Beglaubigte Abschrift

Landgericht Berlin
Az.: 8 O 77/22

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 LimitedFacebook Ireland Ltd., 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 8 - durch die Vorsitzende Richterin am Landgericht [redacted] als Einzelrichterin aufgrund der mündlichen Verhandlung vom 11.07.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger 500,00 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 25.07.2022 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen Schäden zu ersetzen, die dem Kläger aufgrund des mittels sog. Scrapings in der Zeit von Januar 2019 bis September 2019 erfolgten unbefugten Zugriffs Dritter auf das Datenarchiv der von der Beklagten betriebenen Plattform „Facebook“ noch entstehen werden.

3. Die Beklagte wird verurteilt, dem Kläger Auskunft über die den Kläger betreffenden, von der

Beklagten verarbeiteten personenbezogenen Daten zu erteilen.

4. Die Beklagte wird ferner verurteilt, den Kläger von vorgerichtlichen Rechtsanwaltskosten in Höhe von 90,96 € freizustellen.

5. Im Übrigen wird die Klage abgewiesen.

6. Die Kosten des Rechtsstreits trägt der Kläger zu 63 % und die Beklagte zu 37 %.

7. Das Urteil ist vorläufig vollstreckbar, für den Kläger jedoch hinsichtlich des Tenors zu Ziffer 4 nur gegen Sicherheitsleistung in Höhe von 300,00 € und im Übrigen gegen Sicherheitsleistung in Höhe des jeweils beizutreibenden Betrags zuzüglich 10 %. Der Kläger kann die Vollstreckung durch Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in entsprechender Höhe leistet.

Tatbestand

Die Parteien streiten über Ansprüche auf Schadenersatz, Unterlassung und Auskunft im Zusammenhang mit einem „Daten-Scraping-Vorfall“.

Der Kläger, der als U-Bahnfahrer bei der BVG beschäftigt ist, unterhält seit 2009 bis zum heutigen Tag ein Nutzerkonto bei dem sozialen Netzwerk „Facebook“. Im Gebiet der Europäischen Union ist die Beklagte Anbieterin dieser Plattform. Der Kläger nutzt die Plattform insbesondere, um mit Freunden zu kommunizieren, zum Teilen privater Fotos und für Diskussionen mit anderen Nutzern.

Bei der Erstellung eines Facebook-Accounts muss der Nutzer personenbezogene Daten, namentlich seinen Vor- und Zunamen, sein Geschlecht und sein Geburtsdatum sowie seine E-Mail-Adresse oder alternativ seine Handynummer in die Registrierungsmaske der Beklagten eintragen. Die Handynummer kann zudem - auch im Nachgang - im eigenen Profil ergänzt und zur Ermöglichung der Z3,wei-Faktor-Authentifizierung – und damit zur Erhöhung der Sicherheit des Profils – angegeben werden.

Das persönliche Nutzerprofil kann auf freiwilliger Basis durch weitere Daten ergänzt werden. Na-

me, Geschlecht und Nutzer-ID gehören hierbei zu den sog. „immer öffentliche Nutzerinformationen“, die also von anderen Nutzern sowie Dritten, die kein Facebook nutzen, einsehbar sind, was durch Einstellungen nicht geändert werden kann.

Hinsichtlich der Sichtbarkeit und Zugänglichkeit der übrigen personenbezogenen Daten, bietet die Beklagte ihren Nutzern eine Reihe von Einstellungsmöglichkeiten an. Hierzu zählen unter anderem der Hilfebereich und die Privatsphäre-Einstellungen. Zu diesen Bereichen gehören wiederum unter anderem einerseits die sog. Zielgruppenauswahl und andererseits die sog. Suchbarkeits-Einstellungen. Bei der Zielgruppenauswahl kann der Nutzer festlegen, wer bestimmte Datenelemente seines Profils – etwa Wohnort, Stadt, Beziehungsstatus und Geburtstag – einsehen kann. Möglich sind die Optionen „Alle“, „Freunde“ und „Freunde von Freunden“. Standardmäßig voreingestellt ist die Option „Alle“, die der Kläger auch nicht veränderte. In den Suchbarkeits-Einstellungen kann der Nutzer festlegen, wer das eigene Profil anhand seiner Telefonnummer finden kann. Im Rahmen der Suchbarkeits-Einstellungen bestehen wiederum die Optionen „Alle“, „Freunde“ und „Freunde von Freunden.“ Seit Mai 2019 steht auch die Option „Nur ich“ zur Verfügung. Wiederum ist die voreingestellte Option „Alle“. Dies ändert sich auch nicht automatisch, wenn der Nutzer die Sichtbarkeit seiner Telefonnummer unter der Zielgruppenauswahl beschränkt.

Die Telefonnummer der Nutzer, soweit diese angegeben wird, und die Voreinstellung bei der Suchbarkeitseinstellung nicht vom Nutzer verändert wird, für das sog. Contact-Import-Tool (kurz: CIT) genutzt. Mit diesem Tool können Facebook-Nutzer aber auch Dritte das Profil des Nutzers anhand seiner Telefonnummer finden. Das Tool gleicht hierfür die in das CIT eingepflegten Zahlenfolgen der Handynummern mit den bei Facebook hinterlegten Handynummern ab, um das zugehörige Facebook-Profil zu identifizieren und die dazugehörigen Daten auszuspielen. Dies funktioniert bei nicht veränderter Voreinstellung der Suchbarkeits-Einstellungen auch dann, wenn die im Profil hinterlegte Nummer aufgrund der Sichtbarkeitseinstellung für die Öffentlichkeit und andere Facebook-Nutzer nicht einsehbar ist.

Über die auf der Plattform stattfindende Datenverarbeitung und ihre Zwecke informiert die Beklagte an verschiedenen Stellen, etwa in der von ihr erstellten „Datenrichtlinie“ sowie ihrer „Cookie-Richtlinie“. Zudem werden im „Hilfebereich“, der unmittelbar auf der Facebook Homepage verlinkt ist, Informationen über die Privatsphäre Einstellungen zur Verfügung gestellt. Diese Informationen waren dem Kläger durchgängig zugänglich. Wegen des Inhalts der Datenrichtlinie sowie des Hilfebereichs der Beklagten und ihrer Nutzungsbedingungen wird auf die Anlagen K9, K19,

K20 und B 14 verwiesen.

Auch der Kläger gab bei der Registrierung auf Facebook seine Handynummer an. In seinem öffentlich sichtbaren Facebook-Profil wird diese allerdings nicht angezeigt, sondern heißt es vielmehr „keine Kontaktinformationen vorhanden“; angezeigt werden der Vor- und Nachname „Stefan Hakelberg“, die Anzahl der Freunde „398 Freunde“, sein Geschlecht „männlich“, das Geburtsdatum „3. Juli“ (Anlage B15). Der Kläger stellte in der Suchbarkeitseinstellung die Voreinstellung „alle“ zu seiner Mobilfunknummer nicht um auf beispielsweise „nur ich“ oder „Freunde“.

Im Zeitraum bis September 2019 sammelten Dritte massenhaft durch automatisierte Verfahren und unter Ausnutzung des CIT personenbezogene Daten von Facebook Nutzern (sog. „Scraping“).

Anfang April 2021 verbreiteten unbekannte Dritte Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern öffentlich im Internet und/oder sog. „Darknet“. Öffentlich wurde der Vorfall nicht durch eine gezielte Information der Betroffenen durch die Beklagte, sondern erst im Rahmen einer öffentlichen Berichterstattung im Jahr 2021. Unter den veröffentlichten Daten befanden sich auch solche des Klägers.

Mit vorgerichtlichem Schreiben, der Beklagten zugegangen am 21.05.2021, forderte der Kläger die Beklagte wegen Verstoßes gegen verschiedene Bestimmungen der Datenschutzgrundverordnung (DSGVO) zunächst jedenfalls zur Auskunft bezüglich seiner gescrapten Daten auf. Die Beklagte wies mit Schreiben vom 23.08.2023 (Anlage K2) jegliche Verantwortlichkeit zurück und teilte mit, dass sich nach bisherigen Analysen unter den abgegriffenen und veröffentlichten Daten auch solche des Klägers befanden, nämlich Nutzer ID, Vorname, Nachname, Land, Geschlecht und Telefonnummer. Ferner erläutert die Beklagte dem Kläger hierin im Einzelnen, wie er über das „Access Your Information Tool“, dessen Zugangsdaten er mitteilt, sich unter „Deine Informationen herunterladen“ über die Kategorien von Facebook-Daten informieren kann. Zudem verweist sie auf die allgemeinen Informationen u.a. zur Datenverarbeitung gemäß ihrer Datenrichtlinie. Mit weiterem Schreiben, gesendet mit E-Mail vom 27.10.2021 erfolgt klägerseits eine anwaltliche Fristsetzung zur Zahlung von Schadensersatz in Höhe von 500,00 € sowie vorgerichtlich entstandenen Rechtsanwaltskosten von 887,03 €, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft darüber, welche konkreten Daten abgegriffen wurden.

