Aktenzeichen:
4 O 261/22

Landgericht Ulm

Im Namen des Volkes

Urteil

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **Wilde, Beuger, Solmecke**, Kaiser-Wilhelm-Ring 27 - 29, 50672 Köln, Gz.: 2072/21

gegen

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

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

wegen Persönlichkeitsrechtsverletzung, Verstöße gegen die Datenschutz-Grundverordnung (nachfolgend: DSGVO)

hat das Landgericht Ulm - 4. Zivilkammer - durch den Richter am Landgericht als Einzelrichter aufgrund der mündlichen Verhandlung vom 16.06.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in Höhe von 500,00 € nebst Zinsen seit 20.09.2022 in Höhe von 5 Prozentpunkten über dem Basiszinssatz zu bezahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen Schäden zu ersetzen, die der Klägerseite dadurch entstehen, dass unbefugten Dritter durch das von der Beklagten für das Jahr 2019 eingeräumte „Scraping-Ereignis“ die Verknüpfung der Mobilfunknummer des Klägers mit seiner Facebook ID für das Profil „ “, seinem Geschlecht und Wohnort erlangen konnten.

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,

   die Telefonnummer der Klägerseite durch Kontaktvorschläge für Dritte, welche diese Telefonnummer abfragen, mit dem Facebookprofil „ “ (ID:) zu verknüpfen, solange der Kläger hierzu nicht ausdrücklich einwilligt. Eine Einwilligung liegt nicht vor, solange vor einer solchen Erklärung ggf. keine eindeutige Information darüber erfolgt ist, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert wird und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird, nicht vor.

4. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 367,23 € zu zahlen zuzüglich Zinsen seit 20.09.2022 in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

5. Im Übrigen wird die Klage abgewiesen.

6. Die Kosten des Rechtsstreits werden gegeneinander aufgehoben.

7. Das Urteil ist in Bezug auf Ziff. 1, 4 und 5 gegen Sicherheitsleistung in Höhe von 110 % des zu vollstreckenden Betrages und im Hinblick auf Nr. 3 gegen Sicherheitsleistung von 2.500 € vorläufig vollstreckbar.

8. Der Streitwert wird auf bis 8.000 € festgesetzt.

Tatbestand

Der Kläger macht Ansprüche wegen angeblicher Datenschutzverstöße gegen die Beklagte geltend.

Der Kläger unterhält auf der Social-Media-Plattform Facebook, welche die Beklagte betreibt, das Profil „ “. Der Kläger teilte der Beklagten auf Abfrage seine Handynummer mit. Auf der Abfragemaske ist ein Link zu den Datenrichtlinien und Nutzungsbedingungen gesetzt. Weitere Angaben über die Verwendung der Mobilfunknummer finden sich aber nicht unmittelbar auf der Anmeldemaske, sondern erst im Hilfebereich.

In den „Datenrichtlinien“ war der allgemeine Hinweis vorhanden, dass die Nutzer auswählen können, mit wem sie „Inhalte“ teilen wollen und öffentliche Inhalte sowohl innerhalb des Portals als auch außerhalb jedem zur Verfügung stünden.
Nach der Anmeldung konnten die Nutzer im Hilfebereich folgende Information zur Mobilfunknummer finden:

„*Möglicherweise verwenden wir deine Mobilnummer für diese Zwecke:*

Um dir bei der Anmeldung zu helfen: Wenn du dein Passwort oder deine E-Mail-Adresse vergessen hast, über die du dich bei Facebook anmeldest, kannst [du] diese erfragen, indem du die mit deinem Konto verbundene Mobilnummer eingibst.

Um dein Konto mit Opt-in Funktionen wie die zweistufige Authentifizierung oder SMS-Nachrichten bei Logins über unbekannte Geräte zu schützen.

Um dir Personen, die du kennen könntest, vorzuschlagen, damit du dich mit ihnen auf Facebook verbinden kannst.

Beachte, dass du kontrollieren kannst, wer deine Telefonnummer sehen kann. Mehr dazu erfährst du in unserer Datenrichtlinie.“

In den Privatsphäreneinstellungen, die von den Nutzern aufgerufen werden können, konnten die

Nutzer auswählen, wem die zur Verfügung gestellte Telefonnummer auf dem Profil angezeigt werden sollte. Die Voreinstellung war „Freunde“. Die Telefonnummer war daher nicht für jede Person öffentlich einsehbar. Zudem gab es die Einstellung: „Wer kann mithilfe der von dir zur Verfügung gestellten Telefonnummer nach dir suchen? Das trifft auf die Personen zu, die deine Telefonnummer nicht in deinem Profil sehen können“. Die Voreinstellung hierzu war „Alle“. Der Kläger änderte die Voreinstellungen nicht.

Die Beklagte bot auch einen „Privatsphärencheck“ an, mit dem die Einstellungen aktiv überprüft werden konnten.

Die Beklagte bot zudem für Mobiltelefone eine Applikation an (App), welche die Funktion „Contact Importer Tool“ (CIT) beinhaltete. Diese fragte die auf dem Mobiltelefon gespeicherten Telefonnummern ab und glich diese mit den Telefonnummern ab, die bei der Beklagten gespeichert waren und bei denen die Privatsphäreneinstellungen zur Suche von Kontakten über Telefonnummern auf „Alle“ gestellt waren.

