Aktenzeichen:
46 O 343/22

Landgericht Stuttgart

# Im Namen des Volkes

# Urteil

In dem Rechtsstreit

[redacted]
- Kläger -

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

gegen

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

Prozessbevollmächtigte:
Rechtsanwälte **Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB**, Bockenheimer Anlage 44, 60322 Frankfurt, Gz.: [redacted]

wegen Forderung

hat das Landgericht Stuttgart - 46. Zivilkammer - durch den [redacted] als Einzelrichter am 06.07.2023 aufgrund der mündlichen Verhandlung vom 27.04.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von 400,00 EUR nebst Zinsen seit 02.12.2022 in Höhe von 5 Prozentpunkten über dem Basiszinssatz zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte

2.1 nicht vorhersehbaren entstandenen oder noch entstehenden immateriellen Schäden zu ersetzen.

2.2 entstandenen oder noch entstehenden materielle Schäden zu ersetzen.

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,

3.1 personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, 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,

3.2 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. Im Übrigen wird die Klage abgewiesen.

5. Von den Kosten des Rechtsstreits haben der Kläger 40 % und die Beklagte 60 % zu tragen.

6. Das Urteil ist hinsichtlich Ziffer 3 vorläufig vollstreckbar gegen Sicherheitsleistung in Höhe von 1.100,00 Euro.

7. Das Urteil ist hinsichtlich Ziffer 1 sowie der Kosten vorläufig vollstreckbar. Die Parteien

können insoweit die Vollstreckung der jeweils anderen Partei durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die jeweils andere Partei vor der Vollstreckung Sicherheit in Höhe von 110 % des zu vollstreckenden Betrags leistet.

# Beschluss

Der Streitwert wird auf 3.000,00 Euro festgesetzt.

# Tatbestand

Die Parteien streiten über Schadensersatz-, Unterlassungs- und Auskunftsansprüche auf datenschutzrechtlicher Grundlage.

Der Kläger ist Nutzer des von der Beklagten betriebenen sozialen Netzwerks „Facebook“. Die Informationen Name, Geschlecht und Nutzer ID sind von jedem Nutzer für andere Nutzer zwingend zur Identifizierung öffentlich sichtbar. Weitere persönliche Daten wie Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse können von Nutzern von Facebook hinterlegt werden und sind grundsätzlich öffentlich sichtbar. Jeder Nutzer hat die Möglichkeit, im Rahmen der „Zielgruppenauswahl“ einzustellen, ob diese persönlichen Daten der Öffentlichkeit verborgen werden. Der Kläger hatte seine Mobiltelefonnummer bei Facebook hinterlegt, ohne dass diese öffentlich sichtbar war.

Facebook ermöglichte es Nutzern über ein Kontakt-Import-Tool („**CIT**“), beliebige Telefonnummern bei Facebook abzufragen. Konnte Facebook für eine der Telefonnummern ein bei Facebook bestehendes Nutzerkonto identifizieren, leitete Facebook den Abfragenden auf das öffentlich einsehbare Nutzerprofil des Abgefragten weiter. Nutzer von Facebook können in den Einstellungen die Auffindbarkeit mittels Telefonnummer über das CIT deaktivieren. Als Standardeinstellung ist die Auffindbarkeit aktiviert.

Im April 2021 veröffentlichten unbekannte Dritte im Darknet hunderte Millionen Datensätze von Facebook-Nutzern. Hierunter befanden sich Mobiltelefonnummer, Nutzer-ID, Name, Land und Geschlecht des Klägers. Die Parteien gehen davon aus, dass die unbekannten Dritten an diese Daten gelangten, indem für Millionen zufällig generierter Telefonnummern Anfragen über das CIT bei

Facebook getätigt wurden. Hierdurch konnten Telefonnummern, welche nicht öffentlich freigegeben waren, konkreten Facebookprofilen und den auf diesen öffentlich zugänglich Daten zugeordnet werden. Das Abschöpfen dieser Daten und die hierdurch ermöglichte Erstellung von Nutzerprofilen wird als „**Scraping**“ bezeichnet.

Mit Schreiben vom Mai 2021 forderte der Kläger die Beklagte zur Zahlung von Schadensersatz, Unterlassung und Auskunftserteilung auf. Die Beklagte wies die geltend gemachten Ansprüche auf Zahlung von Schadensersatz und Unterlassung zurück. Mit Schreiben vom 07.10.2021 (Anlage K2/B16) teilte die Beklagte dem Kläger mit, welche Informationen die unbekannten Dritten nach Kenntnis der Beklagten erlangt hatten. Weiterhin wurde dem Kläger mitgeteilt, wie er über eine automatisierte Abfrage eine Kopie der von Facebook verarbeiteten personenbezogenen Daten erlangen könne.

Die irische Datenschutzbehörde verhängte am 28.11.2022 wegen des Scrapings von 533 Millionen von Datensätzen bei Facebook und deren Veröffentlichung im April 2021 gegen die Beklagte ein Bußgeld von 265 Millionen Euro.

Der Kläger änderte weder vor noch nach Klageerhebung die Datenschutz-Einstellung seines Facebook-Kontos, um eine Suchbarkeit über eine Telefonnummer auszuschließen.

Der Kläger behauptet, seit 2021 regelmäßig Anrufe und SMS-Nachrichten von unbekannten Anrufern zu erhalten. Teilweise handelte es sich um Werbung bzw. Kaltakquiseanrufe. In anderen Fällen waren es Betrugsversuche. In einem Fall sei ein Anruf der Tochter des Klägers fingiert worden.

Der Kläger ist der Ansicht, die Beklagte habe in mehrfacher Hinsicht gegen die Datenschutz-Grundverordnung („**DS-GVO**“) verstoßen. Die Beklagte habe für die mit dem CIT erfolgte Datenverarbeitung keine wirksame Einwilligung gemäß Art. 6 Abs. 1 lit. a DS-GVO besessen. Zudem habe die Beklagte gegen Transparenzpflichten verstoßen und keine angemessenen technischen und organisatorischen Maßnahmen zum Schutz der Daten des Klägers implementiert. Die Voreinstellungen der Beklagten verstießen gegen den Grundsatz „Privacy by Default“ gemäß Art. 25 Abs. 2 DS-GVO. Die Beklagte habe zudem gegen Meldepflichten gemäß Art. 33, 34 DS-GVO verstoßen.