Der Kläger behauptet, dass ein Missbrauch seiner Daten und illegale Aktivitäten mit diesen dadurch begünstigt würden, dass infolge des Scraping-Vorfalls seine personenbezogenen Daten abgegriffen und im Internet sowie Darknet, u.a. auf der Seite eines bekannten Hackerforums „raidforums.com“, veröffentlicht worden seien. Hierdurch habe er einen Kontrollverlust hinsichtlich seiner personenbezogenen Daten erlitten, dies insbesondere weil seine Telefonnummer nunmehr seinen weiteren Daten zugeordnet worden sei, was so auf dem öffentlich einsehbaren Profil nicht geschehe, denn seine Mobilfunknummer habe er allein für die Zwei-Faktor-Identifizierung angegeben. Er sei in einem Zustand großen Unwohlseins und großer Sorge über den möglichen Missbrauch seiner persönlichen Daten. Zudem bekomme er seit ungefähr 2 Jahren verstärkt belästigende Spam- und Ping-Anrufe sowie sog. Phishing-Nachrichten über seine private Handynummer, seine Festnetznummer und über seine E-Mail-Adresse, insbesondere auch links zu Glücksspielen, bei denen er nur anfänglich mitgespielt, dies dann jedoch aufgehört habe. Dies belästige ihn und stelle eine Manifestierung des Kontrollverlusts und des Unwohlseins dar. Das Unwohlsein äußere sich auch in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen. Dies habe die Beklagte verursacht, da sie ihn nicht richtig über die Verwendung seiner Handynummer informiert habe und seine Daten nicht vor Scraping-Angriffen geschützt habe. Die Voreinstellung „alle“ bei den Suchbarkeitskriterien sei ihm nicht geläufig gewesen.

Der Kläger behauptet, dass seine Telefonnummer den scrapenden, unbekannten Dritten erst durch das CIT der Beklagten im Rahmen einer automatisierten „Telefonnummernaufzählung“ zugänglich gemacht worden sei.

Der Kläger beantragt mit der der Beklagten am 25. Juli 2023 zugestellten Klage:

1. Die Beklagte wird verurteilt, an ihn immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000 Euro nebst Zinsen seit Rechtshängigkeit i.H.v. 5 Prozentpunkten über dem Basiszinssatz.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen Schäden zu ersetzen, die ihm 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 250.000 Euro, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

a) personenbezogene Daten der 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 Contact-Import-Tools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.

4. Die Beklagte wird verurteilt 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 Contact-Import-Tools erlangt werden konnten.

5. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten i.H.v. 354,62 Euro zuzüglich Zinsen i.H.v. 5 Prozentpunkten über dem Basiszinssatz seit Rechtshängigkeit zu zahlen, hilfsweise den Kläger von vorgerichtlichen Rechtsanwaltskosten in Höhe von 354,62 € gegenüber ihren Prozessbevollmächtigten freizustellen.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte trägt im Wesentlichen vor, dass der sog. Scraping-Vorfall schon nicht auf einem Datenschutzverstoß beruhe. Dies ergebe sich daraus, dass lediglich Daten „gescraped“ worden seien, die die Nutzer selbst der Öffentlichkeit zur Verfügung gestellt hätten. Dies sei über Funktionen geschehen, welche es ordnungsgemäßen Nutzern ermöglichen sollen, mit anderen Nutzern in Kontakt zu treten. Hinsichtlich der Telefonnummer des Klägers, die nach den Voreinstellungen der Beklagten nicht öffentlich einsehbar gewesen sei, müssten die unbekannten Dritten diese selbst eingebracht haben. Jedenfalls sei ihr, der Beklagten, diesbezüglich kein Vorwurf zu machen. Hinsichtlich der von Klägerseite genannten Webseite „raidforums.com“ könne sie die Beschreibung des Klägers weder mit Sicherheit bestätigen noch bestreiten, weil diese Webseite von Dritten betrieben werde.

Sie habe außerdem umfangreiche Maßnahmen getroffen, um das Risiko von Scraping, das im Internet allgegenwärtig sei, zu unterbinden. Einerseits sei automatisiertes Scraping ohne Erlaubnis nach ihren Nutzungsbedingungen untersagt. Als Reaktion auf den Scraping-Sachverhalt beschäftige sie ein Team zur Bekämpfung von Scraping. Außerdem habe sie über Bot-Erkennung und Übertragungsbeschränkungen verfügt, die die Anzahl von Anfragen von bestimmten Daten reduzierten. Sie gehe gegen Scraper aktiv, u.a. mit Unterlassungsaufforderungen, vor und habe im relevanten Zeitraum zudem Captcha-Anfragen genutzt. Sie habe 2021 ihre Systeme angepasst, um sicherzustellen, dass das Verknüpfen von Telefonnummern mit bestimmten Facebook-Nutzern durch das CIT nicht mehr möglich war, auch wenn diese Maßnahme den negativen Effekt hatte, dass eine legitime nützliche Nutzerfunktion entfernt wurde.

Zudem habe sie ihren Nutzern – so auch dem Kläger – alle erforderlichen Informationen zur Datenverarbeitung zur Verfügung gestellt und umfassend über die Möglichkeiten der Anpassung ihrer Privatsphäre-Einstellungen informiert. Außerdem lege sie den Nutzern – schon in der Datenrichtlinie – durch Beispiele dar, welche Konsequenzen sich aus dem Teilen bestimmter Daten ergeben könnten. Der Kläger sei daher sowohl über die Einstellungsmöglichkeiten als auch über mögliche Konsequenzen seiner Einstellungen informiert gewesen. Er habe sich entschieden, bestimmte Daten öffentlich einsehbar auf seinem Facebook-Profil zu teilen. Zudem habe der Kläger es auch weiterhin dabei belassen, die Suchbarkeit nach der Telefonnummer bei der Einstellung „alle“ zu belassen. Eine Kopie der Rohdaten, die durch Scraping abgerufene Daten enthalte, halte sie nicht.

Sie behauptet ferner, es fehle an einer Kausalität zwischen dem Scraping-Vorfall und den belästigenden Nachrichten und Anrufen, soweit es tatsächlich zu solchen gekommen sei, was sie be-

streitet. Schließlich habe der Kläger sogar nach eigenen Angaben an Online-Glücksspielen teilgenommen, was zeige, dass er seine Daten auch anderweitig bereitwillig mitgeteilt habe. Die Beklagte ist des Weiteren der Ansicht, die Anträge zu 1., 2. und 3. seien zu unbestimmt und damit unzulässig. Zudem fehle ein Feststellungsinteresse für den Antrag zu 2.

Wegen der weiteren Einzelheiten des Sach- und Streitstands wird Bezug genommen auf die gewechselten Schriftsätze nebst Anlagen sowie auf das Protokoll der mündlichen Verhandlung vom 11.07.2023 samt informatorischer Anhörung des Klägers.

Entscheidungsgründe

I. Die zulässige Klage ist in dem zuerkannten Umfang begründet. Im Übrigen ist sie unbegründet und daher abzuweisen.

1. Zulässigkeit:

a) Das Landgericht Berlin ist international, sachlich und örtlich zuständig.

aa) Internationale Zuständigkeit:

Die internationale Zuständigkeit deutscher Gerichte ergibt sich aus Art. 79 Abs. 2 DSGVO, denn der Kläger stützt seine Ansprüche auf die DSGVO.

Hiernach können Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist. Verantwortliche sind gemäß Art. 4 Nr. 7 DSGVO natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.

Der Kläger als Betroffener hat seinen Wohnsitz in Deutschland. Die Beklagte ist Verantwortliche im vorgenannten Sinne. Sie entscheidet als Betreiberin von Facebook in der EU über das Schicksal der dort gespeicherten personenbezogenen Daten der Nutzer, insbesondere über Zwecke und Mittel der Verarbeitung dieser Daten. Sie ist keine hoheitlich handelnde Behörde.

bb) Sachliche Zuständigkeit:

Das Landgericht ist aufgrund rügeloser Einlassung der Beklagten nach Hinweis des Gerichts auf die sachliche Unzuständigkeit trotz des Streitwerts von 4.500,00 € sachlich zuständig (§§ 23 Nr. 1; 71 Abs. 1 GVG i.V.m. § 39 ZPO).

cc) Örtliche Zuständigkeit:

Die örtliche Zuständigkeit des Landgerichts Berlin ergibt sich aus § 44 Abs. 1 S. 2 Bundesdatenschutzgesetz (BDSG) sowie Art. 18 Abs. 1 EuGVVO, da der Kläger - er ist Verbraucher - seinen gewöhnlichen Aufenthalt in Berlin und damit im Bezirk des angerufenen Gerichts hat.

b) Bestimmtheit der Klageanträge:

Die Klageanträge sind hinreichend bestimmt (§ 253 Abs. 2 Nr. 2 ZPO); dies gilt auch für die Anträge zu 1 bis 3.

aa) Antrag zu 1:

