Abschrift

Landgericht Berlin

Az.: 14 O 149/22

Im Namen des Volkes

Urteil

In dem Rechtsstreit

[redacted]
- Kläger -

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

gegen

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

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

hat das Landgericht Berlin - Zivilkammer 14 - durch die Vorsitzende Richterin am Landgericht [redacted] als Einzelrichterin aufgrund der mündlichen Verhandlung vom 29.06.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in Höhe von 1000 Euro zu zahlen nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 19.10.2022.

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 er-

folgte, 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,

   personenbezogene Daten der Klägerseite, namentlich Telefonnummer, Facebook-ID, Familiennamen, Vornamen 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.

4. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 800,39 Euro zu zahlen zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 19.10.2022.

5. Im Übrigen wird die Klage abgewiesen.

6. Von den Kosten des Rechtsstreits haben die Beklagte 2/3 und der Kläger 1/3 zu tragen.

7. Das Urteil ist vorläufig vollstreckbar; für den Kläger jedoch hinsichtlich des Tenors zu Ziffer 3 nur gegen Sicherheitsleistung in Höhe von 1000,00 € und im Übrigen gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrags. Dem Kläger wird nachgelassen, die Vollstreckung gegen ihn durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrages abzuwenden.

Tatbestand

Der Kläger macht gegenüber der Beklagten Ansprüche wegen behaupteter Verstöße gegen die sog. Datenschutzgrundverordnung (EU) 2016/679 (im Folgenden: DSGVO) sowie einen Auskunftsanspruch geltend.

Die Beklagte betreibt auf dem Gebiet der Europäischen Union die Social-Media-Plattform „Facebook“, auf die sowohl über die Website www.facebook.com als auch über die sog. „Facebook-Messenger-App“ zugegriffen werden kann. Die Dienste der Beklagten ermöglichen es den Nutzern u.a., persönliche Profile für sich zu erstellen und diese mit anderen Nutzern zu teilen. Auf ihren persönlichen Profilen können die Nutzer Angaben zu verschiedenen Daten zu ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können. Der Kläger ist Nutzer dieser Plattform.

Wird auf der Plattform ein Konto eröffnet, fragt die Beklagte verschiedene personenbezogene Daten von dem künftigen Nutzer ab und weist auf die Datenrichtlinie und die Cookie-Richtlinie hin. Erfragte Pflichtangaben sind Vor- und Nachname, Passwort und entweder die Handynummer oder die E-Mail-Adresse. Der Kläger gab gegenüber der Beklagten seinen Vor- und Nachnamen und seine Telefonnummer an.

Der angegebene Vor- und Nachname, eine von Facebook erstellte Benutzer-ID und das Geschlecht sind als „immer öffentliche Nutzerinformationen“ für jeden Plattformnutzer sichtbar. Andere Daten, die dem Profil hinzugefügt werden können, sind für alle Plattformnutzer sichtbar, wenn dies die jeweiligen persönlichen Profileinstellungen („Zielgruppenauswahl“) vorsehen. Zudem regeln die sog. Suchbarkeitseinstellungen, wer das Profil des Nutzers finden kann. Gibt ein Nutzer seine Telefonnummer an, ist für diese Angabe voreingestellt, dass sie nur von sog. „Freunden“ eingesehen, jedoch von jedem Nutzer mittels des sog. Contact-Import-Tools (im Folgenden: CIT) zur Suche des dazugehörigen Profils genutzt werden kann. Diese Voreinstellungen wurden von dem Kläger bis Februar 2020 nicht abgeändert; seither ist die Nummer des Klägers allerdings auf gesperrt für die Suche vermerkt ("only me").

In der Zeit von Januar 2018 bis September 2019 griffen Dritte unter Verwendung nicht öffentlich einsehbarer, aber aufgrund der Voreinstellung „suchbarer“ Nutzer-Telefonnummern mittels sog. „Scrapings“ die den jeweiligen Nutzer-Profilen zugeordneten, öffentlichen personenbezogenen Daten ab und veröffentlichten diese zusammen mit der Telefonnummer des jeweiligen Nutzers im April 2011 im Internet (im Folgenden: Scraping-Vorfall). Um die Telefonnummer jeweils zu korrelieren, prüften die Dritten dabei mit Hilfe des von der Beklagten zur Verfügung gestellten CITs fiktive Nummern bis ihnen ein zugehöriger Facebook-Nutzer angezeigt wurde (sog. „Telefonnum-

mernaufzählung“).

Mit anwaltlicher E-Mail vom 16.05.2022 forderte der Kläger die Beklagte dazu auf, an den Kläger bis zum 20.6.2022 ein Schmerzensgeld zu zahlen, dem Kläger binnen eines Monats u.a. darüber Auskunft zu erteilen, inwieweit die Beklagte den Kläger betreffende personenbezogene Daten „im Zusammenhang mit dem im April 2021 bekannt gewordenen Datenschutzvorfall“ verarbeite, sowie dazu, den Kläger von vorgerichtlichen Rechtsanwaltskosten (basierend auf einem Streitwert von 8.501,00 €) in Höhe von 887,03 € freizustellen. Wegen der weiteren Einzelheiten der E-Mail wird auf Anlage K1 Bezug genommen.

Mit anwaltlichem Schreiben vom 13.06.2022 teilte die Beklagte u.a. mit, dass sie über keine Kopie der unter Verstoß gegen die Nutzungsbedingungen der Beklagten durch Scraping abgerufenen Rohdaten verfüge, jedoch nach den von ihr vorgenommenen Analysen davon ausgehe, dass die Datenkategorien Nutzer-ID, Vorname, Nachname, Land und die Telefonnummer betroffen seien, wobei das Land nicht notwendigerweise vom Facebook-Nutzerprofil des Klägers abgerufen worden sei, sondern die Scraper diese Information vielmehr anhand der Telefonnummer ermittelt haben dürften. Wegen der weiteren Einzelheiten des Schreibens wird auf Anlage B 16 Bezug genommen.