Wohl im Jahr 2019 nutzten „Scraper“ das Contact Importer Tool, entgegen der Nutzungsbestimmungen der Beklagten, um zu einer vorgegebenen Nummer, welche die „Scraper“ aus unbekannter Quelle hatten oder eventuell einfach „durchzählten“, das zugehörige Facebookprofil vorgeschlagen zu bekommen, um somit einen Datensatz zu erstellen, welcher Facebooknutzername zu welcher Telefonnummer gehört. Zudem griffen die Scraper die öffentlich auf dem Profil einsehbaren Informationen ab. “Scraping“ bezeichnet das Sammeln von Daten aus zugänglichen Quellen im Internet, um diese zu einem Datensatz zusammenzufügen.

Die Beklagte stellte fest, dass der Kläger von dem Scrapingereignis in verschiedenen Kategorien betroffen ist.

Mit E-Mail vom 10.06.2021 forderte der Kläger vertreten durch die Klägervertreter ein Schmerzensgeld von 500 €, „*die rechtswidrige Verarbeitung der personenbezogenen Daten unserer Mandantschaft – hier das Zugänglichmachen für Unbefugte - (...) zu unterlassen*“ und verschiedene Auskünfte, darunter: „*Wie oft wurden diese, unsere Mandantschaft betreffende personenbezogenen Daten abgefragt?*“.

Der Kläger trägt vor und ist der Meinung,

Die Beklagte habe keinerlei Sicherheitsmaßnahmen vorgehalten, um das Ausnutzen des CIT zur Datensammlung zu verhindern. Außerdem habe sie die Einstellungen zur Sicherheit der Telefon-

nummer auf Facebook so undurchsichtig und kompliziert gestaltet, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Die Einstellungsmöglichkeiten und Informationen seien gerade nicht einfach zu finden. Die Beklagte habe den Eindruck erweckt, dass die Telefonnummer gerade nicht veröffentlicht werde, dann aber jedem die Verknüpfung der Nummer mit dem Profil der Klägerin ermöglicht.

Als Sicherheitsmaßnahmen wären z.B. eine Abfragebegrenzung oder eine Captchaabfrage in Betracht gekommen. Keine dieser Sicherheitsmaßnahmen hätte die Beklagte eingerichtet. Zudem habe sie ihn von dem Datenleck benachrichtigen müssen, was sie ebenfalls unterlassen habe. Auch die Datenauskunft sei nicht richtig erfolgt, da nicht mitgeteilt worden sei, wem die Daten zur Verfügung gestellt worden seien.

Auf Grund dieser Versäumnisse sei nun im Internet folgendes Datenpaket frei verfügbar:

„*[Telefonnummer des Kl.],[Facebook ID des Klägers],*

,“

Der Kläger behauptet, dass er in Kenntnis der Reichweite eine Zustimmung zur Nutzung der Telefonnummer nie erteilt hätte. Auf Grund des veröffentlichten Datensatzes erhalte er Anrufe und Nachrichten auf sein Handy, denen jeweils ein Betrugsversuch zu Grunde liege.

Die Beklagte schulde auch eine Auskunft darüber, welchen „Scrapern“ die Daten des Klägers über das CIT zugänglich gemacht worden seien. Die Beklagte habe Log-Dateien zu diesen Vorgängen. Da dies nicht erfolgt sei, sei die Auskunftspflicht nach DSGVO nicht erfüllt.

Der Kläger beantragt daher,

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, Facebook ID, 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.

Sie trägt vor und ist der Meinung,

einen „Datenschutzvorfall“ oder ein „Hacking“ habe es nicht gegeben. Sie habe lediglich die persönlichen Daten des Klägers weitergegeben, für welche die erforderliche Zustimmung vorliege.

So bedinge schon der Abschluss eines „Social-Media-Vertrages“, wie er zwischen den Parteien bestehe, dass der Name, die NutzerID und andere Basisdaten, die zum Betrieb eines „sozialen Netzwerkes“ notwendig seien, offen gelegt werden dürften. Die Telefonnummer sei gerade nicht offen gelegt worden. Beim Scraping sei diese von den Anfragenden vorgegeben worden. Sie habe dann lediglich auf das Nutzerprofil verwiesen, auf dem Namen, Geschlecht und die BenutzerID öffentlich hinterlegt seien.

Die Hinweise, wie die Funktion der Kontaktsuche per Telefonnummer ausgeschaltet werden könne, seien auch gut zu finden. Sie habe den Kläger jederzeit über die Hilfeseite, den Privatsphärencheck und die Datenrichtlinien über die Nutzung der Daten informiert.

Die Daten seien auch jederzeit nach dem Stand der Technik geschützt gewesen. Die Beklagte habe ein Sicherheitsteam eingerichtet und Anfragelimits sowie Captchaabfragen implementiert gehabt.

Der Kläger habe auch keinen Schaden erlitten. Das „Abhandenkommen“ der Daten allein stelle einen solchen nicht dar. Die lästigen Nachrichten und Anrufe von Fremden seien nicht auf das Datenpaket zurückzuführen, da dabei auch keine weitergegebenen Daten benutzt worden seien.

Die Beklagte wisse auch nicht, bei wann ein „Scraper“ unberechtigterweise Daten des Klägers abgefragt hätte. Die von Klägerseite behaupteten Logdateien gebe es nicht.

Die Auskunft über die bei der Beklagten gespeicherten Daten könne der Kläger jederzeit selbst über eine Selbstabfragetool ausführen. Weitere Auskünfte seien nicht geschuldet.