Insbesondere ist es - entgegen dem Vorbringen der Beklagten - nicht so, dass mit dem Antrag zu 1 ein Betrag geltend gemacht wird, der sich aus mehreren begehrten Schadensersatzansprüchen gestützt auf Rechtsverletzungen aufgrund mehrerer Lebenssachverhalte zusammensetzt, wobei unklar bleibt, welcher Anteil des Betrags auf welchen Anspruch entfallen soll. Vielmehr stützt der Kläger die Klage auf einen einheitlichen Lebenssachverhalt, nämlich den 2021 bekannt gewordenen und näher beschriebenen „Scrapingvorfall“, der seiner Auffassung nach aus verschiedenen Rechtsgründen einen Schadensersatzanspruch nach der DSGVO begründet.

bb) Auch der Feststellungsantrag zu 2 genügt somit nach Vorstehendem den Bestimmtheitsanforderungen.

cc) Gleiches gilt für den Unterlassungsantrag zu 3. Die Formulierung „*die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen*“ in dem Antrag zu Ziffer 3.a ist zwar auslegungsbedürftig aber noch hinreichend bestimmt, § 253 Absatz 2 Nr. 2 ZPO. Eine auslegungsbedürfte Formulierung des Antrags ist hinzunehmen, wenn dies zur Gewährleistung eines effektiven Rechtsschutzes notwendig ist, weil der Kläger seinen Antrag nicht konkreter fassen kann (vgl. BGH, Urteil vom 21. Mai 2015 – I ZR 183/13 –, juris Rn. 12 ff.). Hier ist eine konkrete Bezeichnung der erforderlichen Maßnahmen aufgrund der stetig fortschreitenden technischen Entwicklung nicht geeignet, das vom Kläger angestrebte Begehren zu erreichen. Ebenso führen die auslegungsbedürftigen Begriffe „unübersichtlich“ und „unvollständig“ in dem Antrag zu Ziffer 3.b nicht dazu, dass dieser Antrag nicht den Bestimmtheitsanforderungen der ZPO genügt. Denn dem Antrag

kann unter Berücksichtigung der Klagebegründung entnommen werden, wann nach Auffassung des Klägers eine übersichtliche und vollständige Gestaltung vorliegt, nämlich wenn ausdrücklich über die Verwendung der Telefonnummer in den hierauf gerichteten Einstellungsmöglichkeiten belehrt wird (vgl. auch LG Berlin, Urteil vom 07.02.2023, Gz. 56 O 75/22).

d) Feststellungsinteresse für Antrag zu 2:

Das gemäß § 256 Abs. 2 ZPO für den Antrag zu 2 erforderliche Feststellungsinteresse ist anzunehmen. Ein Feststellungsantrag ist schon dann zulässig, wenn nach dem insoweit schlüssigen Vortrag des Klägers nicht auszuschließen ist, dass die Schadensentwicklung noch nicht abgeschlossen ist und der Kläger seinen Anspruch deswegen teilweise nicht beziffern kann (vgl. Zöller-Greger, ZPO, 34. Aufl. 2023, § 256 Rn. 9). Dies ist hier der Fall, denn es ist nicht auszuschließen, dass noch materielle Schäden des Klägers aufgrund des damaligen Scrapingvorfalls bekannt werden können. .

2. Begründetheit:

Der Klage ist teilweise - nämlich in dem aus dem Tenor ersichtlichen Umfang - begründet, so dass ihr insoweit stattzugeben ist. Im Übrigen ist sie unbegründet und daher abzuweisen.

a) Antrag zu 1 gerichtet auf Schmerzensgeld:

Dem Kläger steht gegen die Beklagte ein Anspruch auf Schadensersatz in Form eines Schmerzensgeldes für seinen immateriellen Schaden zu, wobei das Gericht diesen mit 500,00 € bemisst.

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

Nach Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen. Art. 82 Abs. 2 S. 1 DSGVO konkretisiert diese Regelung dahingehend, dass bei mehreren an der Verarbeitung beteiligten Parteien, jede Partei für den Schaden haftet, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO ist diejenige, die allein oder mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten i.S.d. Art. 4 Nr. 1 DSGVO entscheidet. Dabei umfasst die Verarbeitung gem. Art. 4 Nr. 2 DSGVO u.a. das Erheben, das Erfassen, die Speicherung, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbrei-

tung oder andere Form der Bereitstellung, den Abgleich oder die Verknüpfung.

aa) Die Beklagte verursachte eine nicht dieser Verordnung entsprechende Verarbeitung. Dabei verstieß die Beklagte kumulativ gegen mehrere Vorschriften der DSGVO, nämlich jedenfalls gegen Art. 13 Abs. 1 Buchst. c DSGVO (1), Art. 24; 32; 5 Abs. 1 Buchst. f DSGVO (2), Art. 24 Abs. 2; 25 Abs. 1; 5 Abs. 1 Buchst. a, b, c, f DSGVO (3); Art. 25 Abs. 2; 5 Abs. 1 Buchst. a, b, c, f DSGVO (4).

(1) Die Beklagte verstieß gegen ihre datenschutzrechtlichen Aufklärungs- und Informationspflichten nach Art. 13 Abs. 1 Buchst. c DSGVO.

Gemäß Art. 13 DSGVO hat der Verantwortliche eines Datenverarbeitungsprozesses gegenüber dem Betroffenen, umfangreiche Informations- und Aufklärungspflichten zu erfüllen. Entsprechend der Legaldefinition des Art. 4 Nr. 2 DSGVO entstehen diese Informations- und Aufklärungspflichten bereits mit der Erhebung personenbezogener Daten. Teilt der Verantwortliche dem Betroffenen die in Art. 13 Abs. 1 und Abs. 2 DSGVO vorgesehenen Informationen nicht vollständig, inhaltlich unrichtig oder verspätet mit, verletzt er seine Informationspflichten.

Nach Art. 13 Abs. 1 Buchst. c) DSGVO besteht eine Informationspflicht insbesondere dahingehend, dass der Verantwortliche dem Betroffenen die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung mitteilt. Sinn und Zweck dieser Regelung ist, dass der Betroffene eines Datenverarbeitungsprozesses unter Berücksichtigung der Grundsätze einer fairen und transparenten Verarbeitung von personenbezogenen Daten nicht nur über die Existenz des Verarbeitungsvorganges, sondern darüber hinaus auch über die Zwecke der Verarbeitung unterrichtet wird (vgl. Knyrim in Ehmann/Selmayr, 2. Aufl. 2018, DS-GVO Art. 13 Rn. 1). Die Aufklärung über die Zwecke der Verarbeitung muss insbesondere für den Nutzer klar und verständlich sowie nachvollziehbar sein.

Diesen Anforderungen wird die Beklagte vorliegend nicht gerecht.

Hinsichtlich der Telefonnummer des Nutzers ist selbst auf Grundlage des unstreitigen Sachverhalts nicht erkennbar, dass die Beklagte über die Zwecke der Verarbeitung zutreffend und in ausreichendem Umfang aufgeklärt hat. Es ist insbesondere nicht erkennbar, dass ein potentieller Nutzer rechtzeitig, also „im Zeitpunkt der Erhebung“ seiner Telefonnummer – ggf. bereits bei der Registrierung – den Hinweis erhält, dass diese (auch) dem Zweck dient, anderen Nutzern und

Dritten das Auffinden seines Profils zu ermöglichen (so auch LG Stuttgart, Urteil vom 26.01.2023, Az.: 53 O 95/22; LG Ulm, Urteil vom 26.06.2023, Az.: 4 O 7/23; LG Berlin, a.a.O., S. 13 ff.). Soweit der Kläger darüber informiert wird, dass ihm seine Telefonnummer nützlich sein kann, um andere Facebook-Nutzer zu finden, mag er daraus zwar Rückschlüsse hinsichtlich der Telefonnummer-Suchfunktion ziehen können. Die Information durch die Beklagte bleibt jedoch selektiv und damit unvollständig (LG Berlin, a.a.O.). Das wird auch nicht durch den 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. 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 (LG Berlin, a.a.O.).

Die mitgeteilten Informationen stellen mithin die Zwecke der Datenverarbeitung nicht in ausreichender Transparenz dar. Da zudem die Funktionsweise des CIT nicht erklärt wird, kann ein Nutzer nicht den Schluss ziehen, dass Dritte durch die Funktionsweise des CIT die Mobilfunknummer des Klägers in Erfahrung bringen können.

Etwaige sonstige – der Registrierung – nachfolgenden Hinweise und Informationen durch die Beklagte sind jedenfalls verspätet.

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 Gala/Heckmann, DSGVO - BDSG, 3. Aufl. 2022, DSGVO Art. 13 Rn. 64).

(2) Die Beklagte hat zudem gegen Art. 32, 24, 5 Abs. 1 Buchst. f DSGVO verstoßen, indem sie es unterließ, geeignete technische und organisatorische (Sicherheits-)Maßnahmen bezüglich der Nutzung des CIT umzusetzen.

