– Beglaubigte Abschrift –

Landgericht Frankfurt am Main
Aktenzeichen:
2-27 O 194/22

Verkündet am: 04.08.2023

[redacted], Justizangestellte

_____

Urkundsbeamter(in) der Geschäftsstelle

Im Namen des Volkes

U r t e i l

In dem Rechtsstreit

[redacted]

- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte und Rechtsanwältinnen Wilde Beuger Solmecke Rechtsanwälte, Kaiser-Wilhelm-Ring 27 - 29, 50672 Köln
Geschäftszeichen: [redacted]

gegen

Meta Platforms Ireland Limited, v.d.d. GF Gareth Lambe u. Shane Crehan, 4 Grand Canal Square, Dublin 2

- Beklagte -

Prozessbevollmächtigte:
Rechtsanwälte und Rechtsanwältinnen Freshfields Bruckhaus Deringer, Bockenheimer Anlage 44, 60322 Frankfurt am Main

hat das Landgericht Frankfurt am Main – 27. Zivilkammer – durch die Vorsitzende Richterin am Landgericht [redacted] als Einzelrichterin auf die mündliche Verhandlung vom 28.07.2023 für Recht erkannt:

Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von 1000,00 € nebst Zinsen seit 15.12.2022 i.H.v. 5 Prozentpunkten über dem Basiszinssatz zu zahlen.

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

Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten i.H.v. 159,94 € zu zahlen zuzüglich Zinsen seit 15.12.2022 i.H.v. 5 Prozentpunkten über dem Basiszinssatz.

Im Übrigen wird die Klage abgewiesen.

Von den Kosten des Rechtsstreits haben der Kläger 81% und die Beklagte 19% zu tragen.

Das Urteil ist vorläufig vollstreckbar.
Die Beklagte darf die Vollstreckung gegen Sicherheitsleistung in Höhe von 110% des aus dem Urteil vollstreckbaren Betrages abwenden, wenn nicht der Kläger vor der Vollstreckung Sicherheit in Höhe von 110% des jeweils zu vollstreckenden Betrages leistet.
Der Kläger darf die Vollstreckung gegen Sicherheitsleistung in Höhe von 110% des aus dem Urteil vollstreckbaren Betrages abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110% des jeweils zu vollstreckenden Betrages leistet.

Tatbestand

Der Kläger macht gegen die Beklagte Ansprüche wegen Verstoßes gegen die DSGVO geltend.

Die Beklagte ist Anbieterin der Plattform facebook.com auf dem Gebiet der Europäischen Union. Zusätzlich bietet die Beklagte eine Messenger-App an. Die App und die gewöhnlichen Funktionen von facebook sind verknüpft über den Zugang zum selben Account.

Der Kläger nutzt die von der Beklagten betriebene Social Media Plattform. Die von der Beklagten auf der Seite angebotenen Dienste ermöglichen es Nutzer:innen, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. In dem von der Beklagten vorgegebenen Rahmen können die Nutzer:innen darüber entscheiden, welche anderen Gruppen von Nutzer:innen auf ihre Daten zugreifen können. Die Beklagte stellt hierzu Tools und Informationen zur Verfügung. Soweit keine individuellen Einstellungen gewählt werden, richtet sich die Einsehbarkeit der Informationen nach den Standard-Einstellungen, wobei eine Vielzahl von Einstellungsmöglichkeiten existiert.

Im hier maßgeblichen Zeitraum von Januar 2018 bis September 2019 waren Name der Nutzer:in, Geschlecht und Nutzer-ID als Informationen auf facebook stets erforderlich und öffentlich einsehbar. Die Angabe der Handynummer war hingegen freiwillig. In der Zielgruppenauswahl waren die Einstellungen vorhanden, die festlegten, wer einzelne Informationen im Profil einer Nutzer:in sehen kann. Bei dem Kläger war insoweit die Handynummer nicht öffentlich sichtbar. Weiterhin gab es Suchbarkeits-Einstellungen, die bestimmten, wer das Profil einer Nutzer:in anhand von bestimmten Informationen finden konnte. Hiernach war es potentiell möglich, Nutzer:innen anhand der Telefonnummer zu finden, wenn die Einstellung hierfür auf „alle“ gestellt war. Dies war bei dem Kläger der Fall, was der Standardeinstellung entsprach.

Anfang April 2021 wurden Daten von ca. 533 Mio. facebook-Nutzer:innen im Internet veröffentlicht. Es handelte sich um Telefonnummer, Nutzer-ID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus und ggf. weitere Daten. Auch Daten des Klägers wurden im Internet veröffentlicht.

