchliche Abgreifen der Daten. Das Gericht ist auch davon überzeugt, dass die von der Klagepartei geschilderten Spamanrufe und Nachrichten auf dem vorliegenden Scraping-Sachverhalt beruhen. Dies folgt aus dem zeitlichen Zusammenhang zwischen dem Datenvorfall im Jahr 2019 und der anschließenden Veröffentlichung der Daten seit 2020. Es ist nicht ersichtlich, woher die Anrufer die Nummer des Klägers sonst erlangt haben sollten.

g)

Der Kläger hat Anspruch auf Zahlung eines immateriellen Schadensersatzes in Höhe von 500,00 €.

aa)

Bei der Bestimmung des vom Kläger in das Ermessen des Gerichts gestellten Höhe des Schadensersatzes gemäß § 287 Abs. 1 Satz 1 ZPO sind alle Umstände des Einzelfalls zu würdigen. Die Kriterien des Art. 83 Abs. 2 DSGVO, die Anhaltspunkte für die Höhe der von der Aufsichtsbehörde zu verhängenden Geldbuße geben sollen, können auch für die Bemessung des immateriellen Schadensersatzes herangezogen werden. Danach sind unter anderem Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der Verarbeitung, der Grad des Verschuldens, Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens sowie die Kategorien der personenbezogenen Daten zu berücksichtigen. Gemäß Erwägungsgrund 146 S. 6 DSGVO sollen die betroffenen Personen einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten. Schadensersatzforderungen sollen abschrecken und weiter Verstöße unattraktiv machen.

bb)

Das Gericht hält unter Berücksichtigung der Ausgleichs- und Genugtuungsfunktion sowie der generalpräventiven Funktion des immateriellen Schadensersatzes einen Betrag in Höhe von 500,00 € für erforderlich, aber auch für ausreichend.

Anspruchserhöhend ist zu berücksichtigen, dass der Beklagten mehrere schadensursächliche Verstöße gegen die DSGVO zur Last zu legen sind, wobei sie die Vorschriften systematisch und über einen längeren Zeitraum missachtet hat. Anspruchsmindernd ist demgegenüber zu berücksichtigen, dass es sich bei den gescrapten Daten nicht um besonders sensible Inforationen wie etwa Gesundheits- oder Kontodaten handelt. Anspruchserhöhend ist weiter zu berücksichtigen, dass der Kläger glaubhaft von störenden Anrufen hinsichtlich seiner Nebenerwerbstätigkeit berichtet hat und ihn dies erkennbar beeinträchtigt hat.

2.

Der Kläger kann auch die Feststellung verlangen, dass die Beklagte verpflichtet ist, ihm alle künftigen Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten entstanden sind und/oder noch entstehen werden.

Es besteht die Möglichkeit eines zukünftigen Schadens

Hinsichtlich der Frage einer Ersatzpflicht für künftige Schäden können die Grundsätze der höchstrichterlichen Rechtsprechung für Feststellungsanträge nach einem Gesundheitsschaden übertragen werden. Der Anspruch auf Feststellung beim Schmerzensgeld als immaterieller Schaden ist begründet, bei einer nicht eben entfernt liegenden Möglichkeit künftiger Verwirklichung der Schadensersatzpflicht durch das Auftreten weiterer, bisher noch nicht voraussehbarer und erkennbarer Leiden oder bei einer noch nicht abschließend überschaubaren weiteren Entwicklung des Krankheitsverlaufs. Das trifft bei schweren Unfallverletzungen in aller Regel zu, es sei denn, es besteht überhaupt kein Grund, mit Spätschäden zu rechnen (BGH NJW-RR 1989, 1367 = VersR 1989, 1055; BGH NJW 1972, 198; BGH MDR 1974, 825 [826]; BGHZ 4, 133 [135]; RGZ 61, 164 [171]). Die Feststellungsklage ist bei noch nicht voraussehbaren und erkennbaren weiteren Beeinträchtigungen oder bei einer noch nicht abschließend überschaubaren weiteren Entwicklung begründet.