Der Kläger behauptet, in einer im Darknet für jedermann abrufbaren Datenbank u.a. seine Telefonnummer, seine Facebook-ID und seinen Vor- und Nachnamen gefunden zu haben. Diese Daten seien im Rahmen des Scraping-Vorfalls abgegriffen worden. Er leide seither und noch andauernd unter vermehrten SMS-Nachrichten, die Spam enthielten, und einzelner dubioser Warn- oder Werbeanrufe unter seiner Telefonnummer, während dies vorher gar nicht oder extrem selten vorgekommen sei. Auch sei er in Sorge über einen möglichen weitergehenden Missbrauch seiner Daten. Er meint, die Beklagte habe gegen ihre Pflichten nach der DSGVO verstoßen - u.a. wegen der Verarbeitung personenbezogener Daten des Klägers ohne Rechtsgrundlage nach Art. 6, 7 DSGVO und ausreichende Informationen nach Art. 13, 14 DSGVO, die Zugänglichmachung der Daten für unbefugte Dritte unter Missachtung der Pflichten nach Art. 5 (Grundsätze für die Verarbeitung personenbezogener Daten), Art. 25 Abs. 1, 2 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), Art. 32 (Sicherheit der Verarbeitung) und Art. 34 Abs. 1, Abs. 2 (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person) sowie wegen der Verletzung der Betroffenenrechte des Klägers nach Art. 15, 17 und 18 DSGVO -, weshalb ihm gegen die Beklagte Ansprüche auf Schmerzensgeld, Feststellung der Schadensersatzpflicht für weitere Schäden und auf Unterlassung weiterer unzulässiger Datenverarbeitungen zustünden. Des Weiteren ist der Auffassung, dass ihm gegen die

Beklagte ein bislang nicht erfüllter Anspruch auf Auskunft über die Verarbeitung seiner personenbezogenen Daten zusteht.

Der Kläger beantragt unter Konkretisierung einer zuvor missverständlichen Formulierung seiens ursprünglich angekündigten Antrags zu 2 nunmehr,

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

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

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

a. personenbezogene 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 zu verurteilen, der Klägerseite Auskunft über die Klägerseite betreffende

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

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

Die Beklagte beantragt,

die Klage abzuweisen.

Sie meint, die Klage sei bereits teilweise unzulässig, da die Klageanträge zu Ziffer 1, 2 und 3 nicht hinreichend bestimmt seien und der Kläger kein Feststellungsinteresse habe. Weiter vertritt sie die Auffassung, ihren datenschutzrechtlichen Pflichten auch im Zusammenhang mit dem Scraping-Vorfall vollumfänglich nachgekommen zu sein. Scraping lasse sich nicht vollständig verhindern. Es liege jedoch schon deshalb kein Verstoß gegen die DSGVO vor, da die abgegriffenen Daten öffentlich zugänglich gewesen seien. Der Kläger habe auch einen der Beklagten zurechenbaren ersatzfähigen immateriellen Schaden weder erlitten noch dargelegt. Der Auskunftsanspruch sei bereits durch Erfüllung erloschen.

Wegen des weiteren Sach- und Streitstandes wird auf die ausgetauschten Schriftsätze nebst Anlagen und das Sitzungsprotokoll vom 29.06.2023 verwiesen, was auch die Ergebnisse der persönlichen Anhörung des Klägers durch die Kammer enthält.

Entscheidungsgründe

Die Klage ist zulässig und in dem aus dem Tenor ersichtlichen Umfang begründet.

A.

Die Klage ist zulässig.

1.
Das Landgericht Berlin ist international, sachlich und örtlich zuständig.

Die internationale Zuständigkeit deutscher Gerichte ergibt sich aus Art. 79 Abs. 2 DSGVO. Danach können Klagen gegen einen Verantwortlichen im Sinne der Verordnung bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist. Der Kläger als betroffene Person hat seinen Wohnsitz in Berlin in Deutschland.

Die örtliche Zuständigkeit des Landgerichts Berlin folgt aus Art. 79 Abs. 2 S. 2 DSGVO, da der Kläger seinen Wohnsitz in Berlin und damit im Bezirk des angerufenen Gerichts hat.

2.
Die Klageanträge sind hinreichend bestimmt, vgl. § 253 Abs. 2 Nr. 2 ZPO.

Der Klageantrag zu Ziffer 1 ist hinreichend bestimmt.

Da die Bemessung der Höhe des immateriellen Schadensersatzes in das Ermessen des Gerichts gestellt ist, ist die Stellung eines unbezifferten Zahlungsantrags ausnahmsweise zulässig. Ein Verstoß gegen den in § 253 Abs. 2 Nr. 2 ZPO normierten Bestimmtheitsgrundsatz liegt dann nicht vor, wenn die Bestimmung des Betrages von einer gerichtlichen Schätzung nach § 287 ZPO oder vom billigen Ermessen des Gerichts abhängig ist. Die nötige Bestimmtheit soll hier dadurch erreicht werden, dass der Kläger in der Klagebegründung die Berechnungs- bzw. Schätzgrundlagen umfassend darzulegen und die Größenordnung seiner Vorstellungen anzugeben hat (vgl. Greger in: Zöller, 33. Aufl. 2020, § 253 ZPO Rn. 14 m.w.N.).

Diese Voraussetzungen liegen hier vor. Der Kläger hat sowohl in der Klagebegründung als auch bereits in dem Klageantrag zu 1 einen Mindestbetrag von 1.000,- € angegeben.

Soweit die Beklagte ferner beanstandet, der Antrag zu 1 sei deshalb unbestimmt, weil er auf zwei Lebenssachverhalten fuße und damit zwei Streitgegenstände betreffe, deren Verhältnis zueinander nicht hinreichend bestimmt sei, ist dem nicht zu folgen. Tatsächlich ist hier lediglich ein einheitlicher Lebenssachverhalt zu beurteilen, nämlich derjenige, ob die Beklagte vor dem Scraping

durch Dritte hinreichende Datenschutzvorkehrungen getroffen hatte und danach etwaige Lücken geschlossen hat bzw. ihre Nutzer unzureichend bzw. intransparent informiert hat (ebenso LG Essen, Urteil vom 10. November 2022 – 6 O 111/22, juris Rn. 51; LG Kiel, Urteil vom 12. Januar 2023 – 6 O 154/22, juris Rn. 34; LG Offenburg, Urteil vom 28. Februar 2023 – 2 O 98/22, juris Rn. 31).

Auch der Klageantrag zu Ziffer 2 ist jedenfalls nach der erfolgten Begrenzung auf künftige Schäden hinreichend bestimmt.

Schließlich ist auch der auf Unterlassung gerichtete Klageantrag zu Ziffer 3 hinreichend bestimmt. Bezüglich des Klageantrags zu Ziffer 3a. steht dem – entgegen der von der Beklagten vertretenen Auffassung – die Verwendung des Begriffs „Stand der Technik“ nicht entgegen. Klageanträge sind der Auslegung zugänglich. Dies ist insbesondere dann hinzunehmen, wenn dies zur Gewährleistung eines effektiven Rechtsschutzes (vgl. Art. 19 Abs. 4 GG) erforderlich ist und die Klägerseite ihren Antrag nicht konkreter fasst (LG Kiel, Urteil vom 12. Januar 2023 - 6 O 154/22, juris Rn. 35; LG Gießen, Urteil vom 3. November 2022 - 5 O 195/22, juris Rn. 24).