Jedenfalls Name, Nutzer-ID und Geschlecht wurden aus dem Datenbestand von facebook „gescrapt“. Scraping bezeichnet grundsätzlich das massenhafte Sammeln von öffentlich verfügbaren Daten, wobei Funktionen einer Webseite verwendet werden, die für ordnungsgemäße Nutzer:innen entworfen wurden. Vorliegend wurde das facebook-Tool Kontakt-Importer sowie eine sog. Telefonnummernaufzählung verwendet. Mit der Kontakt-Importer-Funktion konnten Nutzer:innen ihre Kontakte von ihrem Mobilgerät auf facebook hochladen, um diese Kontakte auf der Plattform anhand der Telefonnummer zu finden und mit ihnen in Verbindung zu treten.
Die Scraper luden eine Vielzahl von Kontakten hoch, die mögliche Telefonnummern von Nutzer:innen der Beklagten enthielten, um so festzustellen, ob diese Telefonnummern mit einem facebook-Konto verbunden waren. Soweit dies der Fall war, wurden die einsehbaren Informationen aus dem betreffenden Nutzerprofil kopiert und die Telefonnummer hinzugefügt.

Die Beklagte informierte den Kläger zu keinem Zeitpunkt darüber, dass Informationen durch Dritte abgegriffen und veröffentlicht wurden. Auch die zuständige Datenschutzbehörde wurde nicht über den Vorfall informiert.

Mit anwaltlichem vorgerichtlichem Schreiben forderte der Kläger die Beklagte zur Zahlung von 500,00 € sowie zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft darüber auf, welche konkreten Daten abgegriffen und im April 2021 veröffentlicht wurden. Die Beklagte wies den Schadensersatzanspruch sowie den Unterlassungsanspruch zurück, räumte aber ein, dass unter den abgegriffenen und veröffentlichten Daten auch solche des Klägers waren. Weiterhin erklärte sich die Beklagte in ihrem Schreiben vom 14.1.2022 zu dem Auskunftsanspruch des Klägers (Anlage B 16).

Der Kläger behauptet, die gescrapten Daten seien nur zum Teil bei facebook öffentlich zugänglichen gewesen, namentlich hinsichtlich der Telefonnummer sei dies nicht der Fall gewesen. Die Telefonnummer habe wegen einer Sicherheitslücke bei der Beklagten mit den restlichen Personendaten korreliert werden können. Die Beklagte habe keinerlei Sicherheitsmaßnahmen vorgehalten, um ein Ausnutzen des bereitgestellten Kontakt-Importer-Tools zu verhindern. Die Zuordnung der Telefonnummer zu den weiteren Daten eröffne eine weite Bandbreite an kriminellen Möglichkeiten. Der Kläger erhalte seit dem Vorfall unregelmäßig Kontaktversuche von Unbekannten via SMS und E-Mail, die Nachrichten mit offensichtlichen Betrugsversuchen und potentiellen Virenlinks enthielten.
Bei der Messenger-App sei gesondert einzustellen, ob Telefonkontakte mit dem facebook-Dienst synchronisiert werden sollen.
Der Kläger ist der Auffassung, eine wirksame Einwilligung zur Verarbeitung seiner Daten fehle. Zudem habe die Beklagte nicht in ausreichendem Maße über die Verarbeitung der personenbezogenen Daten informiert bzw. aufgeklärt. Es sei nicht transparent, dass die Nutzer:in über die angegebene Nummer gefunden werden könne, auch wenn diese im Profil als „privat“ eingestellt sei. Es hätte auch auf die Risiken des Scraping hingewiesen werden müssen. Weiterhin habe die Beklagte die personenbezogenen Daten nicht in ausreichendem Maße geschützt. Es habe keine Sicherheitscaptchas und keinen Mechanismus zur Überprüfung der Plausibilität von Anfragen gegeben. Weiterhin verstoße die Beklagte mit ihren Einstellungen zur Privatsphäre gegen die Grundsätze von „privacy by design“ und „privacy by default“. Sie habe keine datenschutzfreundlichen Voreinstellungen bereitgehalten. Hierzu behauptet der Kläger, es sei mit hoher Wahrscheinlichkeit zu erwarten, dass Nutzer:innen die vor eingestellten Standardeinstellungen beibehalten. Schließlich habe die Beklagte gegen Art. 33 und 34 DSGVO verstoßen und sei dem Auskunftsersuchen des Klägers nach Art. 15 DSGVO nicht ausreichend nachgekommen.