Art. 32 DSGVO regelt die Pflicht des Verantwortlichen und des Auftragsverarbeiters, bestimmte technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Schutzni-

veau im Hinblick auf die verarbeiteten personenbezogenen Daten zu gewährleisten. Gemäß Art. 32 Abs. 1 Hs. 1 DSGVO haben der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Art. 32 Abs. 1 DSGVO verpflichtet den Verantwortlichen mithin nicht zu einem absoluten Schutz(niveau) der Daten. Das Schutzniveau muss jedoch nach Verarbeitungskontext, Art, Umfang und Zwecken der Verarbeitung sowie dem Risiko bezüglich der Rechte und Freiheiten der betroffenen Personen im Einzelfall angemessen sein.

Art. 32 DSGVO konkretisiert damit die als Generalauftrag gestalteten Datensicherheitsmaßnahmen des Art. 24 DSGVO und dient damit u.a. der Gewährleistung der Absicherung der Datenschutzgrundsätze der Vertraulichkeit und Integrität nach Art. 5 Abs. 1 Buchst. f DSGVO. Zielrichtung ist ein umfassender Schutz der für die Verarbeitung von personenbezogenen Daten genutzten Systeme, also im Kern die Datensicherheit (Mantz in Sydow/Marsch DS-GVO/BDSG, 3. Aufl. 2022, DSGVO Art. 32 Rn. 1;s.a. Hartung in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, DSGVO § 24 Rn. 24).

Diesen Anforderungen genügten die von der Beklagten behaupteten und zum gegenständlichen Zeitpunkt eingesetzten Schutzmaßnahmen nicht. Denn 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 (ausführlich hierzu LG Ulm, a.a.O.; LG Berlin, a.a.O.). Soweit die Beklagte etwa vorträgt, gegen Scraper mit Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren vorzugehen, ist schon nicht ersichtlich, wie diese Maßnahmen – die einen Scraping-Vorfall denklogisch nachgeordnet sind – ein angemessenes Schutzniveau der Daten sicherstellen sollen. Auch die nach der Behauptung der Beklagten bereits zum Zeitpunkt des Scraping-Vorfalls eingesetzten Maßnahmen, wie etwa Übertragungsbeschränkungen und Bot-Erkennung, sind für sich genommen nicht geeignet, ein angemessenes Schutzniveau im Sinne des Art. 32 DSGVO herzustellen. Die Beklagte selbst trägt vor, dass Scraper solche Systeme mit geringem Aufwand umgehen können.

Das CIT ermöglichte unbekannten Dritten ohne Weiteres einen unbefugten Zugang i.S.d. Art. 32 Abs. 2 DSGVO. Es konnte – mangels angemessener Schutzmaßnahmen – von Dritten insbe-

sondere so genutzt werden, dass diese – bekannte oder generierte – Telefonnummern mit den bei der Beklagten hinterlegten Telefonnummern abgleichen konnten und so mit bestimmten Nutzerprofilen verknüpfen konnten. Hierdurch lieferte die Beklagte faktisch gesehen einen Mechanismus zur Identifikation der einem Nutzer zugehörigen und öffentlich nicht einsehbaren Telefonnummer, wodurch eine etwaige Pseudonymisierung aufgehoben wird. Zugleich wird die Möglichkeit eröffnet, die Telefonnummer mit weiteren (Profil-)Daten des Inhabers der Nummer zu verknüpfen. Dies birgt für die Nutzer das Risiko von gezielten Phishing-Attacken, Identitätsdiebstahl oder sonstigem Missbrauch der Daten und damit dem Eintritt von materiellen oder immateriellen Schäden. Insbesondere unter Berücksichtigung dessen, dass das Phänomen „Scraping“ der Beklagten – wie sich auch aus dem Beklagtenvortrag selbst ergibt – durchaus als regelmäßig vorkommendes Problem bekannt ist, drängt sich die Erforderlichkeit weiterer Schutzmaßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus geradezu auf. Eine denkbare Maßnahme wäre etwa, neben der Abfrage der Telefonnummer im CIT, zusätzlich weitere Informationen, z.B. einen Vor- oder Zunamen abzufragen, bevor das CIT einen Kontaktvorschlag ausspielt. Dies hätte jedenfalls die Ausnutzung des CIT durch eine Telefonnummeraufzählung erschwert.

Die Beklagte nahm allerdings erst den Vorfall zum Anlass, ihre Schutzmaßnahmen zu evaluieren und traf ausweislich des in das Verfahren eingeführten Artikels „Scraping nach Zahlen" vom 19.05.2021 „eine Reihe von Verbesserungen" jedenfalls im September 2019. So etablierte die Beklagte erst im Nachgang zum Scraping-Vorfall weitergehende Sicherheitsmaßnahmen, wie etwa den sog. ,,Social Connection Check".

Soweit die Beklagte versucht, sich mit dem Hinweis, dass sich,,Scraping" nicht vollständig verhindern lasse, der Pflicht nach Art. 32 DSGVO zu entziehen, kann sie hiermit nicht durchdringen. Art. 32 DSGVO verpflichtet – wie aufgezeigt – schließlich nicht zu einem vollständigen und bestmöglichen Schutz im Sinne einer Erfolgspflicht, sondern lediglich zur Sicherstellung eines angemessenen Schutzniveaus der Daten im Sinne einer Bemühenspflicht. Wenn die Beklagte – wie vorliegend – jedoch daran scheitert, eine ihrer Kernpflichten der DSGVO umzusetzen und 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 den bei der Beklagten hinterlegten, grundsätzlich nicht öffentlichen Telefonnummern zugeordnet werden können, kann sie eine entsprechende Funktion schlicht nicht oder jedenfalls nicht in diesem Zuschnitt anbieten.

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

(3) Die Beklagte hat zudem gegen Art. 24 Abs. 2; 25 Abs. 1; 5 Abs. 1 Buchst. a, b, c, f DSGVO verstoßen.

Nach Art. 25 Abs. 1 DSGVO muss der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen treffen – wie etwa Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze - wie etwa Datenminimierung - wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DGVO zu genügen und die Rechte der betroffenen Personen zu schützen. Dies ist der Beklagten nicht gelungen.

Wie bereits zu Art. 32 Abs. 2 DSGVO ausgeführt, waren die von der Beklagten im relevanten Zeitpunkt eingesetzten technischen und organisatorischen Maßnahmen schon nicht dazu geeignet, dem Grundsatz der „Integrität und Vertraulichkeit“ im Sinne des Art. 5 Abs. 1 Buchst. f DSGVO gerecht zu werden. Auch waren die technischen und organisatorischen Maßnahmen der Beklagten in Bezug auf das CIT sowie die Information über die Datenverarbeitung in diesem Zusammenhang nicht dazu geeignet, die Grundsätze der „Datenminimierung“ (Art. 5 Abs. 1 Buchst. c DSGVO), der „Zweckbindung“ (Art. 5 Abs. 1 Buchst. b DSGVO) oder der „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“ (Art. 5 Abs. 1 Buchst. a DSGVO) wirksam umzusetzen.

Hierfür sprechen auch die Feststellungen der irischen Datenschutzbehörde CDC, die in ihrem Bescheid vom 25.11.2022 (Anlage K3) umfassend dargelegt hat, dass die Beklagte hinsichtlich des CIT nicht den Anforderungen der DSGVO gerecht wurde und ein Verstoß gegen Art. 25 Abs. 1 DSGVO - den sie als den schwerwiegendsten Verstoß der Beklagten gegen die DSGVO einordnet (u.a. Rn. 169, 320 der Entscheidung) - gegeben ist. Berücksichtigt wurde dabei insbesondere, dass angesichts der enormen Datenmengen, die die Beklagte in ihren Datenbanken

vorhält, ein erhebliches Angriffsrisiko und eine Anfälligkeit für Scraping-Angriffe besteht. In Rn. 141 ff. (S. 45 f.) der Entscheidung wird ausgeführt, dass die Beklagte weitere technische Schutzmaßnahmen hätte ergreifen können, beispielsweise, indem Telefonnummern keine exakten Profile durch Einsatz des CIT zugeordnet würden, sondern mehrere verwandte Profilvorschläge. Rn. 142 der Entscheidung stellt die Bedeutung von quantitativen Beschränkungen ("rate limiting") heraus. Rn. 143 verweist auf die Möglichkeit technischer Maßnahmen wie "Captchas" (dazu und zu den Einwänden der Beklagten insoweit auch Rn. 165 f.) oder Veränderungen in der Benutzeroberfläche. Als organisatorische Maßnahme wird beispielsweise der Einsatz eines "red team" genannt, um Scraping-Aktivitäten zu erkennen und das Risiko eines Datenscraping zu mindern.