Der Kläger ist der Auffassung, ihm stünde daher ein Anspruch auf Ersatz immaterieller Schäden gemäß Art. 82 DS-GVO zu. Hieraus ergäbe sich auch ein Anspruch auf Ersatz zukünftiger Schäden. Weiterhin habe der Kläger Anspruch auf Unterlassung der Beklagten. Darüber hinaus be-

stünde ein ergänzender Auskunftsanspruch.

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 453,87 €€ zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt

Die Klage wird abgewiesen.

Die Beklagte ist der Ansicht, sie habe das Auskunftsbegehren des Klägers ordnungsgemäß beantwortet.

Die Beklagte ist der Ansicht, die Klageanträge Ziffer 1 bis 3 seien unbestimmt und damit unzulässig.

Die Beklagte ist der Ansicht, der Kläger hab keine hinreichende persönliche spürbare Beeinträchtigung dargelegt. Es fehle daher bereits an einem ersatzfähigen immateriellen Schaden.

Im Übrigen wird auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen sowie das Sitzungsprotokoll der mündlichen Verhandlung vom 02.05.2023 Bezug genommen.

# Entscheidungsgründe

Die überwiegend zulässige Klage ist im tenorierten Umfang begründet.

**A.**

Die Klage ist überwiegend zulässig.

I. Zuständigkeit

Die deutschen Gerichte sind international zuständig, Art. 17 Abs. 1 lit. c) EuGVVO, da der Kläger als Verbraucher seinen Wohnsitz in Deutschland hat.

Das Landgericht ist mangels Rüge der Zuständigkeit durch die Beklagte streitwertunabhängig gemäß § 39 ZPO sachlich zuständig.

Das Landgericht Stuttgart ist gemäß Art. 18 Abs. 1 Alt. 2 EuGVVO örtlich zuständig, da der Kläger seinen Wohnsitz im Zuständigkeitsbereich des Landgerichts Stuttgart hat.

II. Zulässigkeit Klageantrag Ziffer 1

Klageantrag Ziffer 1 ist ausreichend bestimmt. Unbedenklich ist, dass der Kläger seinen Schadensersatzanspruch auf mehrere Pflichtverletzungen stützt. Der von dem Kläger geltend gemachte Anspruch besteht aus einem einheitlichen immateriellen Schaden.

III. Zulässigkeit Klageantrag Ziffer 2

Klageantrag Ziffer 2 ist teilweise unzulässig, soweit der Ersatz bereits entstandener sowie vorhersehbarer immaterieller Schäden begeht wird. Im Übrigen ist der Klageantrag zulässig.

1. Bestimmtheit

Der Antrag genügt dem Bestimmtheitserfordernis des § 253 Abs. 2 Nr. 2 ZPO.

Soweit der Antrag widersprüchlich erscheint, als „künftige bereits entstandene Schäden“ ersetzt werden sollen, ist er der Auslegung zugänglich. Der Kläger begehrt nach seinen Ausführungen auf S. 55 der Replik eine Feststellung der Ersatzpflicht sowohl entstandener als auch zukünftig entstehender Schäden.

2. Feststellungsinteresse

Dem Kläger fehlt ein Feststellungsinteresse, soweit der Ersatz bereits entstandener sowie vorhersehbarer immaterieller Schäden begeht wird. Für diese besteht ein Vorrang der - vorliegend mit Klageantrag Ziffer 1 bereits erhobenen - Leistungsklage.

Im Übrigen liegt für Klageantrag Ziffer 2 das erforderliche Feststellungsinteresse gemäß § 256 Abs. 1 ZPO vor. Der Kläger hat die Möglichkeit des Eintritts zukünftiger materieller Schäden hinreichend dargelegt. 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 Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (*Bacher* in BeckOK ZPO, Stand: 01.09.2022, § 256, Rn. 24). Unter Berücksichtigung des Umstandes, dass die im Wege des "Scrapings" erlangten personenbezogenen Daten im Internet veröffentlicht worden sind, erscheint es bei lebensnaher Betrachtung möglich, dass es bei dem Kläger aufgrund der Veröffent-

lichung der Telefonnummer und weiterer persönlicher Daten wie des Namens des Klägers im Internet zu künftigen materiellen oder immateriellen Schäden kommt, etwa durch betrügerische Anrufe.

IV. Zulässigkeit Klageantrag Ziffer 3

Klageantrag Ziffer 3 a) und b) sind hinreichend bestimmt.

Soweit die Beklagte rügt, dass die Formulierung "nach dem Stand der Technik möglichen Sicherheitsmaßnahmen" im Klageantrag Ziffer 3 a) zu unbestimmt sei, führt dieses nicht zur Unzulässigkeit des Antrags.

Ein Verbotsantrag darf im Hinblick auf § 253 Abs. 2 Nr. 2 ZPO zwar nicht derart undeutlich gefasst sein, dass Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts (§ 308 ZPO) nicht erkennbar abgegrenzt sind, sich die Beklagte deshalb nicht erschöpfend verteidigen kann und letztlich die Entscheidung darüber, was der Beklagten verboten ist, dem Vollstreckungsgericht überlassen bleibt. Aus diesem Grund sind Unterlassungsanträge, die lediglich den Wortlaut eines Gesetzes wiederholen, grundsätzlich als zu unbestimmt und damit unzulässig anzusehen. Etwas anderes kann dann gelten, wenn entweder bereits der gesetzliche Verbotstatbestand selbst entsprechend eindeutig und konkret gefasst oder der Anwendungsbereich einer Rechtsnorm durch eine gefestigte Auslegung geklärt ist oder wenn der Kläger hinreichend deutlich macht, dass er nicht ein Verbot im Umfang des Gesetzeswortlauts beansprucht, sondern sich mit seinem Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert. Die Bejahung der Bestimmtheit setzt in solchen Fällen allerdings grundsätzlich voraus, dass zwischen den Parteien kein Streit darüber besteht, dass das beanstandete Verhalten das fragliche Tatbestandsmerkmal erfüllt. Eine auslegungsbedürftige Antragsformulierung ist jedoch dann hinzunehmen, wenn eine weitergehende Konkretisierung nicht möglich und die gewählte Antragsformulierung zur Gewährung effektiven Rechtsschutzes erforderlich ist (vgl. BGH, Urteil vom 26.01.2017, Az. I ZR 207/14). Unzulässigkeit liegt hingegen vor, wenn die Klägerseite seinen Antrag ohne weiteres konkreter fassen kann (vgl. BGH, Urteil vom 11.06.2015, Az. I ZR 226/13).