So liegt es hier. Der auch in der DSGVO verwendete Begriff „Stand der Technik“ (vgl. etwa ErwGr (78), (83), (91), Art. 25, 32 DSGVO) beschreibt einen Zustand, der aufgrund der sich ständig wandelnden Technik aktuell vorherrscht, sich aber gleichermaßen rasch ändern kann. Insoweit ist es dem Kläger unmöglich, den derzeitigen Stand der Technik explizit zu benennen. Je nach dem Stand der Technik sind dabei verschiedene, aufeinander aufbauende Sicherheitsmaßnahmen möglich, die nicht näher konkretisiert werden können. Es bedeutet keinen effektiven Rechtsschutz, müsste bei einer solchen expliziten Benennung erneut geklagt werden, sobald sich der Stand der Technik und mithin die Sicherheitsmaßnahmen ändern (vgl. LG Bielefeld, Urteil vom 19. Dezember 2022 - 8 O 182/22, juris Rn 31; LG Gießen, Urteil vom 3. November 2022 – 5 O 195/22, juris Rn. 24). Dies muss der Kläger nicht hinnehmen.

Auch der Klageantrag zu Ziffer 3b. ist hinreichend bestimmt. Durch die Formulierung „namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann [...].“ kann dem Antrag unter Berücksichtigung der Klagebegründung entnommen werden, wann nach Auffassung des Klägers eine übersichtliche Gestaltung vorliegt, nämlich dann, wenn explizit über die Verwendung der Telefonnummer in den hierauf gerichteten Einstellungsmöglichkeiten belehrt wird (LG Kiel, Urteil vom 12. Januar 2023 - 6 O 154/22, juris Rn. 36).

3.
Des Weiteren liegt auch das für den Antrag zu 2 erforderliche Feststellungsinteresse gemäß § 256 Abs. 1 ZPO vor.

Voraussetzung dafür ist, dass einem subjektiven Recht des Klägers eine gegenwärtige Gefahr der Unsicherheit dadurch droht, dass die Beklagte es ernstlich bestreitet oder sie sich eines Rechts gegen den Kläger berühmt, und wenn das erstrebte Urteil infolge seiner Rechtskraft geeignet ist, diese Gefahr zu beseitigen (*Greger* in: Zöller, Zivilprozessordnung, 34. Auflage 2022, § 256 ZPO Rn. 7). Begehrt die Klägerseite – wie hier – gerade die Feststellung einer Ersatzpflicht für künftige Schadensfolgen aus einer bereits eingetretenen Verletzung eines Rechtsguts, so ist dies bereits dann zu bejahen, wenn die Möglichkeit besteht, dass solche Schäden eintreten (BeckOK ZPO/Bacher, 47. Ed. 1.12.2022, ZPO § 256 Rn. 24, 25). Insoweit ist ein großzügiger Maßstab anzulegen. Ein berechtigtes Interesse ist nur dann zu verneinen, wenn aus Sicht der Klägerseite bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (BGH, Beschluss vom 9. Januar 2007 – VI ZR 133/06, juris Rn. 5; BGH, Urteil vom 20. März 2001 – VI ZR 325/99, juris Rn. 11). Davon kann hier jdeoch nicht die Rede sein.

B.
Die Klage ist in dem aus dem Tenor ersichtlichen Umfang begründet.

I.

Dem Kläger steht gegen die Beklagte ein Anspruch auf Schadensersatz in Form eines Schmerzensgeldes in Höhe von 1000,00 € zu.

1.
Der Anspruch auf Schadensersatz beruht auf Art. 82 Abs. 1, 2 S. 1 DSGVO.

Art. 82 Abs. 1 DSGVO bestimmt, dass jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadenersatz gegen den Verantwortlichen hat. Abs. 2 S. 1 konkretisiert dies dahin, dass jeder an einer Verarbeitung beteiligte Verantwortliche für den Schaden haftet, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.

a.

Die Beklagte hat die personenbezogenen Daten des Klägers nicht in einer den Vorgaben der DS-GVO entsprechenden Weise verarbeitet.

aa.
Für die erfolgte Verarbeitung fehlt es bereits an einer tauglichen Rechtsgrundlage.

Gem. Art. 6 DSGVO ist eine Verarbeitung nur bei Vorliegen mindestens einer der dort genannten Rechtsgrundlagen rechtmäßig. „Verarbeitung“ bezeichnet dabei gem. Art. 4 Nr. 2 DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Vorliegend ordnete die Beklagte auf Anfrage unbekannter Dritte über das von ihr eingesetzte CIT die von diesen automatisiert abgefragte Telefonnummer dem Kläger und damit dessen weiteren bei der Beklagten gespeicherten (öffentlich zugänglichen) personenbezogenen Daten zu. Bei der Telefonnummer handelte es sich bis zu diesem Zeitpunkt um kein öffentlich zugängliches Datum. Erst durch die Abfrage bei der Beklagten konnte die Telefonnummer als dem Kläger gehörend identifiziert werden, so dass aus einer mehrstelligen Zahl ohne jeden nachvollziehbaren Bezug zu einer Person ein personenbezogenes Datum wurde. Diese Offenlegung durch Bereitstellung von personenbezogenen Daten bedarf als Verarbeitung einer Rechtsgrundlage nach Art. 6 DSGVO. Das Vorliegen einer solchen Rechtsgrundlage hat die Beklagte nicht dargetan.

Die Beklagte hat nicht dargelegt, dass der Kläger in die Übermittlung seiner Daten gem. Art. 6 Abs. 1 lit. a DSGVO wirksam eingewilligt hat. Gemäß Erwägungsgrund (32) der DSGVO können Stillschweigen, standardmäßig angekreuzte Kästchen oder Untätigkeit nicht als Einwilligung gewertet werden. Vielmehr sind „Opt-out-Einwilligungen“ ausgeschlossen (Gola/Heckmann/Schulz, 3. Aufl. 2022, DSGVO Art. 7 Rn. 42). Soll die Einwilligung mehrere Zwecke legitimieren, müssen sämtliche Zwecke in der Erklärung aufgeführt werden (Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 7 Rn. 45). Vorliegend war die Suchbarkeit der Telefonnummer durch jeden Nutzer von der Beklagten voreingestellt. Der Kläger hat eine diesbezügliche Einwilligung nicht erteilt.

Anders als die Beklagte meint, war die Übermittlung auch nicht gem. Art. 6 Abs. 1 lit. b DSGVO

zur Erfüllung des zwischen den Parteien geschlossenen Nutzungsvertrags erforderlich.