Die Ausführungen der Fachbehörde sind überzeugend, zahlreiche Sicherheitsmaßnahmen, die unterlassen wurden, wurden genannt. Zu berücksichtigen ist auch, dass die Beklagte in Reaktion auf den Vorfall nach eigenem Vorbringen ihre Sicherheitsvorkehrungen angepasst und nunmehr ein Team zur Bekämpfung von Scraping-Aktivitäten eingesetzt hat. Vor diesem Hintergrund steht zur Überzeugung des Gerichts fest, dass ein Verstoß gegen Art. 25 Abs. 1 DSGVO gegeben ist (so bereits LG München, Urteil vom 20.04.2023, Az.: 15 O 6231/22). Dieser ist auch geeignet, einen Schadensersatzanspruch gem. Art. 82 DSGVO auszulösen (anders LG Ulm, a.a.O.). Der organisatorische Charakter der Vorschrift kann die Feststellung eines Verstoßes gegen diese Vorschrift erschweren, verhindert ihn jedoch nicht; hier kann ein Verstoß jedoch klar festgestellt werden, so dass sich Feststellungsprobleme nicht ergeben (siehe dazu auch Hartung in Kühling/Buchner, a.a.O., Art. 25 DSGVO Rn. 31; Mantz in Ehmann/Selmayr, a.a.O., Art. 25 Rn. 25).

(4) In evidenter Art und Weise hat die Beklagte durch ihre Voreinstellung zudem gegen Art. 25 Abs. 2 DSGVO verstoßen.

Nachdem Art. 25 Abs. 1 DSGVO den Verantwortlichen, hier die Beklagte, verpflichtet, bereits bei der Entwicklung von Produkten, Diensten und Anwendungen sicherzustellen, dass die Anforderungen der DSGVO erfüllt werden (“privacy by design“), konkretisiert Artikel 25 Abs. 2 DSGVO diese Verpflichtung, indem sie verlangt, vorhandene Einstellungsmöglichkeiten standardmäßig auf die „datenschutzfreundlichsten“ Voreinstellungen zu setzen (“privacy by default“) wie folgt:

> *„Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ih-*

re Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.“

Der hier geregelte „Datenschutz durch Voreinstellungen" soll - so ausdrücklich Art. 25 Abs. 2 S. 3 DSGVO - sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Insbesondere sollen hierdurch diejenigen Nutzer geschützt werden, 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 (LG Berlin, a.a.O., S. 14). Die Nutzer sollen keine Änderungen an den Einstellungen vornehmen müssen, um eine möglichst „datensparsame" Verarbeitung zu erreichen. Vielmehr soll umgekehrt jede Abweichung 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, a.a.O., DSGVO Art. 25 Rn. 28).

Die Beklagte hat aber hier durch ihre Technik- und Organisationsgestaltung mit Hilfe von Voreinstellungen gerade nicht sichergestellt, dass nur personenbezogene Daten - hier die Mobilfunknummer des Klägers - verarbeitet werden, die für den Verarbeitungszweck erforderlich sind. Vielmehr hat sie das Gegenteil einer datenschutzfreundlichen Voreinstellung vorgenommen, indem sie für die Telefonnummer die Voreinstellung „alle“ im Bereich der „Suchbarkeits-Einstellungen“ vorgab.

Die „Suchbarkeit“ der Telefonnummer war vielmehr durch die Beklagte im relevanten Zeitraum gerade auf „Alle“ voreingestellt, so dass Dritte - entgegen Art. 25 Abs. 2 S. 3 DSGVO mit der Telefonnummer nach einem Nutzerprofil suchen und über das CIT eine Verknüpfung zwischen Telefonnummer und dazugehörigem Nutzerprofil herstellen konnten. Um dies zu ändern hätte ein Nutzer die Suchbarkeits-Einstellung in seinen Privatsphäre-Einstellungen proaktiv ändern müssen, wozu – mangels entsprechender Information über die Funktionsweise des CIT und den einschlä-

gigen Voreinstellungen – jedoch aus Sicht eines durchschnittlichen Nutzers schon kein Anlass bestand. Mit der Bereitstellung dieses Systems und den genannten Voreinstellungen machte die Beklagte die personenbezogenen Daten des Klägers daher ohne dessen Eingreifen einer unbestimmten Anzahl von Personen zugänglich (vgl. LG Lüneburg, Urteil vom 24.01.2023, Az.: 3 O 83/22, juris). Entsprechend hat auch die irische Datenschutzbehörde einen Verstoß der Beklagten gegen Art. 25 Abs. 2 DS-GVO angenommen.

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, a.aO., Art. 25 DSGVO Rn. 77; Martini in Paal/Pauly, DSGVO – BDSG 3. Aufl., Art. 25 DSGVO Rn. 6;). 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 eben nicht ohne Weiteres möglich gewesen.

(5) Nur ergänzend wird festgehalten, dass die Beklagte zudem auch gegen Art. 33 und Art. 34 Abs. 1 und 2, Art. 15 DSGVO verstieß, indem sie erstens den Kläger nach dem Scraping-Vorfall nicht von der Verletzung des Schutzes der personenbezogenen Daten der klagenden Partei unterrichtet hat, zweitens auch die zuständige Datenschutzbehörde nicht benachrichtigte und drittens dem Kläger zunächst in - in Bezug auf sein Begehren - nicht ausreichendem Maße Auskunft erteilte. Hierdurch wurde dem Kläger insbesondere die Möglichkeit genommen, früher auf die Verletzung der DSGVO reagieren zu können (vgl. LG Ulm, a.a.O.).

Ferner ergänzend ist festzuhalten, dass die Beklagte die Telefonnummer im CIT ohne Rechtsgrundlage verarbeitete, da es insbesondere an einer freiwilligen Zustimmung i.S.d. Art. 6 Abs. 1 Buchst. a; 7 DSGVO und einer anderen Berechtigung gem. Art. 6 Abs. 1 Buchst. b - f DSGVO fehlte. Es ist eben nicht so, dass der Kläger gemäß Art. 6 Abs. 1 DSGVO i.V.m. Art. 4 DSGVO seine Einwilligung zur Verarbeitung dieser Daten - Mobilfunknummer - für den Zweck der Suche durch „alle“ gegeben hätte oder diese Verarbeitung aus anderen in Art. 6 Abs. 1 DSGVO genannten Gründe gerechtfertigt wäre. Die Bedingungen der Einwilligung gem. Art. 7 DSGVO liegen nicht vor, insbesondere kann - so Erwägungsgrund 32 der DSGVO - eine Einwilligung nicht durch Stillschweigen, standardmäßig angekreuzte Kästchen oder Untätigkeit erteilt werden. Vielmehr sind „Opt-out-Einwilligungen“ - wie hier die Voreinstellung „alle“ - keine Einwilligungen im Sinne der Verordnung (Schulz in Gola/Heckmann, a.a.O., Art. 7 Rn. 45).

Die Rechtmäßigkeit der Verarbeitung ergibt sich auch nicht aus anderen Bedingungen gem. Art.

6 Abs. 1 Buchst. b - f DSGVO, denn eine Erforderlichkeit der Zugänglichkeit der Mobilfunknummer für „alle“ hat die Beklagte nicht dargelegt. Allein das Zusatzangebot der „Suchfunktion“ für alle über die Telefonnummer, um die Plattform - so die Äußerungen der Beklagten - für die Nutzer „noch attraktiver“ zu machen, erfüllt nicht die Erforderlichkeitskriterien dieser Bestimmung.

bb) Dem Kläger ist im Zusammenhang mit dem Scraping-Vorfall auch ein nach Art. 82 DSGVO ersatzfähiger - immaterieller - Schaden kausal entstanden.

Nach Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Der Schaden muss nach dem Wortlaut der Norm tatsächlich entstanden sein und ist damit nicht mit der zugrundeliegenden Rechtsgutverletzung gleichzusetzen (s.a. EuGH, (3. Kammer), Urteil vom 04.05.2023, Rs. C-300/21, UI/Österreichische Post AG, beck-online, NJW 2023, 1930 ff.). Für die Ersatzpflicht genügt demnach nicht allein ein Verstoß gegen die DSGVO, sondern es muss auch ein Schaden eingetreten sein (EuGH, a.a.O.).