Daran gemessen weist der Klageantrag Ziffer 3) a) eine ausreichende Bestimmtheit auf. 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 entgegen. Zudem wird aus der Klagebegründung deutlich, dass der Kläger Sicherheitsstandards verlangt, die möglichen (weiteren) Scraping-Angriffen vorbeugen. Die gesetzlich vorgeschrieben Sicher-

heitsstandards einzurichten ist jedoch zuvorderst die Aufgabe der Beklagten. Insoweit kann diese nicht von ihren Nutzern die konkrete Benennung der Sicherheitsmaßnahmen verlangen.

Dass mit dem Klageantrag Ziffer 3) b) begehrte Anspruchsziel ist ebenfalls hinreichend bestimmt. Das Anspruchsziel wird jedenfalls durch die Klagbegründung hinreichend konkretisiert.

**B.**

Klageanträge 1, 2 und 3 sind im tenorierten Umfang jeweils teilweise begründet, im Übrigen ist die Klage unbegründet.

I. Schadensersatz (Klageantrag Ziffer 1)

Dem Kläger steht ein Anspruch auf Schadensersatz in Höhe von 400,00 Euro gemäß Art. 82 Abs. 1 DS-GVO zu.

Voraussetzung eines Schadensersatzanspruchs gemäß Art. 82 DS-GVO ist ein Verstoß gegen Pflichten der DS-GVO, dass der Verstoß geeignet ist, einen Schadensersatz nach Art. 82 DS-GVO auszulösen, ein eingetretener Schaden sowie Kausalität zwischen Pflichtenverstoß und Schaden. Der Beklagten dürfte zudem gemäß Art. 82 Abs. 3 DS-GVO kein Nachweis gelingen, dass sie kein Verschulden am Schadenseintritt trifft.

1. Verstoß gegen die DS-GVO

Die Beklagte hat gegen Pflichten der DS-GVO verstoßen, indem sie die technischen Voraussetzungen schuf, über eine Abfrage zufälliger Nummern die Telefonnummer mit dem Nutzerkonto des Klägers zu verknüpfen, ohne dass hierfür eine Einwilligung vorlag. Die Beklagte hat hierbei insbesondere gegen ihre Pflicht gemäß Art. 32 DS-GVO verstoßen, geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu treffen, gegen die Verpflichtung datensparsamer Grundeinstellungen nach Art, 25 Abs. 2 DS-GVO sowie im Anschluss gegen ihre Meldepflichten nach Artt. 33, 34 DS-GVO.

a. Verstoß gegen Datenverarbeitungssicherheit

Die Beklagte als Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO verstieß aufgrund unzureichender Sicherheitsmaßnahmen bezüglich der Nutzung des CIT auch gegen Art. 32, 24, 5 Abs. 1 lit. f) DS-GVO (so auch LG Paderborn, Urteil vom 19.12.2022, Az. 3 O 99/22; LG Stuttgart, Urteil

vom 18.04.2023, Az. 54 O 9/23).

aa. Voraussetzungen

Gemäß Art. 32 Abs. 1 Hs. 1 DS-GVO haben der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen 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 DS-GVO regelt die Pflicht des Verantwortlichen und des Auftragsverarbeiters, bestimmte technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Schutzniveau im Hinblick auf die verarbeiteten personenbezogenen Daten zu gewährleisten. Er konkretisiert die als Generalauftrag gestalteten Datensicherheitsmaßnahmen des Art. 24 DS-GVO und dient damit u.a. der Gewährleistung der Absicherung der Datenschutzgrundsätze der Vertraulichkeit und Integrität nach Art. 5 Abs. 1 f) DS-GVO. Zielrichtung ist ein umfassender Schutz der für die Verarbeitung von personenbezogenen Daten genutzten Systeme, also im Kern die Datensicherheit (*Mantz* in Sydow/Marsch, Art. 32 DS-GVO, 2022, 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, Art. 32 DS-GVO, 2021, Rn. 2; vgl auch *Hladjk* in Ehmann/Selmayr, Art. 32 DS-GVO, 2018, Rn. 2). Bei der Implementierung von geeigneten technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO 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. Dies bedeutet allerdings nur, dass sie in die Verhältnismäßigkeitsprüfung einzustellen, jedoch nicht notwendigerweise absolut zu befolgen sind (*Piltz* in Gola/Heckmann, Art. 32 DS-GVO, 2022, Rn. 14). Die DS-GVO legt zur Bemessung der Geeignetheit der Maßnahmen insbesondere weiter fest, dass diese ein dem Risiko der Verarbeitung angemessenes Schutzniveau bieten müssen. Dabei kommt es letztlich darauf an, wie groß die Risiken sind, die den Rechten und Freiheiten der betroffenen Person drohen und wie hoch die Wahrscheinlichkeit eines Schadenseintritts ist. Damit ergibt sich, dass die Maßnahmen umso wirksamer sein müssen, je höher die drohenden Schäden sind (Hladjk a.a.O. Rn. 4; *Laue* in Spindler/Schuster, Art. 32 DS-GVO, 2019, Rn. 4). Dies wird vor allem anhand der Sensibilität der Daten und der Wahrscheinlichkeit eines Schaden-

eintritts bestimmt (*Piltz* a.a.O. Rn. 41). Art. 32 Abs. 1 DS-GVO verpflichtet den Verantwortlichen und Auftragsverarbeiter aber nicht zu einem absoluten Schutz(niveau) der Daten. Das Schutzniveau muss vielmehr, je nach Verarbeitungskontext, dem Risiko bezüglich der Rechte und Freiheiten der betroffenen Personen im Einzelfall angemessen sein. Dies bedeutet gleichzeitig, dass das Risiko nicht völlig ausgeschlossen werden kann und dies auch nicht Ziel der umzusetzenden Maßnahmen ist (*Piltz* a.a.O. Rn. 11; *Laue* a.a.O. Rn. 3). Zur Bestimmung des angemessenen Schutzniveaus sind gem. Art. 32 Abs. 2 DS-GVO insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. Diese sind zwingend in die Risikobetrachtung einzubeziehen (*Laue* a.a.O. Rn. 5). Ausweislich des Erwägungsgrunds 76 zur DS-GVO sollten die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt (zum Ganzen LG Paderborn, Urteil vom 19.12.2022, Az. 3 O 99/22, Rn. 77 - 83 [juris]).

bb. Im vorliegenden Verfahren

Diesen Anforderungen genügten die beklagtenseits behaupteten Schutzmaßnahmen nicht.