Zum weiteren Vortrag der Parteien wird auf die Schriftsätze bei der Akte Bezug genommen. Das Gericht entscheidet nach mündlicher Verhandlung und Anhörung des Klägers ohne weitere Beweisaufnahme.

Entscheidungsgründe

Die zulässige Klage ist teilweise begründet.

I.

1.

Die Klage ist zulässig.

Das Landgericht Ulm ist nach Art. 18 Abs. 1 2. Alt EuGVVO örtlich und international zuständiges Gericht. Die sachliche Zuständigkeit ergibt sich aus § 71 GVG i.V.m. § 23 Nr. 1 GVG.

2.

Der Schmerzensgeldantrag konnte in unbezifferter Weise gestellt werden, da der Kläger eine vom Gericht zu schätzende billige Entschädigung beantragt. Der Antrag ist nicht deshalb unzulässig, da er auf alternative Sachverhalte gestützt werden würde. Zwar ist eine Klage unzulässig, die sich alternativ auf mehrere Klagegründe stützt (Zöller ZPO, Greger, 34. Aufl. 2022, § 260 Rn. 5). Der Klagegrund ist aber der Lebenssachverhalt, welcher der Klage zu Grunde gelegte wird. Er wechselt erst, wenn der bisherige Lebenssachverhalt wesentlich, d.h. im Kern geändert wird (Musielak/Voit/Foerste, 19. Aufl. 2022, ZPO § 263 Rn. 3). Gerade im Falle des Schmerzensgeldes ist dabei zu sehen, dass dieses einheitlich ausgesprochen wird, also für alle auf dem gleichen Grund bestehenden Beeinträchtigungen (BGH NJW 2004, 1243 (1244)).

Der Kernsachverhalt, den der Kläger hier vorträgt, ist, dass im Internet ein Datensatz aufgetaucht sei, der aus dem System der Beklagten stamme und seinen Namen mit der Telefonnummer verbinde. Dieser Sachverhalt wird nur weiter ausgestaltet dadurch, dass der Kläger auch rügt, dass ihm keine Mitteilung hierüber gemacht worden sei und auch auf sein Auskunftsbegehren hin keine nähere Information erfolgt seien, wohin die Daten geflossen wären. Dies betrifft alles im Kern den gleichen Sachverhalt. Der Kläger verdeutlicht in den Ausführungen zur Bemessung des Schmerzensgeldes, dass das Schmerzensgeld nicht alternativ auf eine Verletzung der Auskunftspflicht gestützt werden soll, sondern dies den eigentlichen Verstoß nur intensiviere (Klageschrift S. 46f.).

3.

Der Feststellungsantrag Ziff. 2 hat das erforderliche Feststellungsinteresse nach § 256 Abs. 1 ZPO, jedenfalls soweit der Feststellungsantrag begründet ist. Das Feststellungsinteresse liegt regelmäßig vor, wenn eine zukünftige Schadensentstehung möglich ist (BeckOK ZPO/Bacher, 47. Ed. 1.12.2022, ZPO § 256 Rn. 24). Dies ist hier der Fall, da nach dem Vortrag der Klägerin die Daten im Internet verfügbar sind und somit z.B. zukünftig eine Betrugstat zu ihrem Nachteil auf Grund der Datenkenntnis in Betracht kommt.

Zwar ist der Klageantrag wohl zu unbestimmt und zu weit gefasst, so dass er die unerlaubte Handlung der Beklagten kaum erkennen lässt, insbesondere weil der Antrag nicht aufführt, warum ein Zugriff „unbefugt“ gewesen sein soll: (“unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten“). Klageanträge sind jedoch vor dem Hintergrund der Klagebegründung nach ihrem Sinn und Zweck auszulegen (OLG Brandenburg Urt. v. 5.4.2019 – 4 U 68/18, BeckRS 2019, 6708 Rn. 11). Demnach steht für den Kläger im Vordergrund, dass Unbefugte durch Eingabe einer Telefonnummer auf Grund der Datenherausgabe der Beklagten herausfinden konnten, dass diese Telefonnummer seinem Namen zuzuordnen ist. Der Kläger will daher feststellen lassen, dass die Beklagte es hätte unterlassen und/oder verhindern müssen, dass Unbefugte bei Eingabe der Telefonnummer seinen Namen genannt bekommen.

4.

Auch die Unterlassungsanträge sind bestimmt genug i.S. des § 253 Abs. 2 Nr. 2 ZPO.

Dies gilt im Hinblick auf den Antrag Nr. 3a) im Hinblick auf die technischen Einrichtungen „nach dem Stand der Technik“. Der Kläger hat einen Anspruch darauf, dass der begangene Rechtsverstoß und ein kerngleicher Verstoß nicht wiederholt wird. Dazu muss er den begangenen Verstoß bezeichnen, was jedenfalls nach sachgemäßer Auslegung des Antrags vor dem Hintergrund der Klagebegründung möglich ist (s.o.). Sodann hat die Beklagte ein Wahlrecht, wie sie den Verstoß verhindern will. Klägerseits kann daher kein genaues Vorgehen vorgegeben werden, so dass die Angabe des rechtlichen Rahmens, in dem die Abhilfe erfolgen muss (“nach dem Stand der Technik“) ausreicht (MüKoBGB/Raff, 9. Aufl. 2023, BGB § 1004 Rn. 320). Eine weitere Bestimmung ist dem Kläger nicht möglich.