Der Kläger beantragt,

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 1000,00 € nebst Zinsen seit Rechtshängigkeit i.H.v. 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, entstanden sind und/oder noch entstehen werden.
3. die Beklagte zu verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 €, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder ein an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu 6 Monaten, im Wiederholungsfall bis zu 2 Jahren, zu unterlassen,
    a. personenbezogene Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,
    b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Information 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 i.H.v. 887,03 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit i.H.v. 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte ist der Ansicht, die Anträge zu 1.-3. seien unzulässig. Sie seien zu unbestimmt. Bei dem Antrag zu 2. fehle zudem das Feststellungsinteresse.
Die Beklagte behauptet, sie stelle ihren Nutzer:innen umfassende Informationen über die Privatsphäre-Einstellungen zur Verfügung. Soweit Daten durch unbekannte Dritte von der facebook-Plattform abgerufen worden seien, sei dies im Einklang mit den jeweiligen Privatsphäre-Einstellungen geschehen. Die Telefonnummer sei dabei von den Scrapern zur Verfügung gestellt worden. Weiterhin habe sie zum maßgeblichen Zeitpunkt eine Übertragungsbegrenzung und Bot-Erkennung gehabt und Captcha-Abfragen genutzt. Im Nachgang zu dem Vorfall habe die Beklagte ihre Systeme so angepasst, dass das Verknüpfen von Telefonnummern mit bestimmten facebook-Nutzer:innen durch die Kontakt-Importer-Funktion nicht mehr möglich gewesen sei.
Die Beklagte ist der Ansicht, ihr sei kein Verstoß gegen die DSGVO vorzuwerfen. Sie sei nicht verpflichtet gewesen, die Vertraulichkeit von Informationen sicherzustellen, die nach dem Willen des Klägers hätten öffentlich sein sollen. Die Verarbeitung von Kontaktdaten wie der Telefonnummer sei erforderlich, um den Verarbeitungszweck, nämlich die Auffindbarkeit und Vernetzung, zu erreichen. Die Beklagte sei nicht verpflichtet gewesen, die personenbezogenen Daten nur einer möglichst geringen Zahl von Personen zugänglich zu machen. Es hätten ferner auch keine Meldepflichten bestanden.

Wegen des weiteren Vorbringens der Parteien wird auf die gewechselten Schriftsätze nebst Anlagen verwiesen.

Entscheidungsgründe

Die zulässige Klage ist teilweise begründet.

Zulässigkeit

Die Klage ist zulässig, insbesondere ist das angerufene Gericht wegen des klägerischen Wohnsitzes gemäß Art. 79 Abs. 2 S. 2 DSGVO und Art. 18 Abs. 1 2. Alt. EuGVVO international

und gemäß §§ 12, 13 ZPO örtlich zuständig. Das Gericht ist auch sachlich zuständig, da der Streitwert über EUR 5.000,00 liegt, §§ 23, 71 GVG.

Die Klageanträge sind insgesamt auch hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO. Auch das erforderliche Feststellungsinteresse für den Klageantrag zu Ziffer 2. liegt vor, § 256 ZPO.

Der Klageantrag zu 1. ist hinreichend bestimmt. Der Antrag auf Zahlung eines in das Ermessen des Gerichts gestellten unbezifferten Betrages begegnet angesichts des begehrten Ersatzes für immaterielle Schäden keinen Bedenken. Unter Hinzuziehung der Klagebegründung für die Auslegung des Antrages ist der Klagegegenstand auch hinreichend abgrenzbar. Der in Bezug genommene Lebenssachverhalt stellt die Anmeldung des Klägers auf facebook, die dabei erteilten Informationen, den in der Sache unstreitigen Scraping-Vorfall und die damit verbundenen Folgen dar. Der Kläger begehrt auf dieser Basis unter kumulativer Zusammenfassung der gerügten Verstöße und daraus resultierenden Folgen einen immateriellen Schadensersatz. Der in der Sache unstreitige Scraping-Vorfall stellt dabei den Kern des Streitgegenstands dar, der die verschiedenen vorgeworfenen DSGVO-Verstöße umklammert.

Auch der Antrag zu 2) begegnet keinen Bedenken. Es ist hinreichend bestimmt und verständlich gemacht, dass der Kläger Feststellung der Ersatzpflicht zukünftiger Schäden begehrt. Ein Missverständnis aus der Formulierung des Antrags – „entstanden sind“ –, wie es die Beklagte anführt, ist jedenfalls unter Berücksichtigung der Klagebegründung nicht zu befürchten. Zudem können hierdurch materielle Schäden umfasst sein, die bereits entstanden, jedoch dem Kläger noch nicht bekannt sind.

Das erforderliche Feststellungsinteresse gemäß § 256 Abs. 1 ZPO besteht auch. Ein solches ergibt sich bei der Geltendmachung möglicher zukünftiger Schäden bereits dann, wenn künftige Schadensfolgen - sei es auch nur entfernt - möglich, ihre Art, ihr Umfang und sogar ihr Eintritt aber noch ungewiss sind (OLG Düsseldorf, Urteil v. 08.05.2012 – 24 U 195/11). Die Möglichkeit eines Schadenseintritts ist nur zu verneinen, wenn aus der Sicht des Klägers bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines derartigen Schadens wenigstens zu rechnen (vgl. BGH, NJW 2001, 1431). Der Kläger hat hier hinreichend dargetan, dass sich aus dem Verlust persönlicher Daten in der Zukunft Vermögensschäden ergeben könnten, sollten Dritte mit den erlangten Daten missbräuchlich umgehen. Dass eine dahingehende Möglichkeit denkbar ist, entspricht allgemeiner Lebenserfahrung.