Die Beklagte hat schon nicht dargelegt, dass zwischen den Parteien bei Vertragsschluss, d.h. während des Registrierungsprozesses, ausdrücklich oder konkludent die Nutzung der Telefonnummer des Klägers zur Suche vereinbart wurde. Vielmehr war die Suchbarkeit mittels Telefonnummer durch jeden Nutzer voreingestellt, ohne dass dies für die Nutzung der Hauptfunktionen der Plattform erforderlich gewesen wäre. Eine hierauf gerichtete Willenserklärung des Klägers hat die Beklagte nicht dargelegt. Auch mag die Suchbarkeit von Nutzerprofilen mittels Telefonnummer im Einzelnen je nach Geschmack des Nutzers für die Nutzung der Facebook-Plattform nützlich und behilflich sein. Erforderlich für die Nutzung schlechthin ist sie aber nicht. Diesbezügliche Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten müssen sich auf das absolut Notwendige beschränken. Die Daten sind für eine Nutzung der Facebook-Plattform durch Dritte bzw. für den Betrieb derselben durch die Beklagte nicht unabdingbar (anders für ein Ärztebewertungsportal: BGH, Urteil vom 13.12.2022 – VI ZR 60/21 Rn. 21). Das zeigt sich auch daran, dass sämtliche Voreinstellungen, um die es hier geht, ohne weiteres abgewählt werden können, ohne dass dies ersichtlich der weiteren Vertragsdurchführung entgegensteht (so ausdrücklich KG, Urteil vom 20.12.2019 – 5 U 9/18, BeckRS 2019, 35233 Rn. 39). Daher kann sich die Beklagte nicht darauf zurückziehen, dass der Zweck der Facebook-Plattform gerade darin bestehe, es Menschen zu ermöglichen, sich mit Freunden, Familie und Gemeinschaften zu verbinden und dass die Funktionen gezielt so konzipiert worden seien, dass sie den Nutzern helfen, andere zu finden, sich mit ihnen zu verbinden und mit ihnen in Kontakt zu treten. Gerade das widerspricht den Anforderungen der DSGVO. Die Beklagte darf nicht durch die Definition ihres Leistungsangebots den Umfang der zulässigen Datenverarbeitung unter Hintanstellung der Nutzerinteressen allein an ihrem Interesse an der Vermarktung eines durch die Internetnutzung innerhalb und außerhalb von Facebook generierten Bestands personenbezogener Daten seiner Nutzer ausrichten und über das für die Benutzung des sozialen Netzwerkes erforderliche Maß ausweiten (so BGH, Beschluss vom 23.06.2020 – KVR 69/19 Rn. 110). Für die Durchführung des Schuldverhältnisses ist es z.B. für den jeweiligen Nutzer nicht erforderlich, dass Name, Profilbild und Titelbild anderen Nutzern helfen, andere zu finden, auch wenn das hilfreich und von vielen gewünscht sein mag. Würde allein die Nutzung von Facebook unter Beibehaltung der von dem Verantwortlichen gewählten Voreinstellungen zur Annahme einer auf die Nutzung gerade dieser voreingestellten Funktionen gerichteten vertraglichen Vereinbarung führen, würde dies zudem die Anforderungen der DSGVO - insbesondere im Hinblick auf die Wirksamkeit einer Einwilligung - aushöhlen.

Es ist auch nicht ersichtlich, dass die Offenlegung der Telefonnummer zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich war (Art. 6 Abs. 1 Satz 1 lit. f DS-GVO).

bb.
Die Beklagte hat des Weiteren gegen ihre datenschutzrechtlichen Aufklärungs- und Schutzpflichten verstoßen.

Der Beklagten fällt bereits ein Verstoß gegen die Transparenzpflichten aus Art. 5 Abs. 1 lit. a, 13, 14 DSGVO zur Last.

Nach dem Grundsatz des Art. 5 Abs. 1 lit. a DSGVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Das Erfordernis der Transparenz führt Art. 13 DSGVO in Form von Informations- und Aufklärungspflichten fort. Die Aufklärung über die Zwecke der Verarbeitung muss insbesondere für den Nutzer klar verständlich und nachvollziehbar sein. Ähnliche Vorgaben sieht auch Art. 14 DSGVO für den Fall vor, dass der Verantwortliche die Daten nicht direkt bei der betroffenen Person erhebt. Auch Art. 12 DSGVO sieht eine Information in präziser, transparenter und leicht zugänglicher Form vor (LG Kiel, Urteil vom 12. Januar 2023 – 6 O 154/22, juris Rn. 45)

Diesem Maßstab wurde die Beklagte vorliegend nicht vollumfänglich gerecht.

Die Beklagte hat den Kläger zum Zeitpunkt der Datenerhebung seiner Telefonnummer nicht ausreichend über die Zwecke der Verarbeitung dieser Nummer aufgeklärt. Nach Art. 13 Abs. 1 lit. c DSGVO sind die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, zum Zeitpunkt der Erhebung der Daten mitzuteilen. Dem hat die Beklagte zumindest hinsichtlich der Verwendung der Telefonnummer für das von ihr verwendete CIT nicht genügt (so auch LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 54 - 70, juris). Mit diesem ermöglicht die Beklagte einem Nutzer z.B. einen Abgleich der in seinem Smartphone gespeicherten Kontakte mit auf Facebook registrierten Nutzerprofilen, die ihr Profil mit einer Telefonnummer verknüpft haben. So können diese Kontakte auf der Facebook-Plattform gefunden, und es kann mit ihnen in Verbindung getreten werden. Aus den vorgelegten Unterlagen ist nicht ersichtlich, dass insoweit durch die Beklagte eine geeignete Aufklärung erfolgt wäre. Derlei vermag die Beklagte insbesondere im Rahmen der Klageerwiderung vom 07.10.2022 nicht aufzuzeigen. Vielmehr wird durch die Information „*Möglicherweise verwenden wir deine Mobilnummer für diese Zwecke: … Um dir*

Personen, die du kennen könntest, vorzuschlagen, damit du dich mit ihnen auf Facebook verbinden kannst“ gerade ein gegenteiliger Eindruck erweckt: Es wird nicht darüber informiert, dass andere den Kläger als Nutzer finden können, sondern darüber, dass dem Kläger seine Telefonnummer nützlich sein kann, um andere Facebook-Nutzer zu finden. Das eine mag zwar mit dem anderen unmittelbar zusammenhängen, indes gestaltet sich die Information der Beklagten selektiv und damit unvollständig. Das wird auch nicht durch den anschließenden Hinweis, dass man kontrollieren könne, wer die eigene Telefonnummer sehen (nicht suchen) könne, geheilt, zumal auch in der vorgelegten „Datenrichtlinie“ in der Rubrik „*Wie werden diese Informationen geteilt?*“ hierauf in keiner Weise hingewiesen wird. Vor diesem Hintergrund ist es auch nicht ausreichend, dass die Beklagte über die Möglichkeiten der Anpassung ihrer Suchbarkeits-Einstellungen und Zielgruppenauswahl informiert. Die Voreinstellung, die die Beklagten hinsichtlich einzelner Aspekte mit „öffentlich“ einräumt, läuft den Erfordernissen des Art. 25 Abs. 2 DSGVO evident zuwider. Auch ist nicht erheblich, wie die Beklagten einen „Hilfebereich“ ausgestaltet, da diesen i.d.R. nur derjenige Nutzer anschauen wird, der die Notwendigkeit einer Änderung für sich wahrgenommen hat. Das ist bei einem Nutzer, der die Anmeldeprozedur mit vorgegebenen Einstellungen durchläuft, nicht notwendigerweise der Fall. Ein Verstoß gegen Art. 13 DSGVO kann – entgegen der Annahme der Beklagten – auch ohne weiteres einen Schadensersatzanspruch nach Art. 82 DSGVO nach sich ziehen (vgl. nur Schmidt-Wudy in BeckOK-Datenschutzrecht, Stand: 01.11.2022 DSGVO Art. 13 Rn. 18; Franck in Gola/Heckmann, DSGVO – BDSG, 3. Aufl. DSGVO Art. 13 Rn. 64; aA LG Essen, Urteil vom 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818).