Das ist der Fall, denn es besteht die evidente Möglichkeit, dass mit einer weiteren Verbreitung der Telefonnummer weitere materielle oder immaterielle Beeinträchtigungen beim Kläger eintreten können (OLG Stuttgart a.a.O.).

3.

Dem Kläger steht gegen die Beklagte der geltend gemachte Unterlassungsanspruch nicht zu.

Aus Art. 17 DSGVO kann der vom Kläger geltend gemachte Anspruch nicht hergeleitet werden, Ansprüche aus §§ 823, 1004 BGB sind gesperrt (OLG Stuttgart a.a.O.).

a.

Mit dem OLG Stuttgart (a.a.O.) ist der differenzierten Lösung des Bundesgerichtshofs (Urteil vom 13.12.2022, VI ZR 60/21) und des OLG Frankfurt (GRUR 2023, 904; GRUR-RS 20222, 4491) zu folgen, wonach Unterlassungsansprüche nicht auf nationales Recht, sondern lediglich auf Art. 17 DSGVO gestützt werden können. Im Hinblick auf die in Art. 17 DSGVO erfolgte Anknüpfung an das Löschungsrecht bezüglich personenbezogener Daten besteht jedoch nur ein Anspruch auf Unterlassung der Speicherung von Daten, es kann jedoch keine weitergehende Unterlassung begehrt werden, Daten nicht zugänglich zu machen. Art. 17 Abs. 1 DSGVO gibt einen Anspruch auf Löschung personenbezogener Daten, wenn sie für den Zweck der Erhebung oder Verarbeitung nicht mehr notwendig sind (Art. 17 Abs. 1 lit. a) DSGVO), die Einwilligung in eine Verarbeitung widerrufen wird und keine anderweitige Rechtsgrundlage für eine Verarbeitung gegeben ist (Art. 17 Abs. 1 lit. b) DSGVO), Widerspruch eingelegt wird und keine berechtigten Gründe für eine Verarbeitung vorliegen (Art. 17 Abs. 1 lit. c) DSGVO), die personenbezogenen Daten unrechtmäßig verarbeitet wurden (Art. 17 Abs. 1 lit. d) DSGVO), die Löschung zur Erfüllung von Pflichten nach EU-Recht oder dem nationalen Recht erforderlich ist (Art. 17 Abs. 1 lit. e) DSGVO), unzulässig Daten von Kindern erhoben wurden (Art. 8, 17 Abs. 1 lit. f) DSGVO). Nachdem Art. 17 DSGVO lediglich ein Löschungsrecht bezüglich personenbezogener Daten einräumt, jedoch gerade keine weitergehenden Rechte bezüglich der Datenverarbeitungsvorgänge an sich normiert worden sind, können keine Unterlassungsansprüche geltend gemacht werden, die im Ergebnis die Verarbeitungsvorgänge des Verant-

wortlichen reglementieren können. Mit einem Unterlassungsantrag kann danach nicht verbunden werden, dem Verarbeiter der Daten bestimmte Verarbeitungsmethoden vorzugeben. Im Ergebnis geht es jeweils immer nur darum, bei Rechtsverletzungen ein effektives Rechtsfolgensystem zur Verfügung zu stellen (OLG Stuttgart a.a.O.).

b.

Der Bundesgerichtshof (BGH GRUR 20222, 258, GRUR 2020, 1331) stellt ausdrücklich nur auf Art. 17 DSGVO ab, die Anwendung von §§ 1004, 823 BGB wird wegen des unionsweit abschließend vereinheitlichen Datenschutzrechts jeweils abgelehnt, der Anspruch kann also nicht auf Vorschriften des nationalen deutschen Rechts gestützt werden. Der Bundesgerichtshof hat im Beschluss vom 26.09.2023, VI ZR 97/22 für eine über den Wortlaut des Art. 17 DSGVO hinausgehende Auslegung darauf hingewiesen, dass dies über eine systematische Auslegung von Art. 17, 18 DSGVO erreicht werden kann.

c.