Der Begriff des Schadens ist nach dem Erwägungsgrund 146 S. 3 DSGVO weit auszulegen, sodass die Betroffenen einen wirksamen Ersatz bekommen. Es handelt sich um einen autonomen Begriff des Unionsrechts, der in allen Mitgliedstaaten einheitlich auszulegen ist (EugH, a.a.O.). Dabei kommt es insbesondere auf die Ziele und den Sachzusammenhang der Verordnung an. Soweit zwar einerseits nicht allein der bloße Verstoß gegen die Bestimmungen der DSGVO zur Begründung eines Schadensersatzanspruchs ausreicht, so bedarf der erlittene Schaden andererseits nicht eines bestimmten Grades an Erheblichkeit (EuGH, a.a.O., Rdnrn. 51, 59). Der Schaden kann bereits etwa in dem unguten Gefühl liegen, dass personenbezogene Daten Unbefugten bekannt geworden sind, insbesondere, wenn nicht ausgeschlossen ist, dass die Daten unbefugt weiterverwendet werden. Er kann bereits in der Ungewissheit darüber bestehen, ob personenbezogene Daten an Unbefugte gelangt sind (LG Berlin, a.a.O. mit Verweis auf: Bergt in Kühling/Buchner, a.a.O., Art. 82 Rn. 18b). So können unbefugte Datenverarbeitungen zu einem Gefühl des Beobachtetwerdens und der Hilflosigkeit führen, was die betroffenen Personen letztzlich zu einem Objekt der Datenverarbeitung degradiert. In Erwägungsgrund 75, 85 der DSGVO werden ausdrücklich der Kontrollverlust und die „unbefugte Aufhebung der Pseudonomysierung“ als „insbesondere“ zu erwartende Schäden genannt. Bei den genannten Beeinträchtigungen kann es sich denklogisch nur um immaterielle Schäden handeln (Bergt, a.a.O.). Spezifische Angaben, wie konkret sich der Kontrollverlust auf die Persönlichkeit und auf das Leben der

betroffenen Person ausgewirkt hat, sind nicht erforderlich, (Bergt, a.a.O.). Als mögliche Schäden kommen beispielsweise auch Ängste, Stress, sowie Komfort- und Zeiteinbußen in Betracht, die sich vor allem nach den im konkreten Fall erforderlichen Abhilfemaßnahmen richten (Bergt, a.a.O.).

Hier hat der Kläger einen Schaden erlitten. Seine öffentlichen Profildaten wurden mit seiner Telefonnummer verknüpft und so im Zusammenhang mit dem Datenscraping im Internet veröffentlicht. Soweit die Beklagte entwendet, dass die von dem Kläger vorgetragenen Belästigungen insbesondere durch häufige Anrufe und SMS nicht notwendigerweise auf die mit dem Scraping-Vorfall verbundenen Veröffentlichungen der klägerischen Daten zurückzuführen sind, hindert dies einen Anspruch des Klägers nicht. Denn der Kläger hat nachvollziehbar zum Ausdruck gebracht, dass er die Sorge hegt, dass diese Belästigungen auf den Scraping-Vorfall zurückzuführen sind. Er schilderte gleichfalls, dass er aufgrund dieser starken Belästigungen sein Verhalten änderte, nämlich dass er bei der Annahme von Anrufen zögert und eine Unsicherheit empfindet, bei eigentlich ordnungsgemäßen Nachrichten z.B. zu Paketzustellungen. Diese von dem Kläger im Rahmen seiner persönlichen Anhörung im Termin gemachten Angaben haben das Gericht überzeugt; es hält diese für glaubhaft. Dabei kommt es im Ergebnis nicht darauf an, wozu die ohne Einverständnis des Klägers zugänglich gemachten Daten tatsächlich von den „Scrapern“ oder unbefugten Dritten verwendet wurden (vgl. Gola/Piltz in Gola/Heckmann, a.a.O., Art. 82 Rn. 18).

Der Schaden ist kausal auf die Verletzungen der Datenschutzgrundverordnung zurückzuführen. Hierzu genügt eine Mitursächlichkeit. Es muss nach der allgemeinen Lebenserfahrung davon ausgegangen werden können, dass dieser Schaden auch auf die Verletzungen zurückzuführen ist (Bergt in Kühling/Buchner, a.a.O., DSGVO Art. 82 Rn. 45). Das ist hier der Fall. Es ist gerade nicht so, dass eine Kausalität ausgeschlossen ist, weil der Kläger beispielsweise auch an Glücksspielen teilnahm. Im Sinne des von der DSGVO in ihrem 146. Erwägungsgrund, dort S. 6, „effektiven Schadensersatzes“ genügt es daher, dass die Verletzungshandlungen der Beklagten grundsätzlich geeignet waren, den Schaden auszulösen und kein atypischer Kausalverlauf vorlag (Bergt in Kühling/Buchner, a.a.O., DSGVO Art. 82 Rn. 47 f.). Hier hat der Kläger nachvollziehbar beschrieben, dass er die empfundenen Beeinträchtigungen, insbesondere den Kontrollverlust sowie sein zunehmendes Misstrauen auf den streitgegenständlichen Scrapingvorfall zurückführt. Dabei sind alle vorstehend festgestellten Verstöße (1) - (4) gegen die DSGVO kausal für den entstandenen Schaden, denn sie alle - und zwar schon jeder einzelne Verstoß für sich genommen - führten zu dem dem Kläger entstandenen Kontrollverlust und dem bei ihm entstan-

dene Misstrauen.

cc) Keine Entlastung gem. Art. 82 Abs. 3 DSGVO

Der Beklagten gelingt es nicht, sich mit Blick auf den Scraping-Vorfall nach Art. 82 Abs. 3 DSGVO zu entlasten. Hierfür müsste sie nachweisen, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Unabhängig davon, ob man den Begriff der Verantwortlichkeit mit Teilen der Rechtsprechung und der Literatur mit dem Begriff des Verschuldens gleichsetzt (OLG Stuttgart, Urteil vom 31. März 2021 – 9 U 34/21 –, juris) oder Art. 82 DSGVO als Gefährdungshaftungstatbestand versteht (Kreße in Sydow/Marsch, a.a.O., DSGVO Art. 82 Rn. 19 ff.) kann sich die Beklagte nicht entlasten.

Die Beklagte kann auch nicht nachweisen, dass sie kein Verschulden trifft. Das wäre nämlich nur dann der Fall, wenn sie sämtliche Sorgfaltsanforderungen erfüllt hätte und ihr nicht die geringste Fahrlässigkeit vorzuwerfen wäre (Bergt in Kühling/Buchner, a.a.O., DSGVO Art. 82 Rn. 54). Hält die Beklagte als Anspruchsgegnerin etwa sämtliche erforderlichen Sicherheitsmaßnahmen (Art. 32 DSGVO) ein und kommt es dennoch zu einem unbefugten Datenzugriff, fehlt es an einem Verschulden. War der Angriffsweg dagegen bekannt oder auch nur erkennbar, ist der Entlastungsbeweis nicht geführt. Da vorliegend die nach Art. 32 DSGVO erforderlichen Sicherheitsmaßnahmen von der Beklagten nicht eingehalten wurden (s.o.), kann die Beklagte nicht nachweisen, dass sie kein Verschulden trifft. Hinzukommen – wie aufgezeigt – jedenfalls Verstöße gegen Art. 13 Abs. 1 Buchst. c DSGVO, Art. 25 Abs. 1 DSGVO sowie gegen Art. 25 Abs. 2 DSGVO (s.o. zu I.2.a) aa) (1)-(4)).

Auch die Behauptung, dass die Telefonnummern von den Daten-Scrapern „bereitgestellt" worden seien, kann – selbst wenn sie zutreffend wäre – die Beklagte nicht entlasten. Schließlich wurden die (fiktiven) Telefonnummern – wie bereits dargelegt – erstens erst durch die Zuordnung über die Suchfunktion der Beklagten zu einzelnen Nutzerprofilen zu personenbezogenen Daten und zweitens konnten die Telefonnummern – unter Aufhebung der Pseudonymisierung – konkreten Nutzerprofilen zugeordnet werden. Es wäre an der Beklagten gewesen, ein solch automatisiertes Verfahren zu verhindern.

Der Entlastungsnachweis gelingt der Beklagten mithin nicht.

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 ausgestaltet ist.

dd) Mitverschulden:

Ein Mitverschulden des Geschädigten, kann - anders als nach § 254 BGB - den Anspruch nicht mindern, denn nach Art. 82 Abs. 3 DSGVO ist ein Haftungsausschluss nur dann möglich, wenn dem Verantwortlichen der Schaden „in keiner Hinsicht“ zur Last gelegt werden kann (Bergt in Kühling/Buchner, a.a.O., Art. 82 DSGVO, Rn. 59). Dies ist hier nach Vorstehendem nicht der Fall.

ee) Schadenshöhe:

Das Gericht hält nach Anhörung des Klägers und dem dabei gewonnenen Eindruck in Ausübung des ihm durch § 287 ZPO eingeräumten Ermessens ein Schmerzensgeld von 500,00 € für unter Berücksichtigung der Unionsgrundsätze der Äquivalenz und Effektivität (EugH a.a.O., Rn. 59) für angemessen, aber auch ausreichend. Hiermit trägt es einerseits der Ausgleichs- und Genugtuungsfunktion und andererseits der auch generalpräventiven Funktion des immateriellen Schadensersatzes hinreichend Rechnung.