Die Beklagte hat überdies gegen die Verpflichtung zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen aus Art. 25 DSGVO verstoßen.

Art. 25 Abs. 1 DSGVO verpflichtet den Verantwortlichen bereits bei der Entwicklung von Produkten, Diensten und Anwendungen sicherzustellen, dass die Anforderungen der DSGVO erfüllt werden („Privacy by Design"). Abs. 2 konkretisiert diese allgemeine Verpflichtung und verlangt, vorhandene Einstellungsmöglichkeiten standardmäßig auf die „datenschutzfreundlichsten" Voreinstellungen („Privacy by default") zu setzen. „Datenschutz durch Voreinstellungen" soll insbesondere diejenigen Nutzer schützen, welche die datenschutztechnischen Implikationen der Verarbeitungsvorgänge entweder nicht zu erfassen in der Lage sind oder sich darüber keine Gedanken machen und sich deshalb auch nicht dazu veranlasst sehen, aus eigenem Antrieb datenschutzfreundliche Einstellungen vorzunehmen, obwohl der Verantwortliche ihnen diese Möglichkeit prinzipiell eröffnet. Die Nutzer sollen keine Änderungen an den Einstellungen vornehmen müssen, um eine möglichst „datensparsame" Verarbeitung zu erreichen. Vielmehr soll umgekehrt jede Abwei-

chung von den datenminimierenden Voreinstellungen erst durch ein aktives „Eingreifen“ der Nutzer möglich werden. Die Regelung soll die Verfügungshoheit der Nutzer über ihre Daten sicherstellen und sie vor einer unbewussten Datenerhebung schützen. 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, DSGVO – BDSG 3. Aufl. DSGVO Art. 25 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, DSGVO - BDSG 3. Aufl. DSGVO Art. 25 Rn. 26).Dies wurde durch die Beklagte nicht gewährleistet.

Der Verstoß gegen Art. 25 Abs. 2 DSGVO ist auch dazu geeignet, einen Ersatzanspruch nach Art. 82 DSGVO auszulösen, da aus der Verletzung der sich aus Art. 25 DSGVO ergebenden Pflichten eine Erhöhung der Gefahr eines Schadens resultieren kann (vgl. Mantz in Sydow/Marsch, DSGVO | BDSG, 3. Aufl. DSGVO Art. 25 Rn. 77; Martini in Paal/Pauly, DSGVO – BDSG 3. Aufl. DSGVO Art. 25 Rn. 6; aA Nolte/Werkmeister in Gola/Heckmann, DSGVO – BDSG, 3. Aufl. DSGVO Art. 25 Rn. 3, 34). Diese Gefahr hat sich vorliegend realisiert. Bei einer mit Art. 25 Abs. 2 DSGVO konformen Voreinstellung wäre den unbekannten Dritten ein Abgreifen der Telefonnummer des Klägers nicht ohne Weiteres möglich gewesen.

Die Beklagte hat auch gegen ihre Pflichten aus Art. 32, 24 DSGVO zur Ergreifung geeigneter technischer und organisatorischer Schutzmaßnahmen verstoßen.

Art. 32 Abs. 1 DSGVO verpflichtet den Verantwortlichen zwar 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 (Gola/Heckmann/Piltz, 3. Aufl. 2022, DSGVO Art. 32 Rn. 11; vgl. auch Spindler/Schuster/Laue, 4. Aufl. 2019, DSGVO Art. 32 Rn. 3). Zur Bestimmung des angemessenen Schutzniveaus sind gem. Art. 32 Abs. 2 DSGVO jedoch 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 (Spindler/Schuster/Laue, 4. Aufl. 2019, DSGVO Art. 32 Rn. 5). Ausweislich des Erwägungsgrunds (76) zur DSGVO sollten die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten des 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.

Dieser umfassenden Risikobestimmung anhand der genannten Kriterien ist die Beklagte zumindest nicht ausreichend nachgekommen (so auch LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 84 - 85, juris). 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 DSGVO. Das CIT konnte und wurde zweckwidrig nicht zum Auffinden von persönlichen Kontakten, sondern entgegen der Nutzungsbedingungen der Beklagten zu Missbrauchszwecken genutzt. Es wird Dritten eine Zuordnung von Telefonnummer zum Facebook-Profil, bei dem diese angegeben wurde, ermöglicht. Dementsprechend wird in Erfahrung gebracht, welche Person hinter der Telefonnummer steht. Hierbei können durch den Rückgriff auf das Facebook-Profil gleichzeitig weitere Informationen über die Person eingeholt werden. Dies birgt für die Nutzer das Risiko von gezielten Phishing-Attacken, Identitätsdiebstahl und weiteren 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 auch daraus, dass das CIT-Verfahren keine reine Erhebung oder Speicherung von Daten durch die Beklagten 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 Scraping-Vorfall aufzeigt, besonders hoch. „Scraping“ ist weit verbreitet und entsprechende Versuche bei dem weltweit genutzten sozialen Netzwerk der Beklagten auch aus einer ex-ante-Sicht zu erwarten gewesen. 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. Des Weiteren ist die behauptete teilweise Einschränkung des CIT auch nach dem Beklagtenvorbringen erst nach dem streitgegenständlichen Vorfall eingeführt worden. Auch die Beschäftigung eines Teams von Datenwissenschaftlern, -analysten und Softwareingenieuren zur Bekämpfung von Scraping, Übertragungsbeschränkungen sowie CAPTCHA-Abfragen genügen den Anforderungen des Art. 32 DSGVO im vorliegenden Fall allein nicht. Die Beklagte legt diesbezüglich bereits nicht dar, wie es bei den - aus ihrer Sicht im hiesigen Verfahren ausreichenden - Sicherheitsmaßnahmen dennoch zum streitgegenständlichen Scraping-Vorfall kommen konnte. Die genannten Maßnahmen mögen den Schutz von personenbezogenen Daten fördern. Aufgrund des hohen Risikopotenzials, das von einem Missbrauch des CIT ausgeht, waren jedoch weitergehende Maßnahmen für ein angemessenes Schutzniveau erforderlich. So werden z.B. bereits bei geringeren Risiken im Umgang mit personenbezogenen Daten etwa CAPTCHA-Abfragen eingesetzt. Die Arbeit des „External-Data-Misuse-Teams“ der Beklagten (im Folgenden: EDM-Team) entfaltet des Weiteren ausweislich des Vorbringens der Beklagten in der Regel erst während eines bereits begonnen Scraping-Prozesses ihre Wirkung, so dass Scraper in diesem Zeitpunkt bereits Datensätze erlangt haben. Außerdem ist es Scrapern möglich, Übertragungsbeschränkungen zu umgehen. Daher wären weitergehende Maßnahmen notwendig gewesen. Diese hätten beispielsweise so ausgestaltet werden können, dass weitergehende Informationen neben der Telefonnummer für die Nutzung des CIT anzugeben sind. Es kann ein Missbrauch des CIT in Form von Datenscraping dann zumindest erschwert werden, so z.B. durch die weitere Angabe eines Vornamens, der sich neben der Telefonnummer ebenfalls hochladen ließe. So würden weitere Variablen hinzutreten, die auf eine den Nutzungsbedingungen entsprechende Nutzung des CIT hindeuten. Datenscraper hingegen werden vor das Problem gestellt, das neben Variablen in Form von Zahlen auch Variablen in Form von Worten hinzutreten. Dies erschwert ein automatisiertes Verfahren. Zudem wäre ein höherer Datenverkehr erforderlich, der ggf. den bereits behaupteten Maßnahmen der Übertragungsbeschränkungen und der Arbeit des EDM-Teams einen größeren Nutzen verleiht. Dies würde auch nicht dem von der Beklagten verfolgten Zweck zuwiderlaufen. Denn laut der Beklagten sei es Hauptzweck der Plattform, andere Nutzer zu finden und mit diesen in Kontakt zu treten. Das CIT ermöglicht dementsprechend Nut-