In der Sache geht es bei dem Unterlassungsanspruch nicht um die Unterlassung einer (erneuten) Speicherung, sondern der geltend gemachte Unterlassungsanspruch zielt unmittelbar darauf ab, dass die Beklagte nach dem Stand der Technik bestimmte Sicherheitsmaßnahmen vorzusehen hat, die Telefonnummer bei bestimmten Voreinstellungen nicht zugänglich gemacht wird, verlangt wird also neben der Unterlassung auch ein bestimmtes Verhalten der Beklagten. Unabhängig davon, ob damit nicht verdeckt eine (nicht näher bestimmte) Leistung verlangt wird, zielt der Antrag auf Unterlassung bestimmter Datenverarbeitungsvorgänge und ist daher nicht mehr vom Schutzumfang des Art. 17 DSGVO erfasst. Es geht nicht um die Unterlassung einer erneuten Speicherung, sondern der Unterlassungsantrag verlangt etwas Anderes. Da Art. 17 DSGVO lediglich ein Löschungsrecht bezüglich personenbezogener Daten einräumt, jedoch gerade keine weitergehenden Rechte bezüglich der Datenverarbeitungsvorgänge an sich normiert worden sind, können keine Unterlassungsansprüche geltend gemacht werden, die im Ergebnis die Verarbeitungsvorgänge des Verantwortlichen reglementieren können (OLG Stuttgart a.a.O.).

4.

Der Auskunftsantrag ist nicht begründet.

Der Auskunftsantrag (Art. 15 DSGVO) ist nicht begründet. Der Beklagten sind die Scraper namentlich nicht bekannt, weshalb sie über die erteilte Auskunft betreffend das klägerische Nutzungskonto hinaus keine weiteren Auskünfte erteilen kann.

Art. 15 DSGVO gibt der betroffenen Person einen Anspruch, vom Verantwortlichen eine Auskunft darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden (erste Stufe), dazu gehört nach Art. 15 Abs. 1 lit. c) DSGVO eine Information über die Empfänger oder Kategorien von Empfängern, denen gegenüber die Daten offengelegt worden sind (zweite Stufe). Art. 15 DSGVO gewährt einen Anspruch auf umfassende Information hinsichtlich der personenbezogenen Daten der betroffenen Person sowie spezifischer Umstände der Datenverarbeitung. Die zusätzliche Spezifizierung, dass Daten „offengelegt worden sind oder noch offengelegt werden“ macht deutlich, dass nicht nur abgeschlossene Transfers beauskunftet werden müssen, sondern auch solche, die in der Zukunft bevorstehen. Besteht lediglich die Möglichkeit, dass es in Zukunft zu einem solchen Transfer kommen könnte, greift Abs. 1 lit. c) DSGVO (noch) nicht. Der Europäische Gerichtshof hat mit Urteil vom 12.01.2023 (C-154/21) vorgegeben, dass das Auskunftsrecht bei einer Offenlegung der Daten gegenüber Dritten verpflichtet, die Identität der Empfänger mitzuteilen, es sei denn, es ist nicht möglich, den Empfänger zu identifizieren oder der Verantwortliche führt den Nachweis einer offensichtlichen Unbegründetheit oder Exzessivität (Art. 12 Abs. 5 DSGVO). Die Entscheidung verweist insoweit auf den Erwägungsgrund 63 (Anrecht auf Kenntnis der Empfänger), die Vorgaben aus Art. 5 DSGVO (Transparenzgebot), Art. 15 DSGVO insoweit ein Wahlrecht des Betroffenen begründet und nur so eine zulässige Verarbeitung beurteilt werden kann (EuGH, Urteil vom 12.01.2023, C-154/21).

Die Voraussetzungen einer Unmöglichkeit und des deshalb bestehenden Leistungsverweigerungsrechts sind von dem Schuldner darzulegen und zu beweisen, der das Recht zur Leistungsverweigerung in Anspruch nimmt (BGH NJW 2010, 2341 Rn. 9).