Die Klage ist auch bezüglich der Unterlassungsanträge zu 3.a) und b) hinreichend bestimmt. Ein Unterlassungsantrag muss so gefasst sein, dass der Streitgegenstand und der Umfang der Prüfungs- und Entscheidungsbefugnis des Gerichts klar umrissen sind, sich der Beklagte erschöpfend verteidigen kann und nicht im Ergebnis dem Vollstreckungsgericht die Entscheidung darüber überlassen bleibt, was dem Beklagten verboten ist (BGH NJW 2000,

3351). Dies ist vorliegend der Fall. Dem steht hinsichtlich des Antrag zu 3.a) nicht entgegen, dass der Kläger mit der Formulierung „nach dem Stand der Technik mögliche Sicherheitsmaßnahmen“ eine allgemein gehaltene Wendung benutzt. Dem Kläger ist eine spezifischere Benennung konkreter technischer Maßnahmen ersichtlich nicht möglich; es würde aber der Gewährung effektiven Rechtsschutzes widersprechen, würde ihm die Geltendmachung von dahingehenden Unterlassungsansprüchen unter Hinweis auf das Fehlen der Benennung konkreter technischer Vorgänge untersagt. Der Kläger müsste im Falle technischer Fortentwicklungen ansonsten seinen Unterlassungsantrag jeweils wiederholen, um Rechtsschutz zu erfahren.

Dem Kläger fehlt auch nicht das Rechtsschutzbedürfnis für den Unterlassungsantrag, da alleine die Veränderung der Privatsphäreeinstellungen des Klägers bei seinem facebook-Konto nicht gleichzusetzen ist mit der Implementierung technischer Vorkehrungen durch die Beklagte, Vorfälle wie den Streitgegenständlichen zu verhindern.

Auch der Unterlassungsantrag zu Ziffer 3.b) begegnet nach den vorstehenden Ausführungen keinen durchgreifenden Bedenken gegen die Bestimmtheit im Sinne des § 253 Abs. 2 Nr. 2 ZPO. Insbesondere werden die abstrakt gehaltenen Bestandteile („unübersichtlich“, unvollständig“) im Antrag nähergehend konkretisiert.

Begründetheit

Die Klage hat mit den Anträgen zu 1., 2. und 5. teilweise Erfolg, im Übrigen ist sie unbegründet.

Antrag zu 1.

Dem Kläger steht gegen die Beklagte ein Anspruch auf Schadensersatz nach Art. 82 Abs. 1 DSGVO in Höhe von 1000,00 € zu.

Nach Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen die Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen. Die Beklagte war Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO, da sie über die Zwecke und Mittel der stattgefundenen Verarbeitung der Daten des Klägers entschied.

Dem Kläger ist ein Schaden entstanden. Ihm ist zwar unstreitig bisher kein materieller Schaden entstanden, wohl ein immaterieller Schaden. Ein immaterieller Schaden liegt vor, wenn aufgrund eines Verstoßes gegen die DSGVO ein absolut geschütztes Rechtsgut der geschädigten Person verletzt wurde. Vorliegend wurde das allgemeine Persönlichkeitsrecht in der Ausprägung des Rechts auf informationelle Selbstbestimmung verletzt. Das Recht auf informationelle Selbstbestimmung enthält die Befugnis des

Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Dieses Recht des Klägers wurde verletzt. Die Daten des Klägers, insbesondere seine auf der Plattform der Beklagten nicht veröffentlichte Mobilnummer, wurden im Internet gemeinsam mit den Daten einer Vielzahl anderer Nutzer:innen der Beklagten veröffentlicht. Über diese Veröffentlichung, der aufgrund des Vorliegens eines „Datenpakets“ mit Daten vieler Personen ein höherer Nutzwert für kriminell handelnde Dritte zukommt, hatte der Kläger keine Kontrolle. Sie verletzt daher sein Recht auf informationelle Selbstbestimmung. Ob diese Verletzung „erheblich“ ist, ist nicht von Relevanz. Der Europäische Gerichtshof hat entschieden, dass keine Erheblichkeitsprüfung durchzuführen ist (EuGH, Urt. v. 4.5.2023 - C-300/21, juris).

Die Beklagte hat weiter gegen Bestimmungen der DSGVO verstoßen.