zer ihre Kontakte ihrer Mobilgeräte auf Facebook hochzuladen und anhand der Telefonnummern die Nutzerprofile ihrer Kontakte zu finden. Weitergehende Angaben laufen diesen Absichten nicht zuwider, zumal diese ggf. ebenfalls über das CIT automatisch über die Kontaktliste des Mobilgeräts des Nutzers in Erfahrung gebracht werden könnte. Diese oder andere Schutzmaßnahmen, wie die klägerseits angeführten Begrenzungen der abgleichbaren Rufnummern oder Nutzung nur für Freunde von Freunden, implementierte die Beklagte jedoch vor oder während des streitgegenständlichen Datenscrapings nicht. Erst im Nachgang implementierte die Beklagte eine vergleichbare Sicherheitsmaßnahme, der sog. „Social Connection Check“. Die Beklagte nahm damit 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. Überdies kann sich die Beklagte ihren Schutzpflichten nicht allein mit der Begründung entziehen, „Scraping“ lasse sich nicht vollständig verhindern. Wenn die Beklagte nicht in der Lage ist, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Schutzniveau der verarbeiteten personenbezogenen Daten sicherzustellen, und dies dazu führt, dass massenhaft personenbezogene Daten abgegriffen und bei der Beklagten hinterlegten, grundsätzlich nicht öffentlichen Telefonnummer zugeordnet werden können, kann sie eine entsprechende Funktion schlicht nicht anbieten.

Nach alledem liegt ein Verstoß gegen Art. 32, 24, 5 Abs. 1 f) DSGVO vor, der bei Vorliegen der übrigen Anspruchsvoraussetzungen einen Anspruch nach Art. 82 DSGVO zur Folge hat (Kühling/Buchner/Jandt, 3. Aufl. 2020, DSGVO Art. 32 Rn. 40a; Sydow/Marsch DSGVO/BDSG/Mantz, 3. Aufl. 2022, DSGVO Art. 32 Rn. 31).

Es kann dahinstehen, ob die Beklagte auch gegen ihre Pflichten aus Art. 33 (Meldung an die Aufsichtsbehörde), Art. 34 (Information des Klägers) und Art. 15 (Auskunftserteilung) DSGVO verstoßen hat.

Zum einen folgt aus diesen Verstößen letztlich kein weitergehender Unrechtsgehalt als aus den bereits dargelegten Verstößen (vgl. hierzu auch LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 73, juris). Zum anderen hätten auch eine ordnungsgemäße Meldung der Verstöße an die Aufsichtsbehörde nach Art. 33 DSGVO, eine Benachrichtigung des Klägers über die Verstöße nach Art. 34 DSGVO und die Erteilung einer ordnungsgemäßen Auskunft über die verarbeiteten Daten nach Art. 15 DSGVO den beim Kläger aufgrund des Scraping-Vorfalls verursachten Schaden nicht mehr mindern können. Etwaige Verstöße sind für den eingetretenen Schaden mithin nicht kausal.

b.
Die Beklagte kann sich mit Blick auf den Scraping-Vorfall nicht nach Art. 82 Abs. 3 DSGVO entlasten.

Insofern kann dahinstehen, ob überhaupt ein Verschulden erforderlich ist bzw. ob die Haftung nach Art. 82 DSGVO zur Sicherstellung eines möglichst wirksamen Schadensersatzes als Gefährdungshaftung gestaltet ist (so z.B. Geissler/Ströbel, NJW 2019, 3414) (LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 74 - 75, juris).

Der Beklagten ist bereits nach ihrem eigenen Vorbringen eine Entlastung, hinsichtlich derer ihr die Darlegungs- und Beweislast obliegt (vgl. nur Nemitz in Ehmann/Selmayr, DSGVO 2. Aufl. Art. 82 Rn. 19), nicht gelungen.

Sie bringt vor, dass die Daten-Scraper Verfahren eingesetzt hätten, um in großem Umfang Daten mit automatisierten Tools und Methoden zu sammeln, was nach den Nutzungsbedingungen von Facebook untersagt gewesen sei. Damit räumt sie die technische Möglichkeit des Abgreifens von Daten durch die von ihr gewählte Architektur der Facebook-Plattform ein. Wenn aber der Beklagten bewusst ist, dass Daten-Scraper bestimmte Funktionen missbrauchen können, dann wäre es an der Beklagten gewesen, gerade das zu unterbinden - notfalls auch durch Deaktivierung des CIT. Auch wenn das dem eigenen Verständnis der Facebook-Plattform zuwiderlaufen mag - dem Interesse der Nutzer an der Wahrung ihrer datenschutzrechtlichen Belange entspräche das indes sehr wohl.