Dem Kläger geht es um Auskunft über den Datenschutzvorfall an sich, nach dem Klageantrag will er außerdem wissen, welche Daten durch welche Empfänger abgegriffen worden sind. Die Beklagte trägt vor, dass sie die erforderliche Auskunft Anl. B 16 individuell erteilt hat und keine weitere Auskunft geben kann, weil sie keine Kenntnis hat, wie die Scraper im Detail vorgingen, diese daher auch selbst nicht kennt.

Das Schreiben Anl. B 16 erläutert den Vorfall und die (vermutete) Vorgehensweise der Scraper (erläutert also den Datenschutzvorfall an sich, wobei bestritten wird, dass es einen Datenschutzvorfall gegeben hat), zitiert außerdem umfangreich die Datenrichtlinie enthält aber keine konkreten Informationen, welche Daten abgegriffen wurden und wer diesen Abgriff durchgeführt hat, wer also Empfänger der Daten war. Damit ist keine Auskunft erfolgt, welche Daten durch wen abgegriffen wurden. Nachdem zwischen den Parteien jedoch unstreitig ist, welche Daten abgegriffen wurden, ist die Auskunft insoweit erteilt, ein Auskunftsanspruch erfüllt. Soweit sich die Beklagte bezüglich der Empfänger darauf beruft, diese seien ihr nicht bekannt, hat der Kläger diesen Vortrag nicht bestritten.

5.

Der Kläger kann von der Beklagten Zahlung vorgerichtlicher Rechtsanwaltskosten in Höhe von 159,94 € verlangen. Die vorgerichtlichen Rechtsanwaltskosten sind als Teil des zu ersetzenden Schadens gemäß Art. 82 Abs. 1 DSGO zu erstatten. Aufgrund der Schwierigkeit der Sach- und Rechtslage war die Hinzuziehung eines Rechtsanwalts zur effektiven Durchsetzung der klägerischen Ansprüche erforderlich und notwendig. Unter Zugrundelegung des Wertes des berechtigten Verlangens des Klägers (500,00 € immaterieller Schadensersatz plus 500,00 € Feststellungsantrag) zum Zeitpunkt der außergerichtlichen Tätigkeit führt dies zu berechtigten außergerichtlichen Kosten in der tenorierten Höhe (1,3-fache Geschäftsgebühr nebst Pauschale nach Nr. 7002 VV-RVG zuzüglich 19 % Mehrwertsteuer).

**III.**

1. Der Zinsausspruch folgt aus §§ 288 Abs. 1, 291, 187 Abs. 1 BGB analog.

2. Die Entscheidung über die Kosten beruht auf § 92 Abs. 1 ZPO.

3. Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt aus §§ 708 Nr. 11, 711 Satz 1 und 2 ZPO.

4. Die Streitwertfestsetzung hat ihre Rechtsgrundlage in den §§ 39 Abs. 1, 43 Abs. 1, 48 Abs. 1 Satz 1 GKG, § 3 ZPO. Die Klaganträge Ziffer 2. und 4. sind nur mit 500,00 € zu bewerten, weil eine größere wirtschaftlicher Bedeutung für den Kläger nicht erkennbar ist. Den Klageantrag Ziffer 3. (Unterlassung) bewertet das Gericht in Anlehnung an § 23 Abs. 3 Satz 2 RVG mit 5.000,00 €.

**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 Ellwangen (Jagst)
Marktplatz 7
73479 Ellwangen (Jagst)

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 anwalt-

liche Mitwirkung ist nicht vorgeschrieben.

Rechtsbehelfe können auch als elektronisches Dokument eingelegt werden. Eine Einlegung per E-Mail ist nicht zulässig. Wie Sie bei Gericht elektronisch einreichen können, wird auf www.ejustice-bw.de beschrieben.

Vizepräsident des Landgerichts