Der Kläger hat dem Gericht einerseits glaubhaft vermittelt, dass ihn der Verlust der Kontrolle über seine Daten und deren freie Verfügbarkeit im Internet belastet hat und ein Misstrauen sowie ein Gefühl der Hilflosigkeit hervorgerufen hat. Er bekomme zudem regelmäßig Spam-SMS und Phishing-E-Mails sowie fast täglich Ping- und Spamanrufe. Teilweise erhalte er 2-3 Anrufe pro Tag vielleicht 20-30 SMS pro Monat und in den letzten zwei Jahren zwei- bis dreihundert E-Mails. Dies stelle für ihn eine erhebliche Belästigung dar, die er wegen des insoweit passenden Zeitrahmens auf das Datenscraping zurückführe. E-Mails und SMS lösche er nunmehr sofort. Früher habe er stets ans Telefon gehen können, mittlerweile aber meine er genau überlegen zu müssen, ob er ans Telefon gehen könne und/oder auf SMS und E-Mails antworten könne. Da er viel im Internet bestelle, würden ihn auch insbesondere solche Nachrichten verunsichern, in denen ihm mitgeteilt werde, dass er ein Paket abholen könne. Nicht immer könne er die Seriosität solcher Nachrichten beurteilen. Diese Äußerungen des Klägers im Rahmen seiner persönlichen Anhörung überzeugten das Gericht. Der Kläger zeigt sich damit als lebhafter aber noch durchschnittlicher Nutzer des Internet.

Dabei fällt nicht ins Gewicht, dass der Kläger weder sein Facebook-Account gelöscht noch die

Telefonnummer gewechselt hat, denn dies ist mit erheblichen Einschnitten in sein Kontakt- und Sozialverhalten verbunden. Denn es ist nachvollziehbar, dass der Kläger mit dem Account und der aktuellen Nummer weiterhin seine Kontakte pflegen und erreichbar sein können möchte. Auch der Umstand, dass der Kläger die Voreinstellung „Alle“ in der Suchbarkeitseinstellung zur Telefonnummer - nach unbestrittener Angabe der Beklagten - bis heute nicht geändert hat, fällt insoweit nicht ins Gewicht. Denn die Beklagte hatte mitgeteilt, dass das sie die Funktion des CIT verändert habe und eine Suchbarkeit des Profils allein anhand der Telefonnummer nicht mehr möglich ist.

Bei der Bemessung der Schadensersatzhöhe hat das Gericht daneben auch die gesetzgeberisch beabsichtigte abschreckende Wirkung des Schadensersatzes bedacht. Andererseits hat es aber auch berücksichtigt, dass das Allgemeininteresse im Schwerpunkt nach Art. 83 DS-GVO durch die Verhängung von Bußgeldern gewahrt wird

ff) Der zuerkannte Zinsanspruch ergibt sich aus §§ 291, 288 Abs. 1 ZPO.

b) Antrag zu 2 - gerichtet auf Feststellung:.

Der Feststellungsantrag ist begründet. Es liegen die sachlichen und rechtlichen Voraussetzungen eines Schadensersatzanspruchs vor. Ein haftungsrechtlich relevanter Tatbestand, der zu möglichen künftigen Schäden führen kann, ist gegeben (vgl. BGH, Beschluss vom 09.01.2007 - VI ZR 133/06, Rn. 6, beck online). Es bedarf im Rahmen der Begründetheit keiner darüberhinausgehenden gewissen Wahrscheinlichkeit des Schadenseintritts, der aufgrund der neuen Sicherheitsmaßnahmen der Beklagten und des Zeitablaufs unwahrscheinlicher wird. Es reicht vorliegend bereits die nicht fernliegende Möglichkeit eines Schadens aus, die hier anzunehmen ist.

c) Anträge zu 3.a und 3.b gerichtet auf Unterlassung:

Die vom Kläger begehrten Unterlassungsansprüche sind unbegründet.

aa) Antrag zu 3.a:

Soweit der Kläger eine Unterlassung der vorstehenden Verarbeitung erwirken möchte, so-

lange die Beklagte nicht die nach dem Stand der Technik „*möglichen“* Sicherheitsmaßnahmen vorhält, ist der Antrag unbegründet. Es fehlt an einer Anspruchsgrundlage. Denn Art. 32 Abs. 1 und 2 DSGVO - auf den der Kläger sich berufen möchte - strebt eine Unterlassung der Verarbeitung an, soweit keine „geeigneten“ technischen und organisatorischen Maßnahmen bestehen, um ein dem Risiko *angemessenes* Schutzniveau zu gewährleisten. Aus Art. 32 Abs. 1 und 2 DSGVO folgt demnach keine Pflicht zu einem maximalen Schutz im Sinne des technisch Möglichen, sondern lediglich die Pflicht des Verantwortlichen, ein dem Risiko *angemessenes* Schutzniveau zu gewährleisten. Dabei liegt es im Ermessen des Verantwortlichen, aus der Vielzahl möglicher Maßnahmen, die das Risiko der Datenverarbeitung reduzieren können, konkrete Maßnahmen auszuwählen, durch die nach seiner Einschätzung ein angemessenes Schutzniveau erreicht wird (Jandt in Kühling/Buchner, a.a.O., DSGVO Art. 32 Rn. 8). Die Auswahl und Bestimmung der Angemessenheit erfolgt ausweislich Art. 32 Abs. 1 DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Dabei sind nach Art. 32 Abs. 2 DSGVO insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von personenbezogenen Daten bzw. durch unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Der Pflicht nach Art. 32 Abs. 1, 2 DSGVO ist mithin immanent, dass nicht alle technisch *möglichen* Maßnahmen zur Gewährleistung von Datensicherheit zu ergreifen sind, sondern nur solche, die unter Abwägung zwischen Schutzzweck und Aufwand unter Berücksichtigung der Art der Daten, dem Stand der Technik und den anfallenden Kosten als verhältnismäßig anzusehen sind (vgl. Mantz in Sydow/Marsch, a.a.O., DSGVO, Art. 32 Rn. 10). Denn die DSGVO verlangt keine Datensicherheit um jeden Preis und verpflichtet den Verantwortlichen nicht zu einem absoluten Schutz der personenbezogenen Daten, vielmehr muss das Schutzniveau dem jeweiligen Einzelfall angemessen sein, wobei Risiken nicht gänzlich ausgeschlossen werden können. Der Kläger kann daher allenfalls ein *angemessenes* Schutzniveau bzw. die Unterlassung einer Datenverarbeitung verlangen, so-

weit kein *angemessenes* Schutzniveau gewährleistet wird. Darauf, dass eines der Abwägungskriterien in den Vordergrund gestellt wird, hat der Kläger ebenso wenig Anspruch wie auf konkrete Maßnahmen (vgl. BGH, Urteil vom 22. Oktober 1976 — V ZR 36/75 —, BGHZ 67, 252-254, Rn. 11; ders. Urteil vom 17. Dezember 1982 — V ZR 55/82 —, Rn. 17, juris).

Da der Kläger trotz eines entsprechenden richterlichen Hinweises ausdrücklich erklärte, an dem ursprünglichen Klageantrag festhalten zu wollen, kommt eine Auslegung des Antrags nicht in Betracht.

bb) Antrag zu 3.b:

Soweit der Kläger mit dem Antrag zu 3 b) von der Beklagten auch verlangt, es zu unterlassen, seine Telefonnummer auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Contact-Import-Tools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird, kann dahinstehen, ob die Beklagte insoweit gegen die DSGVO verstoßen und den Kläger nicht ausreichend nach Art. 13, 14 DSGVO über die Nutzung der mitgeteilten Mobilfunknummer im Zusammenhang mit dem CIT informiert hat (s.a. LG Berlin, a.a.O. S. 25). Diese Pflichtverletzung löst nämlich für die Zukunft keine Folgen mehr aus, da der Kläger zumindest im Verlauf des Rechtsstreits sämtliche Informationen erhalten hat, die die fragliche Art und Weise der Datenverarbeitung betreffen (vgl. LG Paderborn, Urteil vom 19.12.2022 – 3 O 99/22 –, Rn. 167 - 168, juris). Hinzu kommt, dass die Verarbeitung nicht auf der Rechtsgrundlage einer wirksamen Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO stattfand, wovon der Antrag ausgeht. Die Gefahr der Wiederholung einer Verarbeitung der Telefonnummer „auf der Grundlage einer Einwilligung“ und ohne eindeutige Information besteht danach nicht (mehr).

d) Antrag zu 4 gerichtet auf Auskunft:

Der Auskunftsanspruch ist begründet. Dem Kläger steht der Auskunftsanspruch insoweit gemäß Art. 15, 12 Abs. 1 DSGVO zu. Er kann verlangen, dass ihm Auskunft über die ihn betreffenden Daten, die die Beklagte verarbeitet, erteilt wird (Art. 15 Abs. 1 Hs. 1, 2 DS-GVO).

Dieser Auskunftsanspruch ist nicht durch Erfüllung gem. § 362 Abs. 1 BGB erloschen. Der Beklagten ist allerdings zuzugeben, dass sie mit Schreiben vom 21.06.2021 sowie mit Schreiben vom 25.11.2021 dem Kläger mitteilte, welche personenbezogenen Daten nach ihrer Kenntnis Gegenstand des Scrapings waren und den Kläger zudem auf die Selbstbedienungstools sowie ihre Datenrichtlinie verwies. Ferner versicherte die Beklagte keine „Rohdaten“ des Scraping-Vorfalls vorzuhalten.