Die Beklagte hat gegen die DSGVO verstoßen, weil sie Daten des Klägers, namentlich seine Telefonnummer, ohne seine Einwilligung verarbeitet hat (so auch LG Lübeck CR 2023, 442, 444). Grundsätzlich gilt im Anwendungsbereich der DSGVO, dass jede Datenverarbeitung rechtswidrig ist, wenn nicht eine der in Art. 6 DSGVO genannten Bedingungen für eine rechtmäßige Datenverarbeitung erfüllt ist.
Es lag keine wirksame Einwilligung des Klägers nach Art. 6 Abs. 1a) DSGVO in die Nutzung seiner nicht öffentlich geteilten Mobilfunknummer für die Auffindbarkeit durch Dritte vor. Zwar war nach den vorhandenen Einstellungen im Profil des Klägers die Berechtigung der Beklagten gegeben, die Telefonnummer des Klägers für dessen Auffindbarkeit zu verwenden. Dies war jedoch nicht ausreichend, weil dies dem Kläger nicht zurechenbar war. Denn die entsprechende Einstellung war bei Bekanntgabe der Telefonnummer voreingestellt. Dem Kläger war es also lediglich möglich, die Voreinstellung nachträglich zu verändern und die Suchbarkeitsfunktion abzustellen. Eine solche Opt-out-Möglichkeit genügt jedoch für eine wirksame Einwilligung nicht (Sydow/Marsch DS-GVO/BDSG/Reimer, 3. Aufl. 2022, DS GVO Art. 6 Rn. 18 mwN). Denn es kann nicht ausgeschlossen werden, dass die Nutzer:innen die dem voreingestellten Ankreuzkästchen beigefügte Information überhaupt nicht zur Kenntnis genommen haben.
Die Funktion der Suchbarkeit des Profils durch Dritte anhand der Mobilfunknummer war auch nicht für die Erfüllung des zwischen den Parteien geschlossenen Vertrags erforderlich, Art. 6 Abs. 1b) DSGVO. Insoweit kann jedenfalls dann keine Erforderlichkeit im Sinne der DSGVO angenommen werden, wenn die konkret in Frage stehende Datenverarbeitung für die Erfüllung des konkreten Vertrages jedenfalls in keiner Weise notwendig, sondern allenfalls irgendwie „nützlich“ oder „dienlich“ ist (Kühling/Buchner, 3. Aufl. 2020, DS-GVO Art. 6 Rz. 42 mwN). Dies ist hier der Fall, da die Auffindbarkeit der jeweiligen Profile anhand der hinterlegten Mobilfunknummer für die Vertragsabwicklung

vorliegend allenfalls nützlich, keinesfalls aber notwendig war. Schon der bloße Umstand, dass die Nutzer:innen die fragliche Funktion in ihren Profileinstellungen deaktivieren konnten, ohne dass die Vertragsdurchführung hierdurch von auch nur einer der Parteien in Frage gestellt wurde, zeigt, dass es sich um eine möglicherweise praktische aber eben nicht notwendige Funktion handelt.
Dass eine Rechtmäßigkeit der Verarbeitung über Art. 6 Abs. 1c)-f) DSGVO vorläge, ist weder vorgetragen noch sonst ersichtlich.

Die Beklagte hat ferner gegen die Vorgaben zur Gewährleistung einer angemessenen Sicherheit bei der Verarbeitung der personenbezogenen Daten nach Art. 5 Abs. 1 f) DSGVO verstoßen. Diese erfordern geeignete technische und organisatorische Maßnahmen zum Schutz vor unbefugter und unrechtmäßiger Verarbeitung, wobei die Anforderungen in Art. 32 DSGVO festgelegt werden. Die Beklagte hat keine ausreichenden Maßnahmen getroffen.

Sie kann sich dabei zunächst nicht darauf berufen, sie sei zum Schutz der klägerischen Daten nicht verpflichtet gewesen, weil diese öffentlich verfügbar gewesen seien. Denn der Kläger macht vorliegend nicht geltend, die Beklagte habe ihn davor schützen müssen, dass seine Telefonnummer mit seinen sonstigen Daten durch Personen kombiniert wurde, denen zumindest seine Telefonnummer bekannt war. Vielmehr geht es darum, dass die Beklagte es (massenhaft) ermöglichte, hochgeladene Zahlenfolgen durch Zuordnung zu Nutzerkonten erst als Telefonnummer zu identifizieren und so weitere Daten der jeweiligen Nutzer:in zu erhalten und den Datensatz durch die Telefonnummer anzureichern. Für derartige Zwecke hatte der Kläger seine Mobilnummer nicht zu Verfügung gestellt und es oblag der Beklagten, die Daten des Klägers vor einem derartigen Risiko zu schützen.

Angesichts des Umstands, dass das Risiko von Scraping-Aktionen schon nach dem eigenen Vorbringen der Beklagten vergleichsweise hoch lag, da es sich um „gängige“ Techniken zur Datenabgreifung im Internet handele, und die Nutzung des Kontakt-Import-Tools einen simplen Mechanismus zur Auslesung durch automatisierte Verfahren darstellte, mussten die organisatorischen Verhinderungsmaßnahmen relativ stark ausgeprägt sein. Denn grundsätzlich gilt, dass je höher das Risiko und drohende Schäden sind, desto wirksamer müssen die Maßnahmen im Sinne des Art. 32 Abs. 1 DSGVO ausfallen (vgl. VG Mainz, Urteil v. 17.12.2020 – 1 K 778/19.MZ). Dabei fällt ins Gewicht, dass bei lebensnaher Betrachtung aus den durch Scraping-Vorfällen gewonnen Datensätzen durchaus erhebliche Risiken für Betroffene resultieren können, da sie für Identitätsbetrug, Phishing-Attacken oder sonstige vermögensgefährdende rechtswidrige Handlungen verwendet werden können. Die vorzunehmende Risikoabwägung musste im vorliegenden Fall daher insgesamt zur Gewährleistung eines hohen Schutzniveaus führen.