Im Hinblick auf den Antrag Nr. 3b rügt die Beklagte zu Recht die Verwendung unbestimmter Be-

griffe wie „unübersichtlichen und unvollständigen Informationen“. Im Weiteren nennt der Kläger aber den zu Grunde liegenden Sachverhalt bestimmt, nämlich die Verwendung seiner Telefonnummer zum Zwecke der Kontaktsuche. Nach Auslegung des Antrags ist dieser daher auch bestimmt genug.

II.

Die Klage ist auch teilweise begründet:

1.

Die Klägerin hat gegen die Beklagte einen Anspruch auf Ersatz des immateriellen Schadens nach Art. 82 Abs. 1 DSGVO. Neben der DSGVO ist deutsches Recht anzuwenden (Art 6 Abs. 1 lit. b VO Nr. 593/2008 (Rom I)).

a)

Die Beklagte hat entgegen Art 6 Abs. 1 DSGVO den Namen und die Mobilfunknummer des Klägers, bei denen es sich um personenbezogene Daten nach Art. 4 Nr. 1 DSGVO handelt, verarbeitet, in dem sie bei Abfrage der Mobilfunknummer durch das CIT den Namen des Klägers mitteilte. Hierfür lag keine Einwilligung des Klägers vor.

aa)
Eine Verarbeitung personenbezogener Daten liegt nach der ausdrücklichen Normierung in Art. 4 Nr. 2 DSGVO auch vor, wenn personenbezogene Daten verknüpft werden. Dies hat die Beklagte unstreitig getan. Auf die Abfrage einer Telefonnummer hat die Beklagte hiermit das Profil des Klägers verknüpft und somit seinen Namen, Geschlecht und Heimatstadt (jedenfalls den Bezirk) offengelegt.

Es kommt also nicht darauf an, dass die Beklagte lediglich den Namen des Klägers offengelegt hat, wofür sie nach Art. 6 Abs. 1 lit. b DSGVO die Zustimmung des Klägers hatte, da das Offenlegen des Namens im Social Media Vertrag eine wesentliche Voraussetzung ist, ohne welche die Vertragsdurchführung nicht denkbar wäre. Denn nicht die Offenlegung des Namens stellt die

streitgegenständliche Verarbeitung dar, sondern *die Verknüpfung* mit des Namens mit der abgefragten Telefonnummer. Diese beruht allein auf einer Handlung der Beklagten und war daher nicht Gegenstand dessen, was der Kläger offen legen wollte oder was aus anderen Quellen zu erfahren ist (daher wird der Auffassung in LG Bielefeld GRUR-RS 2022, 38375 Rn. 30 und in LG Halle, Urteil vom 28. Dezember 2022, Az. 6 O 195/22, S. 6-7, nicht gefolgt).

bb)

Dieser Verknüpfung hat der Kläger nicht zugestimmt.

Die wirksame Einwilligung muss im Zeitpunkt der Datenverarbeitung vorliegen und deshalb zuvor erklärt worden sein (BeckOK DatenschutzR/Stemmer, 42. Ed. 1.5.2022, DS-GVO Art. 7 Rn. 88).

Bei Angabe seiner Telefonnummer teilte die Beklagte ihr auf der Anmeldeseite nicht mit, dass diese für die Verarbeitung i.S. der Verknüpfung der mitgeteilten Telefonnummer auf Anfrage mit dem Profil und damit den dort öffentlich enthaltenen Informationen stattfindet.

Unstreitig, stand dem Kläger bei der Eingabe der Telefonnummer lediglich ein Link zu der Datenrichtlinie (und den soweit nicht relevanten Nutzungsbedingungen und Cookie-Richtlinie) zur Verfügung. In dieser war lediglich festgehalten, dass die Nutzer entscheiden können, welche Daten sie öffentlich machen wollen und diese sodann innerhalb und außerhalb der Plattform einsehbar sind. Dass die bei der Anmeldung angegebene Telefonnummer hingegen ohne weitere Willensausübung zur Verknüpfung mit dem Profil führen kann, ist der Datenrichtlinie nicht zu entnehmen. Die Telefonnummer wird gar nicht erwähnt.

Auf eine weitere Prüfung von Art. 7 Abs. 2 DSGVO oder Art. 25 Abs. 2 S. 1 DSGVO kommt es daher gar nicht an. Nur zur Vollständigkeit sei daher erwähnt, dass Art. 25 Abs. 2 S. 1 DSGVO die Zielrichtung hat, das per Voreinstellung eine Verarbeitung nur zulässig ist, soweit der Vertragszweck diese erfordert (Kühling/Buchner/Hartung, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 24). Der Vertragszweck des Social-Media-Vertrages erordert aber nicht unabdingbar, dass Kontaktvorschläge durch einen Abgleich der Telefonnummer möglich sein muss. Die Voreinstellung ist daher eindeutig nicht datensparend und verstößt daher gegen Art. 25 Abs. 2 S. 1 DSGVO. Folge ist, dass eine durch eine solche Voreinstellung erteilte Einwilligung nicht wirksam ist (Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 25 Rn. 45c). Die Ansicht, „*dass es Internetgepflogenheiten gibt, mit denen man sich vertraut zu machen hat*“ (LG Heilbronn Urt. v. 13.1.2023 – 8 O 131/22, BeckRS 2023, 330 Rn. 42, beck-online), ist dagegen nicht geeignet die unmissverständliche gesetzliche Vorschrift außer Kraft zu setzen. „Internetgepflogenheiten“, die datenschonende Grundeinstellun-

gen nicht vorsehen, sind rechtswidrige „Internetgepflogenheiten“.

b)
Dem Kläger ist auch ein immaterieller Schaden i.S. des Art. 82 Abs. 1 DSGVO entstanden.