Die von ihr behaupteten "Anti-Scraping-Maßnahmen" sind selbst, wenn der Beweis zum Vorliegen der Maßnahmen für den streitgegenständlichen Zeitraum geführt werden würde, für sich allein nicht geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das CIT ermöglicht einen unbefugten Zugang i.S.d. Art. 32 Abs. 2 DS-GVO. Beim Zugang zu Daten geht die entscheidende Aktivität vom Empfänger der Daten aus. Der Verantwortliche muss lediglich durch die Ausgestaltung der technischen Bedingungen die Daten grundsätzlich zum Abruf durch Dritte ermöglichen. Dieses Bereithalten der Daten zum Abruf kann z.B. durch das Einräumen von Zugriffsrechten im Rahmen von Netzwerken oder durch Einstellung in eine Datenbank, auf die auch Dritte zugreifen können, erfolgen (*Jandt* in Kühling/Buchner, Art. 32 DS-GVO, 2020, Rn. 34). So liegt der Fall hier, da das CIT zweckwidrig nicht zum Auffinden von persönlichen Kontakten auf der Facebook-Plattform, sondern entgegen der Nutzungsbedingungen der Beklagten zu Missbrauchszwecken genutzt werden konnte und wurde. Es wird Dritten eine Zuordnung von Telefonnummer zum Nutzerprofil ermöglicht. Dementsprechend wird in Erfahrung gebracht, welche Person hinter der Telefonnummer steht. Hierbei können durch den Rückgriff auf das Nutzer-

profil gleichzeitig weitere Informationen über die Person eingeholt werden. Dies birgt für die Nutzer das Risiko von gezielten Phishing-Attacken, Identitätsdiebstahl und weiterem Missbrauch der Daten und damit dem Eintritt von materiellen oder immateriellen Schäden.

Dieses zwingend zu berücksichtigende Risiko bedingt bereits, dass der Maßstab für die Bestimmung der Angemessenheit des Schutzniveaus entsprechend hoch anzusetzen ist. Dies begründet sich unter anderem daraus, dass das CIT-Verfahren nicht eine reine Erhebung oder Speicherung von Daten durch die Beklagte darstellt. Auch handelt es sich bei den Daten nicht um ohnehin öffentlich einsehbare Daten. Vielmehr wird Dritten ein Zugang zu diesen, insbesondere der Telefonnummer des Nutzers, gewährt. Es erfolgt eine Verknüpfung der zuvor nicht öffentlich einsehbaren Telefonnummer zu den weiteren Daten des Nutzers auf der Plattform der Beklagten. Die Gefahr einer Veröffentlichung aller zusammengetragenen Daten, darunter insbesondere die Verknüpfung von Telefonnummer und Name, ist, wie der vorliegende Datenscraping-Fall aufzeigt, besonders hoch. Dies war auch der Beklagten bekannt. Für sie ist ausweislich ihres Artikels "Die Fakten zu Medienberichten über Facebook-Daten" vom 06.04.2021 (Anlage B10) Scraping "eine gängige Taktik". Die Beklagte musste sich daher darüber bewusst sein, dass Maßnahmen für ein angemessenes Schutzniveau für die personenbezogenen Daten hinsichtlich des Risikos von Scraping zu treffen waren.

Soweit die Beklagte nun darauf abstellt, dass sie gegen Scraper mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren vorgehe, kommt diese Maßnahme bereits erst dann zu tragen, wenn ein Datenscraping tatsächlich eingetreten ist. Die Daten sind in diesem Stadium bereits entwendet worden. Eine Veröffentlichung oder anderweitiger Missbrauch kann in diesem Stadium praktisch nicht mehr verhindert werden.

Gleiches gilt für die behauptete teilweise Einschränkung des CIT. Erst im Nachgang an den Scraping-Vorfall implementierte die Beklagte den sogenannten "Social Connection Check". Die Beklagte nahm damit vielmehr erst den Vorfall zum Anlass ihre Schutzmaßnahmen zu evaluieren und traf ausweislich ihres als Anlage B11 vorgelegten Artikel "Scraping nach Zahlen" vom 19.05.2021 "eine Reihe von Verbesserungen" im September 2019 (so insgesamt ausdrücklich und zutreffend LG Paderborn, Urteil vom 19.12.2022, Az. 3 O 99/22, Rn. 84 - 93 [juris]; LG Stuttgart, Urteil vom 18.04.2023, Az. 54 O 9/23).

b. Verstoß gegen Privacy by Default

Die Beklagte hat gegen Art 25 Abs. 2 DS-GVO verstoßen.

aa. Voraussetzungen

Gemäß Art. 25 Abs. 2 DS-GVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Durch die standardmäßige Konfiguration von Privatsphäre-Einstellungen ist zu gewährleisten, dass Nutzer ihre Daten nur den Personenkreisen und nur in dem Umfang zugänglich machen, die sie vorab selbst festgelegt haben. Das hat zur Folge, dass alle für die Nutzung nicht erforderlichen personenbezogenen Daten anderen Nutzern nicht zugänglich gemacht werden dürfen, es sei denn, die betroffene Person nimmt entsprechende Änderungen in den Voreinstellungen vor (vgl. *Nolte/Werkmeister* in Gola/Heckmann, Art. 25 DS-GVO 2022, Rn. 28). Die von Nutzern veröffentlichten Informationen dürfen nicht ohne Einschränkungen der allgemeinen Öffentlichkeit zugänglich gemacht werden, sondern dies muss aktiv erst in den Privatsphäreeinstellungen durch den Nutzer eingerichtet werden (so *Hartung* in Kühling/Buchner, Art. 25 DS-GVO, 2020, Rn. 26). Erforderlich für den Verarbeitungszweck i.S.d Art. 25 Abs. 2 S. 1 sind Daten nur dann, wenn der Verarbeitungszweck sich ohne sie nicht erreichen lässt. Diese Daten darf der Verantwortliche auch durch Voreinstellung verarbeiten. Für solche Daten, die der Verantwortliche nicht notwendig verarbeiten muss, um die legitimen Zwecke der Verarbeitungserlaubnis (Art. 6 DS-GVO) erfüllen zu können, ist ihm der Weg der Voreinstellung demgegenüber verschlossen (*Martini* in Paal/Pauly, Art. 25 DS-GVO, 2021, Rn. 45b).