Dem Kläger ist jedoch bisher keine Auskunft über die von der Beklagten verarbeiteten Daten erteilt worden, sondern nur über die Daten, die nach Kenntnis der Beklagten durch den streitgegenständlichen Vorfall gescraped wurden. Eine solche Auskunftserteilung ist formlos möglich (Art. 12 Abs. 1 DSGVO), wobei die Auskunft in irgendeiner Weise zu fixieren ist (Quass in BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 44. Aufl. 2023, § 12 Rn. 27). Die Beklagte hat nicht dargelegt, dass sie dem Kläger alle seine von ihr verarbeiteten Daten mitgeteilt hat.

Der Verweis auf den Fernzugriff, nämlich das „Access your Information Tool“ kann hierfür nicht genügen. Ein solcher ist allerdings in dem 63. Erwägungsgrund der DSGVO als zusätzliche Möglichkeit für eine Auskunft oder eine zu erteilende Kopie gem. Art. 15 Abs. 3 DSGVO, die hier allerdings nicht verlangt wird, genannt, wenn es sicher ist und für den Verantwortlichen regelmäßig eine handhabbare Plattform zur Erfüllung der Pflichten der Beklagten u.a aus Art. 15 darstellt. Der Fernzugriff kann die Auskunft aber nur dann ersetzen, wenn der Betroffene hiermit einverstanden ist (vgl. Schmidt-Wudy in BeckOK-Datenschutzrecht, a.a.O., DSGVO Art. 15 Rn. 84). Ein solches Einverständnis hat, wie sich aus dem hiesigen Klagebegehren des Klägers gerichtet auf Auskunft trotz vorangegangenem Hinweis der Beklagten auf den Fernzugriff im Selbstbedienungstool ergibt, nicht erteilt (siehe dazu auch LG Berlin, a.a.O., S. 27). Insofern kann dahinstehen, ob der Fernzugriff den vorgenannten Anforderungen, insbesondere die Handhabbarkeit, entspricht.

Es kommt auch nicht darauf an, ob der Kläger diesen Auskunftsantrag bereits vorgerichtlich gestellt hat, denn jedenfalls folgt die Beklagte diesem im hiesigen Verfahren nicht, sondern beantragt, diesen zurückzuweisen.

Ds Gericht versteht den Antrag des Klägers unter Hinzuziehung seiner Begründung unter Auslegung seines Begehrens gem. §§ 133, 157 BGB so, dass er mit der Auskunft über alle personenbezogenen Daten, die die Beklagte von ihm verarbeitet erfüllt ist. Denn damit erlangt erletztlich alle Daten, die potentiell und nicht nur durch den streitgegenständlichen Scraping-Vorfall abgreifbar sind (s.a. LG, a.a.O., S. 26). Damit ist eine erläuternde Aufschlüsselung, wie im Antrag aufgeführt, in der Tenorierung nicht erforderlich.

e) Antrag zu 5 gerichtet auf Ersatz vorgerichtlicher Rechtsanwaltskosten:

Der Hauptantrag gerichtet auf Ersatz vorgerichtlicher Rechtsanwaltsgebühren als Schadensersatz war zurückzuweisen, weil der Kläger bereits nicht dargelegt hat, dass er diese beglichen hat und ihm daher insoweit ein Schaden entstanden ist.

Dem Kläger steht jedoch gegen die Beklagte der in der mündlichen Verhandlung hilfsweise beantragte Anspruch auf Freistellung von den vorgerichtlichen Anwaltskosten zu (Art. 82 Abs. 1 DSGVO).

Die betroffenen Personen sollen einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten, wobei nach den Erwägungsgründen eine weite Auslegung vorgenommen werden soll (s.o.), der Schadensersatz muss daher mehr als symbolisch sein (vgl. Bergt in Kühling/Buchner, a.a.O., DSGVO Artikel 82 Randnr 17 f.; Quaas in BeckOK Datenschutzrecht, a.a.O., DSGVO Art. 82 Rn. 29). Dazu kann auch der Ersatz vorgerichtlicher Rechtsanwaltskosten handeln (Quaas, a.a.O.). Der Prozessbevollmächtigte des Klägers ist hier zur Durchsetzung der Schadensersatzansprüche des Klägers gemäß der DSGVO und damit zur zweckentsprechenden Rechtsverfolgung tätig geworden und was angesichts der Komplexität des Datenschutzrechts auch verhältnismäßig war. Daher kommt es nicht mehr darauf an, ob die vorgerichtlichen Rechtsanwaltskosten auch aus Verzug gem. §§ 286 Abs. 1, 2 Nr. 3; 280 S. 1 und S. 2 BGB geltend gemacht werden können, wofür jedoch das Schreiben des jetzigen Prozessbevollmächtigten vom Mai 2021 (er-

wähnt in Anlage K2) sowie die E-Mail von 27.10.2021 mit Fristsetzung zur Zahlung des Schmerzensgeldes von 500,00 € bis zum 29.11.2021 (Anlage K1) sprechen.

Bei einem teilweisen Obsiegen kann der Kläger grundsätzlich die Rechtsanwaltskosten nur einfordern, soweit er mit dem vorgerichtlich geltend gemachten Anspruch später vor Gericht durchdringt (vgl. BGH, Urteil vom 18.07.2017 – VI ZR 465/16 –, Rn. 7, juris; BGH, Urteil vom 12.12.2017 – VI ZR 611/16 –, Rn. 5, juris). Vorliegend war er mit dem Klageantrag zu 1 teilweise und zwar in der vorgerichtlich durch seinen Anwalt geltend gemachten Höhe von 500 € erfolgreich. Zwar obsiegt er außerdem mit den Klageanträgen zu 2 und 4, allerdings wurde die Beklagte vorgerichtlich nicht aufgefordert, ihre Einstandspflicht für materielle zukünftige Schäden anzuerkennen und auch die Stellung eines dem hiesigen Auskunftsverlangen entsprechendes breites Auskunftsersuchen dargelegt, so dass insoweit keine vergütungspflichtige Tätigkeit entfaltet wurde. Der Freistellungsanspruch beläuft sich damit gem. § 13 Abs. 1 RVG i.V.m. Nrn. 2300, 7002, 7008 VV RVG auf die geltend gemachte 1,3 Geschäftsgebühr nebst Auslagenpauschale und Mehrwertsteuer bei einem Gegenstandswert von 500,00 €, mithin auf 90,96 € (1,3 Geschäftsgebühr i. H. v. 63,70 €; Auslagenpauschale 12,74 €; Umsatzsteuer: 14,53 €). Die Hinzuziehung eines Rechtsanwalts war zur effektiven Durchsetzung der Ansprüche aufgrund der Schwierigkeit der Sach- und Rechtslage auch geboten. Soweit anklingt, dass der Kläger rechtsschutzversichert ist, wird davon ausgegangen, dass der Kläger in Prozessstandschaft klagt, die die Beklagte auch nicht in Frage gestellt hat.

Nur klarstellend wird festgehalten, dass ein Anspruch auf Prozesszinsen insoweit nicht besteht und daher, so versteht das Gericht den Hilfsantrag, mit diesem auch nicht geltend gemacht werden. Gemäß den §§ 288 Abs. 1 Satz 1, 291 Satz 1 BGB sind nämlich nur Geldschulden zu verzinsen, zu denen ein Freistellungsanspruch nicht gehört (vgl. OLG Frankfurt, Urteil vom 20.12.2018 – 8 U 53/17 –, Rn. 96, juris, m.w.N.).

II. Kostenentscheidung

Die Kostenentscheidung beruht auf § 92 Abs. 1 S. 1 ZPO. Der Kläger obsiegt hinsichtlich des Streitwertes in Höhe von 4.050,00 € mit einem Wert von 1.550 €, nämlich hinsichtlich des Klageantrags zu Ziffer 1 (Schmerzensgeld) mit 500 €, des Klageantrags zu Ziffer 2

(Feststellung) vollständig (Wert 800,00 €) und hinsichtlich des Klageantrags zu Ziffer 4 (Auskunft) vollständig (Wert 250,00 €). Bei dem Klageantrag zu Ziffer 5 (vorgerichtliche Rechtsanwaltskosten) handelt es sich um Nebenkosten, die wertmäßig keine Berücksichtigung finden. Das Obsiegen entspricht insgesamt 37 % des Gesamtwertes des Rechtsstreits, so dass der Kläger 63 % der Kosten des Rechtsstreits zu tragen hat und die Beklagte die restlichen Kosten von 37 % trägt.

III. Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf den §§ 708 Nr. 11, 709 S. 1 und 2, 711 ZPO.

[redacted]
Vorsitzende Richterin am Landgericht

Verkündet am 03.08.2023

[redacted], JOSekr´in
als Urkundsbeamtin der Geschäftsstelle

Für die Richtigkeit der Abschrift
Berlin, 04.08.2023

[redacted], JOSekr´in
Urkundsbeamtin der Geschäftsstelle