Dieses hohe Schutzniveau hat die Beklagte nicht gewährleistet. Hierzu hat der Kläger unter Hinweis auf verschiedene, von der Beklagten nicht getroffene Maßnahmen substantiiert vorgetragen. Der hierzu getätigte Sachvortrag der Beklagten, die eine sekundäre Darlegungslast trifft, vermag nicht zu belegen, dass hinreichende Maßnahmen zur Vermeidung von Scraping getroffen wurden.

Die Beklagte trägt zum Teil Mechanismen und Maßnahmen vor, die ersichtlich und/oder nach ihrem eigenen Vorbringen erst nach dem streitgegenständlichen Vorfall ergriffen wurden. Diese Umstände können daher nicht den Nachweis führen, dass zum streitgegenständlich entscheidenden Zeitpunkt erforderliche Einrichtungen vorhanden waren.

Soweit sie überdies auf Unterlassungsverfügungen oder gerichtliche Verfahren gegenüber Scrapern hinweist, betrifft dies keine präventiven Schutzmaßnahmen zur Verhinderung eines Vorfalls wie dem Streitgegenständlichen. Die Maßnahmen sind reaktiver Natur.

Auch der Vortrag zu dem Expertenteam der Beklagten, welches sich um die technischen Vorkehrungen kümmere und diese weiterentwickle, ist zu abstrakt und losgelöst von konkreten Schutzvorkehrungen zur Verhinderung von Scraping-Attacken über die Kontakt-Importer-Funktion im streitgegenständlichen Zeitpunkt.

Einzig relevant ist der Beklagtenvortrag, nach dem schon zum Zeitpunkt des hiesigen Scraping-Vorfalls alle seinerzeit technisch erforderlichen und möglichen Maßnahmen ergriffen worden seien, darunter insbesondere die vom Kläger monierten Mechanismen der Captcha-Abfragen oder Bot-Erkennungen sowie Übertragungsbeschränkungen. Auch dieses Vorbringen war jedoch zur Anspruchsverteidigung unzureichend. Es ist nicht hinreichend konkret, weil die technischen Maßnahmen nicht im Detail beschrieben werden. So fehlen etwa hinsichtlich der Übertragungsbeschränkungen konkrete Daten zu Höchstgrenzen und Zeitfenstern. Aus diesem Grund lässt sich die Geeignetheit der Maßnahmen nicht einschätzen. Hierzu korrespondiert, dass es keinen Vortrag dazu gibt, weshalb es trotz der angeblich implementierten Mechanismen dennoch zu dem streitgegenständlichen Scraping-Vorfall gekommen ist. Hiermit hätte sich die Beklagte jedoch konkret auseinandersetzen müssen und anhand der seinerzeit behauptetermaßen vorhandenen Techniken darlegen müssen, inwieweit diese umgangen werden konnten. Ohne eine solche Auseinandersetzung bleibt die Behauptung, man habe seinerzeit alle technisch erforderlichen Maßnahmen ergriffen, substanzlos, da sie das eigentliche Ereignis nicht erklären können.

Hinzu kommt, dass die Beklagte sich nicht dazu äußert, warum die im Nachgang implementierten Techniken nicht schon vor dem Vorfall vorhanden waren. Dies gilt etwa für die behauptete Einschränkung des Kontakt-Importer-Tools. Für die Beklagte lag das Risikopotenzial bei der Implementierung des Tools in Kombination mit den Grundeinstellungen zur Sucharbeit einer Nutzer:in über die Telefonnummer aus technischer Sicht, anders als für die individuellen Nutzer:innen, auf der Hand. Als „gängige Taktik“ war der Beklagten die

Scraping-Methodik auch bekannt. Die von ihr nun beschriebenen eingeleiteten Maßnahmen hätten ohne weiteres in technischer Hinsicht schon früher implementiert werden können. Dass sie technisch geeignet sind und ein risikoadäquates Schutzniveau gewährleisten würden, entspricht dabei gerade ihrem eigenen Vorbringen zu den nun ergriffenen Maßnahmen.