bb. Im vorliegenden Verfahren

Gemessen an diesen Grundsätzen liegt ein Verstoß der Beklagten gegen Art. 25 Abs. 2 DS-GVO vor (ebenso LG Stuttgart, Urteil vom 26.01.2023, Az. 53 O 95/22; LG Paderborn, Urteil vom 19.12.2022, Az. 3 O 99/22; a.A. LG Essen, Urteil vom 10.11.2022, Az. 6 O 111/22).

Die durch die Voreinstellungen in der „Zielgruppenauswahl“ und der Suchbarkeit über das CIT ermöglichte Datenerhebung ist nicht für die Durchführung des rechtsgeschäftlichen Schuldverhältnisses zwischen den Parteien erforderlich (Art. 6 Abs. 1 S. 1 lit. b) DS-GVO), ebenso wenig zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 Satz 1 lit. f DS-GVO). Unbeachtlich ist der Einwand der Beklagten, es sei der Daseinszweck der Facebook-Plattform, es Menschen zu ermöglichen, sich mit Freunden, Familie und Gemeinschaften zu verbinden und Funktionen seien daher gezielt so konzipiert worden, dass sie den Nutzern helfen, andere zu finden, sich mit ihnen zu verbinden und mit ihnen in Kontakt zu treten. Die Voreinstellung mag im Einzelnen je nach Geschmack des Nutzers für die Nutzung der Facebook-Platt-

form nützlich und behilflich sein. Nützliche und behilfliche Einstellungen sind jedoch bereits begrifflich nicht erforderlich für einen bestimmten Zweck. Es liegt naturgemäß im Interesse der Beklagten, die Nutzbarkeit der von ihr betriebenen Plattform auch unter Hintanstellung der Nutzerinteressen zu vermarkten (vgl. BGH, Beschluss vom 23.06.2020, Az. KVR 69/19, Rn. 110). Ein wesentlicher Zweck der DS-GVO ist hingegen der Schutz derjenigen Nutzer, die einen sparsamen Umgang mit ihren Daten wünschen. Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten müssen sich auf das absolut Notwendige beschränken. Eine „passive“ Nutzung von Facebook als reiner Konsument von Informationen ohne über öffentlich einsehbare Informationen oder das CIT auffindbar zu sein, ist ohne Weiteres möglich. Belegt wird dies durch die Tatsache, dass sämtliche Voreinstellungen, um die es hier geht, ohne weiteres abgewählt werden können, ohne dass eine unmittelbare Beeinträchtigung der weiteren Vertragsdurchführung ersichtlich wäre (so ausdrücklich und überzeugend KG, Urteil vom 20.12.2019, Az. 5 U 9/18, BeckRS 2019, 35233 Rn. 39).

c. Verstoß gegen Meldepflichten

Die Beklagte hat gegen ihre Pflicht aus Art. 33, 34 DS-GVO, eine Verletzung des Schutzes personenbezogener Daten der zuständigen Aufsichtsbehörde sowie dem Betroffenen zu melden, verstoßen.

aa. Keine Meldung

Eine rechtzeitige Meldung ist unstreitig nicht erfolgt.

bb. Verletzung personenbezogener Daten

Es lag eine Verletzung des Schutzes personenbezogener Daten vor. Voraussetzung ist gemäß Art. 4 lit. 12 DS-GVO eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Erfasst ist damit im weitesten Sinn jede objektive Schutzverletzung, unabhängig davon, ob diese beabsichtigt war oder nicht, wie etwa Datenpannen, -lecks, Hackerangriffe oder Datendiebstahl (*Hladjk* in Ehmann/Selmayr, Art. 33 DS-GVO, 2018, Rn. 5; *Laue* in Spindler/Schuster, Art. 33 DS-GVO, 2019, Rn. 6 m.w.N.). Eine Verletzung liegt auch dann vor, wenn im Rahmen bestehender Zugriffsrechte Daten zweckentfremdet werden (*Laue* a.a.O. Rn. 7). Nach der Stellungnahme 3/2014 der Artikel-29-Datenschutzgruppe erfolgt eine Kategorisierung in unterschiedliche Arten von Verletzungen der Sicher-

heit, namentlich der "Verletzung der Vertraulichkeit", bei der es zu einer unbefugten oder unbeabsichtigten Offenlegung von oder zu einem Zugriff auf personenbezogene Daten kommt, der "Verletzung der Verfügbarkeit", bei der es zu einem unbeabsichtigten oder unbefugten Verlust von, Zugriff auf, oder Vernichtung von personenbezogenen Daten kommt, sowie der "Verletzung der Integrität", bei der es zu einer unbefugten oder unbeabsichtigten Veränderung von personenbezogenen Daten kommt. Eine Verletzung der Vertraulichkeit von Daten liegt auch immer dann vor, wenn die Ebene, auf der die Daten zur Verfügung stehen, geändert wurde (Artikel-29-Datenschutzgruppe, Stellungnahme 3/2014 on Personal Data Breach Notification, WP 213, S. 18).