Zwar ist umstritten, ob sich schon aus dem Erwägungsgrund 85 der DSGVO folgt, dass jedenfalls der Kontrollverlust über die Daten einen immateriellen Schaden darstellt (Wortlaut: „... immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten...“, **a.A.** Schlussanträge Sanchez-Bordona, Rs. C 300/21 Rn. 74).

Nach Erwägungsgrund 146 S. 3 der DSGVO muss aber der Begriff des Schadens so ausgelegt werden, dass er den Zielen der Verordnung entspricht. Der Schadensersatzanspruch muss daher weitere Verstöße unattraktiv machen (Paal, MMR 2020, 14 (16); Diekmann, r+s 2018, 345 (352)). Eine schwerwiegende Persönlichkeitsrechtsverletzung ist daher nicht erforderlich (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18a m.w.N.). Der Schaden muss auch keine „Erheblichkeitsschwelle“ überschreiten (EuGH, Urteil vom 04.05.2023 - CTz. 51 (“Österreichische Post“)).

Deshalb kann ein Schaden auch bereits in einem unguten Gefühl liegen, dass personenbezogene Daten Unbefugten bekannt geworden sind (LAG BW, ZD 2021, 436 Rn. 82). Aber jedenfalls, wenn durch die unbefugte Verarbeitung eine Aufhebung der Pseudonymisierung erfolgt und hierdurch die Gefahr eintritt, dass die Daten zu betrügerischen Maßnahmen verwendet werden könne, liegt nach Erwägungsgrund 75 der DSGVO ein immaterieller Schaden vor (Wortlaut: „*...immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, (...), der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann*“).

Die Argumentation der Beklagtenseite, dass nur ein ungutes Gefühl oder das Abgreifen der Daten an sich keinen Schaden darstellen würden, geht fehl. Jedenfalls, wenn der DSGVO Verstoß zu einer unumkehrlichen Offenlegung von Daten geführt hat, die nach dem Schutzzweck des DS-GVO gerade verhindert werden sollte, muss ein Schaden bejaht werden. Andernfalls könnte von der notwendigen „weiten“ Auslegung es immateriellen Schadensbegriffes (EuGH, Urteil vom 04.05.2023 - C- 300/21 Tz. 46 (“Österreichische Post“) nicht mehr gesprochen werden. Es be-

darf gerade keines pathologischen Übels, sondern der Schadensbegriff ist anhand des Schutzzweckes der DSGVO zu bestimmen (EuGH, Urteil vom 04.05.2023 - C- 300/21 Tz. 40 (“Österreichische Post“). Dieser liegt gerade darin, die Offenlegung von personenbezogenen Daten zu verhindern. Findet solch ein Verstoß statt, hat die Person, deren Daten entgegen dem Schutzzweck der DSGVO offen gelegt worden, einen Schaden. Denn der von der DSGVO beabsichtigte Schutz, wurde verletzt.

Dies ist hier der Fall. Das im Internet verfügbare Datenpaket, an dessen Richtigkeit das Gericht keine Zweifel hat, nachdem die Beklagte nicht bestreitet, dass es die abgegriffenen Kategorien enthält, nennt den Namen des Klägers in Verbindung mit seiner Telefonnummer, dem Geschlecht und seinem Heimatort. Dies ist geeignet zu einem Identitätsdiebstahl zu führen, als auch zur namentlichen Ansprache des Klägers am Telefon, was Ausgangspunkt von Betrugsstraftaten sein kann. Die zunächst „anonyme“ Telefonnummer wird somit dem Kläger zuordenbar und zudem besteht mit dem Wohnort weiteres Detailwissen. Mit den Angaben können z.B. über eine Suchmaschine noch weitere Daten des Klägers in Erfahrung gebracht werden, die - was eben ohne die Handlungen der Beklagten nicht möglich gewesen wäre - mit der Telefonnummer verknüpft werden können.

Der Kläger hat daher einen tatsächlichen immateriellen Schaden erlitten.

c)

Der immaterielle Schaden ist mit einem Betrag von 500,00 € auszugleichen.

Die Höhe des Anspruchs ist bei immateriellen Schäden nicht willkürlich, sondern auf der Grundlage der inhaltlichen Schwere und Dauer der Rechtsverletzung zu beurteilen. Ein künstlich niedrig bezifferter Betrag mit symbolischer Wirkung reicht nicht aus, um die praktische Wirksamkeit des Unionsrechts sicherzustellen (Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 12a). Andererseits reichen. Andererseits sind „bloßer Ärger“ oder Bagatellen nicht mit Geldansprüchen auszugleichen (Schlussanträge Sanchez-Bordona, Rs. C 300/21 Rn. 117).