Die Beklagte hat schließlich gegen die Verpflichtung zur Vornahme datenschutzfreundlicher Voreinstellungen nach Art. 25 Abs. 2 DSGVO verstoßen. Hiernach hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Dies soll bewirken, dass ein Betroffener, der Voreinstellungen nicht ändert, vor einer unzulässigen oder ihn beeinträchtigenden Datenverarbeitung geschützt wird, die er durch Veränderung von Voreinstellungen hätte verhindern können (Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 25 Rn. 63). Dem hat die Beklagte keine Rechnung getragen. Durch die Voreinstellungen bei der Suchbarkeitsfunktion war vorgegeben, dass der Kläger über seine auf seinem Profil nicht öffentlich sichtbare Mobilnummer gesucht werden konnte. Für den Verarbeitungszweck erforderlich war dies nicht. Insoweit kann auf obige Ausführungen verwiesen werden.

Demgegenüber hat die Beklagte nicht gegen die Transparenzpflichten aus Artt. 5 Abs. 1 lit. a, 13, 14 DSGVO verstoßen. Nach 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. Die Aufklärung über die Zwecke der Verarbeitung muss insbesondere für die Nutzer:in klar verständlich und nachvollziehbar sein. Die Beklagte informiert die Nutzer:in über sämtliche Nutzungs- und Suchbarkeitsoptionen. So ist ausweislich der Anlage B 5 ein Hinweis zur Suchbarkeit über E-Mail-Adresse oder Handynummer sowie Änderungsmöglichkeiten erfolgt. Die Beklagte hat ihren Nutzer:innen – und damit auch dem Kläger – im streitgegenständlichen Zeitraum in ihrer Datenrichtlinie und dem Hilfebereich klare Informationen über die Verwendung der Daten und insbesondere der Verwendung der Telefonnummer. Dabei fand die Aufklärung über die Verwendung der Daten in verständlicher Sprache statt. Der Umstand, dass die seitens der Beklagten erteilten Informationen umfangreich sind, führt nicht zur Bewertung als unübersichtlich. In Anbetracht der Vorgaben der DSGVO und der damit verbundenen vielseitigen Informationsverpflichtungen liegt es in der Natur der Sache, dass eine Datenschutzinformation umfangreich ausfällt. Stellt der Betreiber einer Social-Media-Plattform den Nutzer:innen in Bezug auf die Verwendung ihrer Daten klar verständliche und nachvollziehbare Informationen über die Zugänglichkeit und über die Änderungsmöglichkeit von Suchbarkeitseinstellungen bereit, verletzt er die Transparenzpflichten nach Art. 5 Abs. 1 lit. a, Art. 13 und 14 DSGVO nicht. Es war auch nicht

erforderlich, über die Gefährlichkeit und Gefahren eines Scrapings zu informieren. Über Missbrauchsgefahren musste die Beklagte nicht aufklären, weil es sich hierbei um das allgemeine Lebensrisiko handelt, dass Daten, die man im Internet verwendet bzw. hochlädt, jederzeit missbraucht werden können.

Ob die Beklagte ihre Meldepflichten aus Art. 33, 34 DSGVO verletzt hat, kann offenbleiben. Denn ein etwaiger Verstoß der Beklagten könnte jedenfalls nicht haftungsbegründend sein. Es kann nicht festgestellt werden, dass die etwaige Verletzung dieser Pflichten für den geltend gemachten Schaden des Klägers überhaupt (mit-)kausal geworden ist und diesen zumindest vertieft hat. Vielmehr ist das streitgegenständliche Scraping der Daten mit der öffentlichen Einstellung der Daten im Internet erstmals offenbar geworden. Dass eine in der Folge unterlassene Information hierüber den damit bereits eingetretenen Schaden in Gestalt der Verletzung des allgemeinen Persönlichkeitsrechtes des Klägers konkret weiter vertieft hätte, lässt sich bei dieser Sachlage nicht feststellen. Insbesondere ist nicht ersichtlich, dass der Gefahr, dass die bereits rechtswidrig zirkulierenden Daten auch auf weiteren Seiten angeboten werden, zum Zeitpunkt der unterstellt unterlassenen Information überhaupt noch hätte begegnet werden können.

Auch ein möglicher Verstoß der Beklagten gegen die Auskunftspflicht nach Art. 15 DSGVO ist für den Schadensersatzanspruch nach Art. 82 DSGVO irrelevant. Es würde jedenfalls an der Kausalität des Verstoßes für den vermeintlichen Schaden in Gestalt der Datenveröffentlichung fehlen. Der Schaden liegt in einer rechtswidrigen Datenverarbeitung begründet, nicht jedoch in einer unterlassenen oder verspäteten Auskunft über die erhobenen Daten als solche.