Die Beklagte trägt überdies nichts Konkretes dazu vor, was sie gegen die ihr bekannte Möglichkeit unternommen haben will. Sie bringt nur – letztlich recht pauschal – vor, sie habe Maßnahmen getroffen, um das Risiko von Scraping zu unterbinden, und entwickle ihre eigenen Maßnahmen zur Bekämpfung von Scraping kontinuierlich und als Reaktion auf die sich ständig ändernden Techniken und Strategien weiter. Ebenso wenig konkret und nachvollziehbar ist die pauschale Feststellung der Beklagten, in der Regel würden lediglich die Methoden, mit denen auf die maßgeblichen Funktionen zugegriffen werden könne, beschränkt, um zu verhindern, dass die gesamte zugrundeliegende Funktion beseitigt werde. Anderes ergibt sich auch nicht aus der ergänzenden Darstellung der Klageerwiderung und des Schriftsatzes vom 25.01.2023, vielmehr gesteht die Beklagte zu, dass die zutreffende Reaktion zur Verhinderung des hier stattgefundenen Daten-Scraping gewesen sei, das Verknüpfen von Telefonnummern mit bestimmten Facebook-Nut-

zern durch das CIT zu verhindern. Das hatte sie – wie sie im Schriftsatz vom 25.01.2023 mitteilt – nicht gemacht, weil zunächst Scraping-Aktivitäten über das CIT nicht festgestellt worden seien. Das nach dem Vorbringen der Beklagten erfolgte Absenken der Übertragungsbeschränkungen war offenkundig unzureichend. Soweit die Beklagte darauf abstellt, es handele sich dabei um eine legitime, nützliche Nutzerfunktion, mag dies zwar nützlich und hilfreich für einzelne Nutzer sein, erforderlich ist es indes nicht.

Auch der Hinweis, dass die Telefonnummern von den Daten-Scrapern „bereitgestellt“ worden sei, entlastet die Beklagte nicht. Wie bereits dargelegt, wurden die fiktiven Telefonnummern erst durch die Zuordnung über die Suchfunktion der Beklagten zu einzelnen Nutzerprofilen zu personenbezogenen Daten. Es wäre an der Beklagten gewesen, ein solch automatisiertes Verfahren zu verhindern.

c.
Dem Kläger ist im Zusammenhang mit dem Scraping-Vorfall auch ein nach Art. 82 DSGVO ersatzfähiger – immaterieller – Schaden entstanden, für den die Verstöße der Beklagten gegen die DSGVO kausal waren. Nach richterlichem Ermessen gem. § 287 Abs. 1 ZPO ist dem Kläger für die erlittenen immateriellen Schäden ein Schmerzensgeld in Höhe von 1000 Euro zuzusprechen (§ 287 Abs. 1 Satz 1 ZPO, vgl. BAG Urteil vom 05.05.2022 – 2 AZR 363/21, BeckRS 2022, 20229 Rn. 14).

Zunächst ist die Kammer überzeugt davon, dass der Kläger vom Scraping-Vorfall betroffen ist. Soweit die Beklagte bestritten hat, dass sich der Datensatz des Klägers, bestehend aus der Facebook-ID, Vor- und Nachname und Mobilnummer im Darknet finden lässt, hat die Beklagte eine Verifizierung unterlassen, so dass ihr Bestreiten schon unbeachtlich sein dürfte. Im Übrigen hat sie vorprozessual selbst eingeräumt, dass der Kläger nach ihren Erkenntnissen vom Scraping betroffen ist.

Die Kammer geht auch davon aus, dass die Daten des Klägers genutzt werden, um ihm ungefragt und ungewollt SMS zu übersenden und ihn mit fragwürdigen Anrufen zu konfrontieren. Zwar ist der Beklagten zuzugestehen, dass nicht für jede vorgetragenen Belästigungen durch Anrufe und SMSen nicht notwendigerweise der Scraping-Vorfall ursächlich gewesen sein muss. Da die Datenerlangung mittels Scraping jedoch gerade auf Erlangung derartiger Kontaktmöglichkeiten zum Zweck deren Nutzung zielt und der Kläger bei seiner Anhörung überzeugend und nachvollziehbar zum Ausdruck gebracht, dass er seitdem spürbar und in einem störenden Ausmaß be-

troffen ist und vorher nicht oder nur ganz vereinzelt, reicht die Zunahme der Belästigung zur Überzeugung des Gerichts aus, um einen Zusammenhang mit dem Scraping-Vorfall zu bejahen.

Es kann dahinstehen, ob ein Mitverschulden des Geschädigten im Rahmen von Art. 82 DSGVO zu berücksichtigen ist (vgl. dazu nur Bergt in Kühling/Buchner, DSGVO - BDSG 3. Aufl. DSGVO Art. 82 Rn. 59 mit Fn. 181). Ein etwaiges Mitverschulden des Klägers (§ 254 BGB), weil er die Datenschutzeinstellungen seines Facebook-Profils nicht geändert und den Zugriff durch die Daten-Scraper mit ermöglicht hat, tritt jedenfalls hinter den Verstößen der Beklagten zurück. Die Beklagte zielt mit ihren Voreinstellungen gerade darauf ab, dass Nutzer diese Einstellungen zur Förderung der Netzwerkaktivitäten beibehalten. Sie kann sich daher nicht, wenn sich die Gefahren, die sich durch ihr verordnungswidriges Verhalten ergeben, realisiert haben, darauf berufen, es sei am Kläger gewesen, dies im Sinne des Schutzes seiner personenbezogenen Daten zu korrigieren (vgl. auch OLG Koblenz, Urteil vom 18.05.2022 – 5 U 2141/21, BeckRS 2022, 11126 Rn. 78; Frenzel in Paal/Pauly, DSGVO – BDSG 3. Aufl. DSGVO Art. 82 Rn. 19). Das gilt umso mehr für das CIT, über dessen Funktionsweise und die damit verbundenen Gefahren seitens der Beklagten nicht hinreichend aufgeklärt wird.

Das Gericht hält ein Schmerzensgeld in Höhe von 1000 € für angemessen, aber auch ausreichend, um sowohl dessen Ausgleichs- und Genugtuungsfunktion als auch dessen generalpräventiver Funktion des immateriellen Schadensersatzes hinreichend Rechnung zu tragen.

Zum einen ist – mit Blick auf den generalpräventiven Auftrag des Art. 82 DSGVO (vgl. Gola/Piltz in Gola/Heckmann, DSGVO – BDSG, 3. Aufl. DSGVO Art. 82 Rn. 5) – insoweit zu berücksichtigen, dass die Art und Weise der Datenerhebung durch die Beklagte systematisch gegen die Vorgaben der DSGVO verstößt, um damit Sinn und Zweck der von ihr betriebenen Facebook-Plattform zu fördern. Andererseits ist auch der Umfang der Daten des Klägers, die abgegriffen worden sind, zu berücksichtigen. Die aufgrund des Scraping-Vorfalls erlangte Telefonnummer des Klägers ermöglicht, dass der Kläger ungewollt kontaktiert werden kann. Weitergehende Daten, die eine Kontaktaufnahme ermöglichen könnten, wurden – nach derzeitigem Kenntnisstand – jedoch nicht von Dritten gescrapt. Daher ist der mögliche Schaden, auch wenn die Gefahr eines Identitätsdiebstahls nicht ausgeschlossen werden kann, für den Kläger letztlich noch überschaubar.

2.