Dabei ist einerseits zu berücksichtigen, dass die Beklagte erkannt haben muss, dass keine wirksame Einwilligung zur Verknüpfung der Telefonnummer zu den Profilinformationen vorliegt. Bei Schaffung der Möglichkeit des CIT muss die Beklagte die datenschutzrechtliche Zulässigkeit überprüft haben. Dabei muss sie erkannt haben, dass die Voreinstellung, dass die Telefonnum-

mer mit den Profilinformationen verknüpft wird, nicht datenschonend ist, sondern das Gegenteil. Sie ist eindeutig rechtswidrig.

Zudem hat der Kläger erst 2021 und auch nicht durch die Beklagte Kenntnis davon erlangt, dass seine Telefonnummer im Internet mit seinem Namen verknüpft ist. Dies wohl schon seit 2019. Es wird ihr auch nicht möglich sein, diese Daten wieder „unter Kontrolle“ zu bringen, da unbekannt bleiben wird, inwieweit sie sich schon verbreitet haben.

Andererseits ist aber zu sehen, dass lediglich eine Verbindung des Namens mit der Telefonnummer vorliegt und somit eine Information die z.B. im Hinblick auf einen Festnetzanschluss häufig schon dem Telefonbuch zu entnehmen ist, oder bei einem Anruf durch das einfache Melden des Gegenparts feststeht. Ein hohes Betrugspotential wird damit nicht geschaffen. Dass die vom Kläger geschilderten, unerwünschten Anrufe und Nachrichten auf seinem Handy auf dem Datenpaket beruhen, ist eher unwahrscheinlich, soweit keine persönliche Ansprache erfolgte, wie bei den vom Kläger geschilderten Sachverhalten der Fall. Das „Raten“ von Telefonnummern z.B. durch einen Anrufcomputer wird dabei von Klägerseite selbst als Möglichkeit genannt.

Es ist aber zu sehen, dass der Kläger glaubhaft dargestellt hat, dass ihm der Schutz seiner Daten wichtig ist, wie die zurückhaltenden Informationen auf dem Facebookprofil und die Änderung der Einstellungen zur Verbreitung der Telefonnummer durch den Kläger noch 2021 beweisen.

Zu berücksichtigen ist auch, dass mit dem weiter tenorierten Feststellungs- und Unterlassungsanspruch auch eine Genugtuung geschaffen wird, da somit die Rechtswidrigkeit des Handelns der Beklagten ausgesprochen wird (vgl. Schlussanträge Sanchez-Bordona, Rs. C 300/21 Rn. 89ff.). Die Festsetzung eines immateriellen Schadensbetrages soll gerade nicht zur Bereicherung einer Person dienen, sondern zur Wiedergutmachung erlittenen Unrechts.

Zur Festsetzung des immateriellen Schadens zieht das Gericht daher folgende Entscheidungen heran:
LG Köln Urt. v. 18.5.2022 – 28 O 328/21, BeckRS 2022, 11236 - 1.200 €: Verlust durch ein Datenleck: Vor- und Nachname, Titel, Anschrift, Geburtsdatum, Geburtsort, Geburtsland, Staatsangehörigkeit, E-Mail-Adresse, Telefon/Mobilfunknummer, Familienstand, Steuerliche Ansässigkeit, Steuer-ID und Bankverbindung

LG München I, ZD 2022, 242 - 2.500 € - Gleicher Sachverhalt wie LG Köln, aao.

ArbG Lübeck ZD 2020, 422 - 1.000 € „Obergrenze“ Veröffentlichung eines Bildes

LAG Köln ZD 2021, 168 - 300 € Veröffentlichtes Mitarbeiterprofil

LG Lüneburg BeckRS 2020, 36932 - 1.000 €: Kurzzeitige, unberechtigte Schufa-Eilmeldung

OLG Frankfurt NJW-RR 2022, 1608 Rn. 53 - 500 €: Alter Kontostand und Dispozins. Kenntnis von nur zwei unberechtigten Personen

Keine der genannten Entscheidungen ist mit dem vorliegenden Sachverhalt vergleichbar. Zu beachten ist aber der wohl „endgültige“ Kontrollverlust des Klägers. Jedoch ergeben sich nur einfach zu entdeckende Betrugsmöglichkeiten und es gibt keine Auswirkungen auf die Bonität des Klägers. Auch kann er durch eine Änderung der Handynummer die Folgen beseitigen.

Ausgehend von dem genannten Rahmen ist der Ausgleichsbetrag daher auf 500 € festzusetzen. Dieser Betrag ist geeignet die Ziele der DSGVO sicherzustellen. Auch wenn der Einzelbetrag für die Beklagte wirtschaftlich sicherlich nicht ins Gewicht fällt, sieht sie sich insgesamt umfangreichen Ansprüchen ihrer Kunden ausgesetzt, die mehrheitlich keine Zahlungen für das Social-Media-Profil erbringen. Angesichts dessen, dass die Beklagte ihren Umsatz mit Milliarden Kunden erwirtschaftet, fällt ein Betrag von 500 € für einen Einzelkunden durchaus ins Gewicht.

Die Verzinsung richtet sich nach §§ 291, 288 Abs. 1 BGB.

2.

Auch der Feststellungsantrag ist zuzusprechen. Wie bereits dargelegt, liegt das Feststellungsinteresse vor, da nicht ausgeschlossen werden kann, dass auf Grund der Daten der Kläger Opfer eines Betrugsschemas werden könnte. Dies reicht aus, um den Feststellungsanspruch zuzusprechen. Das die Haftung der Beklagten auslösende Ereignis ist jedoch die Verarbeitung der Mobilfunknummer der Klägerin durch Verknüpfung mit ihren öffentlich einsehbaren Profilinformationen. Da die Klägerin nur beantragt, festzustellen, dass die Beklagte haftet, soweit diese Daten durch unbefugten Zugriff abgerufen worden sind, kann das Gericht über diesen Antrag nicht hinausgehen (§ 308 Abs. 1 ZPO). Somit ist wie tenoriert zu entscheiden.