Eine solche Verletzung der Vertraulichkeit liegt vor. Denn unabhängig davon, dass Name, Facebook-ID und Geschlecht des Klägers aufgrund seiner Privatsphäre-Einstellungen öffentlich waren und die Handynummer durch die frei zugängliche Nutzung des CIT-Tools mit diesen Daten verknüpft werden konnte, liegt vor dem Hintergrund des massenhaften "Scrapings" und der Veröffentlichung der Daten im "Darknet" eine Zweckentfremdung im Rahmen der grundsätzlich gewährten Zugriffsrechte vor. Der "Scraping"-Vorfall ist allein aufgrund seines Ausmaßes mit Datenpannen, -lecks, Hackerangriffe oder Datendiebstahl gleichzusetzen. Dies zeigt sich auch darin, dass ein solches Vorgehen nach den Nutzungsbedingungen untersagt ist und - so behauptet jedenfalls die Beklagte selbst - Sicherheitsmaßnahmen gegen derartige Vorfälle geschaffen wurden. Durch die Veröffentlichung der Daten im "Darknet" wurde zudem die Ebene, auf denen die Daten zur Verfügung stehen, geändert. Dass die Leitlinien des Europäischen Datenschutzausschusses das "Scraping" selbst nicht ausdrücklich als eines der Beispiele für eine Verletzung des Schutzes persönlicher Daten nennen ist unbeachtlich, da diese ausdrücklich nicht abschließend sind.

cc. Keine Ausnahme der Meldepflicht

Eine Einschränkung der Meldepflicht nach Art. 33 Abs. 1 DS-GVO ist nicht gegeben. Es war nicht vorauszusehen, dass die Verletzung des Schutzes personenbezogener Daten nicht zu einem Risiko für die Rechte und Freiheiten des Klägers führt. Die Verfügbarkeit der Daten im Darknet, wo Kriminelle sich dieser für ihre Machenschaften bedienen konnten, stellte ein Risiko dar.

Die Benachrichtigungspflicht ist auch nicht nach Art. 34 Abs. 3 DS-GVO entbehrlich. Substanziellen Vortrag hierzu hat die Beklagte nicht gehalten.

d. Verstoß gegen Informationspflichten

Ein Verstoß der Beklagten gegen die Pflicht, den Kläger über den Zweck der Datenverarbeitung

zu informieren, Art. 13 Abs. 1 c) DS-GVO, kann vorliegend unterstellt werden. Insoweit fehlt es an der Kausalität der Pflichtverletzung für den eingetretenen Schaden (siehe unten).

e. Verstoß gegen Auskunftspflicht

Ein Verstoß der Beklagten gegen ihre Auskunftspflicht gemäß Art. 15 DS-GVO ist nicht ersichtlich. Die Beklagte hat auf Anfrage des Klägers erklärt, dass sie nicht wisse, welche Informationen durch das Scraping von den Scrapern erlangt wurden. Damit hat sie die Auskunft erteilt.

2. Ersatzfähigkeit

Verstöße gegen Privacy by Default (*Martini* in Paal/Pauly, Art. 25 DS-GVO, 2021, Rn. 6), Datenverarbeitungssicherheit (*Jandt* in Kühling/Buchner, Art. 32 DS-GVO, 2020, Rn. 40a) und Meldepflichten nach Art. 33, 34 DS-GVO (*Jandt* in Kühling/Buchner, Art. 33 DS-GVO, 2020 Rn. 27) sind geeignet, Schadensersatzansprüche nach Art. 82 DS-GVO auszulösen.

Insbesondere vermag ein Verstoß gegen Privacy by Default nach Art. 25 Abs. 2 DS-GVO einen Schadensersatzanspruch gemäß Art. 82 DS-GVO zu begründen. Der Wortlaut von Art. 82 DS-GVO lässt einen Schadensersatzanspruch ohne Weiteres zu. Eine dogmatische Begründung, warum die nutzerschützende Norm des Art. 25 Abs. 2 DS-GVO bei Verstößen keinen Schadensersatzanspruch des Nutzers auslösen soll, findet sich weder bei der Beklagten noch in der zitierten Literatur. Soweit Literaturstellen (von der Beklagten irreführend zitiert: *Hartung* in Kühling/Buchner, Art. 25 DS-GVO, 2020, Rn. 31; *Nolte/Werkmeister* in Gola, Art. 25 DS-GVO, 2018, Rn. 34; *Mantz* in Sydow, Art. 25 DS-GVO, 2018 Rn. 77) sich fragen, ob ein isolierter Verstoß gegen Art. 25 Abs. 2 DS-GVO vorstellbar ist, ist dies ohne Belang. Jedenfalls in Zusammenspiel mit einem Verstoß gegen weitere Normen kann ein Verstoß gegen Art. 25 Abs. 2 DS-GVO sich schadenserhöhend auswirken.

3. Keine Entlastung

Eine Haftung der Beklagten entfällt nicht gemäß Art. 82 Abs. 3 DS-GVO. Hierzu hätte die Beklagte nachweisen müssen, dass in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Dies ist ihr nicht gelungen. Die Beklagte hebt lediglich darauf ab, dass ein Verstoß gegen Vorschriften der DS-GVO jedenfalls nicht fahrlässig war, da nach ihrer Auffassung überhaupt kein Verstoß gegen DS-GVO-Vorschriften vorlag. Dem kann das Gericht nicht folgen. Hätte die Beklagte die im Verkehr erforderliche Sorgfalt beachtet, hätte sie weder ohne Zustimmung den Zugriff auf das Nutzerkonto des Klägers über das CIT zugelassen noch es

versäumt, den Scraping-Vorfall zu rechtzeitig zu melden.

4. Schaden

Dem Kläger ist im Zusammenhang mit dem Daten-Scraping-Vorfall ein nach Art. 82 DS-GVO ersatzfähiger – immaterieller – Schaden entstanden.

a. Eintritt eines Schadens

Voraussetzung eines Schadens ist, dass über den Verstoß gegen eine Norm der DS-GVO hinaus ein feststellbarer Schaden beim Kläger eingetreten ist. Nicht erforderlich ist hingegen, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat (EuGH Urteil vom 04.05.2023, Az. C-300/21)

Der Kläger hat einen konkreten, mit dem Daten-Scraping in Zusammenhang stehenden Schaden behauptet. Diesen hat zur Überzeugung des Gerichts der Sohn des Klägers im Rahmen der persönlichen Anhörung nachvollziehbar erläutert. Danach ist davon auszugehen, dass der Kläger seit 2021 vermehrt Kaltakquiseanrufe, Werbe-SMS sowie in einem Fall einen Betrugsversuch per Telefon, in welchem eine Anruferin sich wahrheitswidrig als Tochter des Klägers ausgab, erhielt. Das Gericht geht davon aus, dass die über das Scraping erlangten Daten hierfür zum Einsatz kamen. Eine nachvollziehbare andere Erklärung hierfür liegt nicht auf der Hand, zumal ein zeitlicher Zusammenhang mit der Veröffentlichung der gescrapten Daten ohne weiteres herstellbar ist (vgl. LG Stuttgart, Urteil vom 26.01.2023, Az. 53 O 95/22).