Der Zinsausspruch beruht auf §§ 291, 288 Abs. 1 BGB.

II.

Dem Kläger steht gegenüber der Beklagten auch der aus dem Tenor zu Ziffer 2 ersichtliche Anspruch auf Feststellung zu.

Nachdem dem Kläger ein Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO zusteht, ist auch auf den Klageantrag zu Ziffer 2 zu erkennen. Es ist nicht ausgeschlossen, dass der Kläger künftig infolge der Verstöße der Beklagten gegen die DSGVO – auch – materielle Schäden erleidet (so auch LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 110, juris).

III.

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

Die DSGVO sieht für den vorbeugenden Unterlassungsschutz grundsätzlich keine gesonderte Anspruchsgrundlage vor. Um Schutzlücken zu vermeiden, ergibt sich ein solche - auch mit Blick auf die Vorgaben des Art. 79 DSGVO - entweder über einen Rückgriff auf §§ 823 Abs. 2, 1004 BGB analog (vgl. nur OLG München, Urteil vom 19.01.2021 – 18 U 7243/19, juris Rn. 62), oder aber aufgrund der erfolgten unrechtmäßigen Datenverarbeitung aus Art. 17 Abs. 1 lit. d DSGVO als Minus zu dem dort normierten Löschungsanspruch (vgl. BGH, Urteil vom 13.12.2022 – VI ZR 60/21 Rn. 10; zum Ganzen auch: OLG Frankfurt, Urteil vom 14.04.2022 – 3 U 21/20, GRUR-RS 2022, 10537).

Soweit die Beklagte gegen die DSGVO verstoßen hat, steht dem Kläger gegen die Beklagte ein auf diese Verstöße bezogener Anspruch auf Beseitigung und künftige Unterlassung zu.

Der Kläger kann danach verlangen, dass die Beklagte es unterlässt, seine Telefonnummer, seine Facebook-ID, seines Landes und seinen Vor- und Nachnamen unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen.

Soweit der Kläger mit dem Klageantrag zu Ziffer 3a. im Übrigen auch Unterlassung hinsichtlich seines Bundeslandes, seines Geschlechts, seiner Stadt und seines Beziehungsstatus begehrt, hat der Kläger die Voraussetzungen eines entsprechenden Anspruchs dagegen schon nicht schlüssig dargelegt. Er hat nicht vorgetragen, gegenüber der Beklagten entsprechende Angaben auf seinem Nutzerprofil gemacht zu haben.

Auch soweit der Kläger von der Beklagten mit dem Klageantrag zu Ziffer 3b. verlangt, es zu unterlassen, „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," hat er die Voraussetzungen eines entsprechenden Anspruchs nicht schlüssig dargelegt. Durch die vom Kläger vorgenommene Änderung der Suchbarkeits-Einstellung im Februar 2020 hat sich die Sachlage grundsätzlich verändert. Insbesondere ist auch nicht ersichtlich, dass im Rahmen des Scraping-Vorfalls auch personenbezogene Daten von solchen Personen abgegriffen wurden, bei denen die Suchbarkeit ihrer Telefonnummer von vornherein deaktiviert war. Weitere Verstöße sind daher nicht mehr zu befürchten.

Die Ordnungsmittelandrohung folgt aus § 890 ZPO.

IV.

Dem Kläger steht gegen die Beklagte gem. Art. 15 DSGVO kein Auskunftsanspruch gemäß dem Klageantrag zu Ziffer 4 (mehr) zu.

Nach Art. 15 DSGVO kann die betroffene Person zwar Auskunft über personenbezogenen Daten verlangen, wenn der Verantwortliche sie betreffende personenbezogene Daten verarbeitet hat. Art. 15 Abs. 1 Hs. 1, 2 DSGVO enthält zunächst einen Anspruch der betroffenen Person gegen den Verantwortlichen, ihm zu bestätigen, ob ihn betreffende personenbezogene Daten verarbeitet werden. Verarbeitet der Verantwortliche personenbezogene Daten der betroffenen Person, so hat die betroffene Person gem. Art. 15 Abs. 1 Hs. 1, 2 DSGVO ein Recht auf Auskunft über diese personenbezogenen Daten (vgl. BGH, Urteil vom 15.06.2021 - VI ZR 576/19 = NJW 2021, 1381). Dem Kläger steht nach dieser Vorschrift daher grundsätzlich ein Auskunftsanspruch über die bei der Beklagten als Verantwortlicher im Sinne des Art. 4 Nr. 7 Hs. 1 DSGVO verarbeiteten ihn betreffenden personenbezogenen Daten zu. Dieser Anspruch ist jedoch gemäß § 362 Abs. 1 BGB durch Erfüllung untergegangen mit dem vorprozessualen Schreiben der Beklagten vom 13.6.2022 und auch im Zuge des Prozesses. Soweit der Kläger mit dem Klageantrag zu Ziffer 4 weitergehende Auskunft insbesondere zu den Nutzern des CITs verlangt, kann nicht angenommen werden, dass die Beklagte über diese Informationen verfügt oder sie beschaffen kann.

V.

Dem Kläger gegen die Beklagte gem. §§ 286 Abs. 1, 2 Nr. 3, 280 Abs. 1, 2 B ein Erstattungsanspruch hinsichtlich der für die anwaltliche E-Mail vom 16.5.2022 vorgerichtlich entstandenen

Rechtsanwaltskosten in Höhe von (nur) 800,39 Euro ausgehend von einem vorgerichtlich berechtigten Streitwert bis 8000 Euro unter Berücksichtigung des damals noch weitgehend berechtigten Auskunftsverlangens zu. Diese Kosten waren zur Geltendmachung des Schmerzensgeldanspruchs und der weiteren Ansprüche erforderlich und angemessen. Die weiteregehende Klage war abzuweisen.

Der Zinsausspruch beruht auf §§ 291, 288 Abs. 1 BGB.

C.

Die Kostenentscheidung beruht auf § 92 Abs. 1 S. 1 ZPO. Der Kläger obsiegt hinsichtlich Anträgen mit einem Streitwert in Höhe von 7500 Euro (voll mit dem Antrag zu 1 bei einem Streitwert von 1000 Euro, voll mit dem Antrag zu 2 mit einem Streitwert von 4.500 Euro, teilweise mit dem Antrag zu 3, was mit 2/5 des Streitwerts von 5000 Euro bemessen werden kann), was die tenorierte Kostenquote bei einem Gesamtstreitwert von 11.000 Euro rechtfertigt.

Die Entscheidung über die vorläufige Vollstreckbarkeit beruht hinsichtlich der Beklagten auf §§ 708 Nr. 11, 711, 709 S. 2 ZPO und im Übrigen auf § 709 S. 1, 2 ZPO.

[redacted]
Vorsitzende Richterin am Landgericht

Verkündet am 27.07.2023

[redacted], JHSekr´in
als Urkundsbeamtin der Geschäftsstelle