3. (zu Antrag 3 lit a)

Soweit der Kläger beantragt, dass die Beklagte es unterlassen solle persönliche Daten ohne die notwendige Sicherung online zu stellen, ist der Antrag unbegründet. Dabei kann dahinstehen, ob die Beklagte durch Sicherheitsmaßnahmen nach dem Stand der Technik hätte verhindern können, dass die Verbindung der Telefonnummer mit dem Namen der Klägerin „gescraped“ wird.

Es fehlt eine nach § 1004 BGB notwendige Wiederholungsgefahr (vgl. BeckOK BGB/Fritzsche, 64. Ed. 1.11.2022, BGB § 1004 Rn. 91).

a)
Legt man den Antrag des Klägers so aus, dass als rechtswidrigen Eingriff die fehlende Sicherung der Daten gegen Scraping im Jahr 2019 gesehen wird, ist zu beachten, dass der Beklagten in diesem Urteil im Tenor überhaupt die Nutzung der Telefonnummer in der Kontaktsuche untersagt wird.

Denn der initiale Rechtsverstoß der Beklagten liegt bereits in der Nutzung der Telefonnummer überhaupt für die Zwecke der Kontaktsuche und damit noch „vor“ der Sicherung der Daten. Wie gezeigt, lag keine Einwilligung des Klägers vor, um anderen Nutzern über die Telefonnummer die Kontaktsuche zu ermöglichen. Der Kläger kann daher verlangen - und tut dies auch -, dass seine Nummer gar nicht zu diesen Zwecken genutzt wird und nicht nur bei der Nutzung gegen Scraping gesichert wird.

Dann kann er aber nicht zusätzlich verlangen, dass er dabei vor Scrapern geschützt wird. Denn dies setzt voraus, dass die Telefonnummer überhaupt bei der Kontaktsuche Verwendung findet. Anders können auch Scraper diese nicht zur Verbindung mit dem Facebookprofil nutzen. Nach dem von Klägerseite vorgetragenen Vorgehen der „Scraper“ haben diese die Telefonnummer über das CIT „abgefragt“ um diese mit den öffentlichen Profildaten des Klägers verbinden zu können. Da die Beklagte die Telefonnummer hierzu aber nicht mehr verwenden darf, besteht keine Gefahr mehr, dass die Telefonnummer bei der Verwendung in der Kontaksuche nicht vor Scrapern geschützt wäre. Denn sie kann gar nicht mehr zu diesem Zweck genutzt werden. Eine Wiederholungsgefahr besteht daher nicht mehr. Die Voraussetzungen von § 1004 BGB liegen nicht vor.

b)

Der Kläger kann auch nicht argumentieren, dass seine Daten vor Scrapern geschützt werden müssen, wenn er der Kontaktsuche über die Telefonnummer noch zustimmen sollte, was er in seiner persönlichen Anhörung ausgeschlossen hat. Denn insofern käme es darauf an, ob die Maßnahmen der Beklagten zu diesem Zeitpunkt dem Stand der Technik entsprächen. Der Kläger leistet aber nur Vortrag zu den Maßnahmen 2019, die ohne Belang sind. Auch insoweit ist eine Wiederholungsgefahr daher nicht anzunehmen.

4. (Zu Antrag 3 lit. b)

Der Antrag ist nach korrekter Auslegung begründet.

Legt man den (sprachlich schon schwer verständlichen) Antrag zu Grunde und beachtet hierbei die Klagebegründung, ist der Kläger der berechtigten Meinung, dass eine Einwilligung zur Nutzung der Telefonnummer zur Kontaktsuche nicht wirksam gegeben worden ist. Wie bereits dargelegt worden ist, ist dies korrekt. Ein Anspruch nach § 1004 Abs. 1 BGB analog (i.V.m § 823 Abs. 2 BGB i.V.m. Art. 6 Abs. 1 DSGVO) besteht somit. Dieser wird auch nicht dadurch ausgeschlossen, dass der Kläger inzwischen die Einstellungen geändert hat und daher sein Profil über die Eingabe der Telefonnummer nicht mehr gefunden werden kann.

Der vormals begangene Verstoß indiziert zunächst die Wiederholungsgefahr. An deren Entfallen sind strenge Anforderungen zu stellen. Sie entfällt nicht schon dann, wenn der Antragsgegner die rechtswidrige Handlung zunächst unterlässt oder auch nur versichert sie nicht weiter vorzunehmen (BeckOK BGB/Fritzsche, 66. Ed. 1.2.2023, BGB § 1004 Rn. 93). Es kann daher nicht ausreichen, dass der Nutzer die Einstellung ändern kann oder auch schon geändert hat (a.A. LG Mönchengladbach Urt. v. 10.1.2023 – 3 O 87/22, BeckRS 2023, 2109 Rn. 37). Denn der Anspruchsinhaber hat nicht nur einen Anspruch auf Unterlassung des konkreten Verstoßes, sondern auch auf Unterlassung kerngleicher Verletzungsformen (BGH GRUR 2006, 421 Rn. 27). Diesen Unterlassungsanspruch kann er sich so lange titulieren lassen, bis die Beklagte durch eine strafbewehrte Unterlassungserklärung die Wiederholungsgefahr ausräumt.