Darüber hinaus kann nicht davon ausgegangen werden, dass der Kläger Angst wegen eines Kontrollverlusts über seine Daten gehabt hätte, vielmehr ist eher das Gegenteil der Fall. Der Kläger hat seine Voreinstellungen auf Facebook nicht geändert und letztlich hierfür zu keinem Zeitpunkt eine Veranlassung gesehen, weil ihm offenkundig die Nutzung der Plattform mit all ihren Funktionen wichtiger gewesen ist. Das wäre anders, stünde eine – in der Klage wiederum nur floskelhaft und ohne jeden Bezug zum konkreten Mandatsverhältnis behauptete – tatsächliche Sorge über einen Kontrollverlust im Raum.

Die Beeinträchtigung des Klägers durch regelmäßige Anrufe und SMS über einen längeren Zeitraum überschreitet die Grenze einer hinzunehmenden Unannehmlichkeit und begründet einen Schaden im Sinne des Art. 82 DS-GVO.

b. Kausalität

Die streitgegenständlichen Verstöße gegen Privacy by Default, Datenverarbeitungssicherheit und Meldepflichten nach Art. 33, 34 DS-GVO waren ursächlich für den beim Kläger eingetretenen immateriellen Schaden.

Etwas anderes gilt für einen unterstellten Verstoß der Beklagten gegen die Informationspflicht nach Art. 13 DS-GVO. Der Kläger ist nach der Darstellung seines Sohnes in der mündlichen Verhandlung von den Informationen und Einstellungsmöglichkeiten bei Facebook eher überfordert. Er hat auch nach dem streitgegenständlichen Scraping-Vorfall seine Datenschutzeinstellungen nicht angepasst. Das Gericht ist nicht der Überzeugung, dass eine weitergehende Information des Klägers über die Verwendung seiner Telefonnummer dazu geführt hätte, dass dieser sein Verhalten oder seine Datenschutzeinstellungen geändert hätte.

c. Schadenshöhe

Dem Kläger erachtet einen gemäß § 287 Abs. 1 Satz 1 ZPO zu schätzenden immateriellen Schadensersatz in Höhe von 400,00 Euro für gerechtfertigt.

Für die Höhe des Schmerzensgeldes ist für das Gericht von entscheidender Bedeutung, dass sich aus dem Scraping-Vorfall kein materieller Schaden des Klägers realisiert hat. Mit zunehmendem Zeitablauf verlieren die gescrapten Daten an Aktualität. Der Kläger ist vorgewarnt und in der Lage, entweder seine Kontaktdaten zu ändern oder missbräuchlichen Kontaktaufnahmen zu widerstehen. Somit verbleibt ein spürbares, jedoch nicht überwältigendes Lästigkeitsmoment des Datenverlustes, welches den Kläger beeinträchtigt.

Das Gericht berücksichtigt, dass die Beklagte durch die Art und Weise der Datenerhebung systematisch gegen die Vorgaben der DS-GVO verstößt, um damit die von ihr betriebene Facebook-Plattform zu fördern.

Keine besondere - schmerzensgelderhöhende - Bedeutung hat das Gericht der monopolnahen Verbreitung der Beklagte beigemessen. Diese führt dazu, dass die Beklagte einer potenziellen Vielzahl von Schadensersatzansprüchen ausgesetzt ist. Dass dies jedoch den Anspruch im Einzelfall erhöhen müsste, sieht das Gericht nicht. Auch einen präventiven Zweck des Schmerzensgeldes unterstellt (vgl. *Quaas* in BeckOK Datenschutz, Art. 82 DS-GVO, Stand: 01.05.2023, Rn. 36), dürfte die Höhe des verhängten Schmerzensgeldes - eine Vielzahl vergleichbarer Ansprüche unterstellt - eine abschreckende Wirkung entfalten.

ll. Feststellung (Klageantrag Ziffer 2)

Nachdem dem Kläger ein Schadensersatzanspruch nach Art. 82 Abs. 1 DS-GVO zusteht, hat er ebenso Anspruch auf Feststellung der Ersatzpflicht weiterer Schäden. Es ist nicht ausgeschlossen, dass der Kläger infolge der Verstöße der Beklagten gegen die DS-GVO – auch – materielle Schäden erleidet.

lll. Unterlassung (Klageantrag Ziffer 3)

Darüber hinaus kann der Kläger die mit dem Klageantrag Ziffer 3 beanspruchte Unterlassung im Wesentlichen erfolgreich gegenüber der Beklagten geltend machen (vgl. LG Stuttgart, Urteil vom 26.01.2023, Az. 53 O 95/22–, Rn. 111 [juris]).

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

Die Beklagte hat gegen Art. 25 Abs. 2 DS-GVO, gegen Art. 32, 24, 5 Abs. 1 lit. f) DS-GVO, gegen Art. 33 DS-GVO und gegen Art. 34 Abs. 1 DS-GVO verstoßen. Diese Rechtsverstöße geben dem Kläger einen darauf bezogenen Anspruch auf Beseitigung und künftige Unterlassung.

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

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.

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 des Klägers nicht entgegen. Durch mögliche, vom Kläger selbst vorzunehmende Änderungen von Einstellungen in seinem Facebook-Profil ist eine Wiederholungsgefahr nicht entfallen, und der Kläger 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 (zum Vorstehenden insgesamt LG Stuttgart, Urteil vom 26.01.2023, Az. 53 O 95/22, Rn. 112 - 118 [juris]).

Die Ordnungsmittelandrohung folgt aus § 890 ZPO.

IV. Auskunft (Klageantrag Ziffer 4)

Dem Kläger steht kein (weiterer) Auskunftsanspruch aus Art. 15 DS-GVO zu.

Ein Anspruch des Klägers auf erneute Auskunft zu den Empfängern der durch Scraping erlangten Daten besteht nicht. Der Kläger hat einen solchen Anspruch grundsätzlich gemäß Art. 15 Abs. 1 lit. c) DS-GVO. Die Beklagte hat diesen Anspruch jedoch erfüllt, indem sie erklärte, welche Daten durch die Scraper veröffentlicht wurden (Anlage B16, dort S. 3). Die Beklagte erklärte darüber hinaus, dass sie keinen Datensatz zum Scraping-Vorgang selbst habe. Da die Beklagte die gescrapten Daten nicht aktiv weitergab, erscheint dies nachvollziehbar und wird von dem Kläger auch nicht substanziiert in Frage gestellt.