Der Antrag der Klägerseite ist jedoch insoweit nicht auf den konkreten Rechtsverstoß bezogen, als auf „eine(r) Einwilligung [des Klägers]“ abgestellt wird. Tatsächlich liegt keine Einwilligung vor. Der Antrag war - wie tenoriert - auszulegen.

5. (Zu Antrag Nr. 4)

Der Kläger macht einen Auskunftsanspruch nach Art. 15 DSGVO geltend. Nach der Klagebegründung rügt er neben einer bisher möglichen Selbstauskunft bzw. erfolgten Auskunft, dass ihm nicht mitgeteilt worden ist, welchen unbefugten Empfänger auf Grund der Eingabe der Telefonnummer sein Kontaktprofil vorgeschlagen worden ist.

Die Beklagte hat aber erklärt, dass ihr keine Daten dazu vorliegen, wem sie über die Nutzung des CIT die Daten des Klägers zur Verfügung gestellt hat. Damit hat sie die erforderliche (Negativ-)Auskunft bereits erteilt. Der Anspruch ist durch Erfüllung untergegangen, § 362 Abs. 1 BGB. Die Richtigkeit der Auskunft wird bei Prüfung der Erfüllung des Auskunftsanspruchs nicht überprüft (BGH GRUR 1994, 630 (632)).

6.

Der Kläger hat nach Art. 82 Abs. 1 DSGVO auch Anspruch auf Ersatz der vorgerichtlichen Rechtsanwaltsgebühren. Die Kosten der außergerichtlichen Aufforderung, da diese berechtigt erfolgt ist, sind als Kosten der berechtigten Rechtsverfolgung ersatzfähig. Der Kläger verfolgte außergerichtlich einen berechtigten Anspruch mit einem Streitwert von 3.000 €. Dieser umfasst den Unterlassungsanspruch, der hälftig berechtigt ist (2.500 €) und die vorgerichtlich geforderten 500 € immateriellen Schadensersatz. Zur Streitwertberechnung wird auf die folgende Begründung zum Streitwert des Verfahrens Bezug genommen. Die Rechtsanwaltskosten betragen daher 367,23 €. Die Verzinsung richtet sich nach §§ 291, 288 Abs. 1 BGB.

III.

Die Kostenentscheidung ergeht nach § 92 Abs. 1 ZPO. Auf Grund der Tatsache, dass der Kläger einen unbezifferten Schmerzensgeldantrag geltend gemacht hat und die Streitwertfestsetzung jeweils innerhalb großer, vertretbarer Spannen erfolgte, scheint eine genaue Verteilung der Kosten prozentual nach den angesetzten Streitwerten der einzelnen Ansprüche nicht dem billigen Ermessen zu entsprechen. Vielmehr dürfte der Kläger bei umfassender Betrachtung des Streitstoffes zu gleichem Teil Obsiegen wie Unterliegen. Die in § 92 Abs. 1 ZPO vorgesehene Kostenaufhebung erscheint daher gerade unter Berücksichtigung des Grundsatzes der Kostengerechtigkeit angemessen. Die vorläufige Vollstreckbarkeit folgt § 709 ZPO.

Der Streitwert ist wie folgt festzusetzen:

Antrag Ziff. 1: 1.000 €

Antrag Ziff. 2: 250 €

Das Feststellungsinteresse ist von sehr untergeordneter Bedeutung, da der Kläger keinen Vorfall geltend machen kann, der wahrscheinlich auf dem Scraping-Vorfall beruht. Zukünftige Schäden sind daher fernliegend.

Antrag Ziff. 3 insgesamt 5.000 €

Streitwerte in Bezug auf Unterlassungsansprüche sind bei Fragen des allgemeinen Persönlichkeitsrechtes im Normalfall zwischen 3.000 € und 5.000 € festzusetzen (Musielak/Voit/Heinrich, 20. Aufl. 2023, ZPO § 3 Rn. 36). Dies muss für den Datenschutz ebenso gelten, wenn ein Datenschutzverstoß so nach außen gewirkt hat, dass das informationelle Selbstbestimmungsrecht verletzt worden ist. In Anbetracht des sich teilweise überschneidenden Inhalts der beiden Unterlassungsanträge, denen im Wesentlichen entsprochen ist, wenn die Beklagte die Nutzung der Telefonnummer der Klägerin für das CIT einstellt, erscheint eine Festsetzung von jeweils 2.500 € und somit insgesamt 5.000 € angemessen (so auch: OLG Stuttgart, Beschluss vom 3. Januar 2023 – 4 AR 4/22 –, juris)

Antrag Ziff. 4: 1.500 €

Hinsichtlich des Auskunftsanspruches besteht eine umfangreiche Rechtsprechung, die überwiegend Streitwerte zwischen 500 € und 5.000 € festsetzt (Leibold, ZD 2022, 18 (37)).

Jedenfalls bei der hier nur noch offenen Teilauskunft und der Betroffenheit eines rein privaten Sachverhalts ohne dahinter stehende Vermögensinteressen kommt daher nur ein Streitwert in der unteren Region dieser Spanne in Betracht.

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 Ulm
Olgastraße 106
89073 Ulm

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.

Richter am Landgericht