Soweit der Kläger darüber hinaus generell „Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet“ begehrt, besteht ein derartiger Anspruch nicht. Die Beklagte hat diesen Anspruch erfüllt, indem sie mit Schreiben vom 07.10.2021 (Anlage B16, dort S. 3 f.) erläuterte, wie der Kläger eine Übersicht der von der Beklagten verarbeiteten personenbezogenen Daten herunterladen könne. Eine Auskunftserteilung über ein elektronisches Auskunftssystem ist ausweislich Erwägungsgrund 63 DS-GVO eine zulässige Art und Weise der Erteilung der Auskunft nach Art. 15 DS-GVO (so auch *Bäcker* in Kühling/Buchner, Art. 15 DS-GVO, 2020, Rn. 31).

V. Außergerichtliche Rechtsanwaltskosten (Klageantrag Ziffer 5)

Der Kläger hat keinen Anspruch auf Ersatz außergerichtlicher Rechtsanwaltskosten.

Im Rahmen des ihm zustehenden materiellen Schadensersatzanspruchs nach Art. 82 Abs. 1 DS-GVO kann der Kläger zwar grundsätzlich Erstattung vorgerichtlich angefallener Rechtsanwaltsgebühren beanspruchen.

Vorliegend fehlt es jedoch an einer schlüssigen Darlegung des Schadens. Der Sachvortrag des Klägers besteht aus einem Verweis auf Anlage K1. Die in dieser genannten angeblichen außergerichtlichen Kosten von 887,03 Euro sind jedoch nicht mit Klageantrag Ziffer 5 in Einklang zu bringen, mit welchem die Zahlung von 453,87 Euro begehrt wird. Ein Hinweis war gemäß § 139 Abs. 2 ZPO entbehrlich, da nur eine Nebenforderung betroffen ist.

**C.**

I. Kosten

Die Kostenentscheidung folgt aus § 92 Abs. 1 S. 1 ZPO.

Der Kläger hat bei einem Streitwert von 3.000,00 Euro obsiegt in Höhe von 1.800,00 Euro (Klageantrag Ziffer 1: 400,00 Euro; Klageantrag Ziffer 2: 400,00 Euro; Klageantrag Ziffer 3: 1.000,00 Euro).

II. Vorläufige Vollstreckbarkeit

Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt aus §§ 709, 708 Nr. 11, 711 ZPO.

**D.**

Der Streitwert der Klage beträgt 3.000,00 Euro. Dieser Wert teilt sich auf Klageanträge 1 bis 4 auf wie folgt:

Klageantrag Ziffer 1: 1.000 Euro

Bei einem bezifferten Schadensersatzanspruch ist diese Bezifferung maßgeblich für deren Streitwert.

Klageantrag Ziffer 2: 500 Euro

Der Kläger beantragt die Feststellung der Schadensersatzpflicht der Beklagten für zukünftige Schäden für eine Datenpanne bei der Beklagten aus dem Jahr 2019. Geht es um die Feststellung der Pflicht zum Ersatz künftigen Schadens, ist zu berücksichtigen, wie hoch oder wie gering das Risiko eines Schadenseintritts und einer tatsächlichen Inanspruchnahme des Beklagten durch den Feststellungskläger ist (*Toussaint* in BeckOK KostR, § 48 GKG, Stand: 01.07.2022, Rn. 61.1). Die Datenpanne liegt drei Jahre zurück und ist heute bekannt. Die Gefahr des Missbrauchs von Daten sinkt mit Zeitablauf, da sowohl mangels Aktualität der Daten deren Eignung für einen Missbrauch sinkt als auch nach Entdeckung einer Panne für besonders sensible Daten von Gegenmaßnahmen - z.B. Austausch erbeuteter Passwörter - auszugehen ist.

Klageantrag Ziffer 3: 1.000 Euro

In nichtvermögensrechtlichen Streitigkeiten ist der Streitwert unter Berücksichtigung aller Umstände des Einzelfalls, insbesondere des Umfangs und der Bedeutung der Sache und der Vermögens- und Einkommensverhältnisse der Parteien, nach Ermessen zu bestimmen, § 48 Abs. 2 S. 1 GKG. Bei einem Unterlassungsanspruch ist maßgeblich die Beeinträchtigung, die von dem beanstandeten Verhalten zu besorgen ist und die mit dem Klageantrag beseitigt werden soll (*Roth* in Stein/Jonas, § 3 ZPO, 2013, Rn. 67). Vorliegend ist insbesondere zu berücksichtigen, dass das Interesse des Klägers vorrangig auf einen Schadensersatzanspruch abzielt. Auf Frage des Gerichts nach dem Ziel der Klage hat der Kläger alleine die Ausgleichszahlung genannt, die Unterlassung als Ziel der Klage hat er nicht einmal erwähnt (S. 2 des Protokolls der mündlichen Verhandlung). Einen möglichen Schadensersatz hat der Kläger selbst mit maximal 1.000,00 Euro beziffert. Das Interesse an einem flankierende Unterlassungsanspruch liegt im Regelfall jedenfalls nicht über dem Wert des auf Zahlung gerichteten Klageantrags, welcher das eigentliche Klageziel darstellt.

Klageantrag Ziffer 4: 500 Euro

Ein Antrag nach Art. 15 DSGVO ist regelmäßig mit 500 Euro angemessen bewertet (LAG Baden-Württemberg, Beschluss vom 23.1.2020, Az. 5 Ta 123/19; LAG Baden-Württemberg, Beschluss vom 23.01.2020, Az. 5 Ta 123/19; *Toussaint* in BeckOK KostR, § 48 GKG, Stand: 01.07.2022, Rn. 58b). Besondere Umstände, welche einen höheren Streitwert begründen könnten, sind vorliegend nicht ersichtlich.

## 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 Stuttgart
Urbanstraße 20
70182 Stuttgart

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

Schriftlich einzureichende Anträge und Erklärungen, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zu Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument zu übermitteln. Ist dies aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig. Die vorübergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen.

Rinnert
Richter am Landgericht