Kausal für den Schaden des Klägers sind demgegenüber die rechtswidrige Verarbeitung der Telefonnummer des Klägers sowie die Verstöße der Beklagten gegen Artt. 25 Abs. 2, 32 DSGVO.
Hätte es die Beklagte unterlassen, die mangels Einwilligung rechtswidrige Funktion der Profilidentifikation anhand Telefonnummer für „alle“ zur Verfügung zu stellen, wäre es nicht zu dem Schaden gekommen.
Überdies war auch die Nichteinhaltung des Art. 32 Abs. 1 DSGVO ursächlich für den Schaden, da ein höheres angemessenes Schutzniveau zur Vermeidung von Scraping-Attacken eine solche bei praxisnaher Betrachtung und angesichts des Beklagtenvorbringens zu den von ihr im Nachgang zu diesem Vorfall ergriffenen Maßnahmen hätte vermeiden oder zumindest signifikant erschweren können.
Auch der Verstoß gegen Art. 25 Abs. 2 DSGVO ist ursächlich für den dem Kläger entstandenen Schaden geworden. Hätte die Beklagte die Voreinstellungen so vorgenommen, dass nicht oder nur durch „Freunde“ über die Telefonnummer gesucht werden kann, so wäre das Scraping mit

hoher Wahrscheinlichkeit verhindert worden. Denn es ist bei lebensnaher Betrachtung davon auszugehen, dass der Kläger die Voreinstellung nicht geändert hätte. Faktisch nehmen Nutzer:innen von Internetdiensten nur in geringem Umfang überhaupt Änderungen der Voreinstellungen vor (vgl. Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 25 Rn. 63).

Eine Haftungsbefreiung der Beklagten nach Art. 82 Abs. 3 DSGVO findet nicht statt. Dass die Beklagte in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist, ist nicht festzustellen. Erforderlich hierfür wäre der Nachweis der Beklagten, dass sie sämtliche Sorgfaltsanforderungen erfüllt hat und ihr nicht die geringste Fahrlässigkeit vorzuwerfen ist (vgl. Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 54 m.w.N.). Die konkrete Konfiguration der Voreinstellungen in den Profilen war ebenso wie die technischen Funktionen zur Nutzung der Mobilnummern von der Beklagten im Rahmen ihres Geschäftsbetriebes offenkundig bewusst wie geschehen verfasst. Insoweit liegt entsprechend zumindest Fährlässigkeit vor. Auch das Fehlen von ausreichenden technischen Schutzmechanismen begründet einen Fahrlässigkeitsvorwurf. Dabei fällt ins Gewicht, dass die Methode des Scrapings nach dem eigenen Beklagtenvorbringen eine „gängige Taktik“ zur Datenabgreifung darstellte, mithin im Wesentlichen bekannt war. Nutzen Dritte bereits erkannte oder erkennbare Angriffswege, um auf Daten zuzugreifen, kann die Nichtverantwortlichkeit des Verantwortlichen regelmäßig nicht nachgewiesen werden (Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 15).

Die Höhe des Schadensersatzes beziffert das Gericht mit 1000,00 €, wobei es diesen Betrag für angemessen, aber auch für ausreichend hält, um den immateriellen Schaden auszugleichen und gleichzeitig der erforderlichen Abschreckungswirkung Rechnung zu tragen sowie dabei die besonderen Umstände des Falles zu würdigen. Dem Gericht steht insoweit gemäß § 287 ZPO ein Ermessen zu. Das Gewicht der Rechtsverletzung sowie der objektive Umfang der Beeinträchtigung der betroffenen Person sind angemessen zu berücksichtigen (Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 82 Rn. 6). Danach ist einerseits in die Bemessung des Schadensersatzes mit einzubeziehen, dass der Beklagten mehrere Verstöße gegen die DSGVO vorzuwerfen sind, wobei aber jeweils kein Vorsatz festgestellt werden kann. Die Beeinträchtigung des Klägers selbst bewegt sich eher im Bagatellbereich. Dies schon deswegen, weil überwiegend ohnehin öffentlich einsehbare Daten über seine Person betroffen waren. Andererseits wurden diese Daten aber durch die Telefonnummer angereichert und sind aus diesem Grunde für kriminell agierende Personen von höherem Nutzwert. Auch werden Daten in einem umfangreichen Datenpaket eher Ausgangspunkt krimineller Aktivitäten sein als in einem Einzelkonto auf facebook veröffentlichte Daten. Berücksichtigt man diesen Aspekt sowie zusätzlich die

erforderliche Abschreckungswirkung des Schadensersatzes (Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 82 Rn. 6), erscheinen 1000,00 € angemessen.
Nicht in die Bewertung mit einzubeziehen war indes die Behauptung des Klägers, es sei vermehrt zu Kontaktversuchen via SMS und E-Mail durch unbekannte Dritte gekommen. Hierzu ist schon nicht feststellbar, dass es eine belastbare kausale Verknüpfung zum streitgegenständlichen Scraping-Vorfall gegeben hat.

Der Zinsanspruch resultiert aus §§ 291, 288 Abs. 1 BGB.

Antrag zu 2.

Der Kläger kann von der Beklagten auch die Feststellung der Ersatzpflicht für mögliche künftige Schäden verlangen. Die grundsätzliche Ersatzpflicht aus Art. 82 Abs. 1 DSGVO ist gegeben. Die für eine solche Feststellung erforderliche Möglichkeit künftiger Schäden, liegt gleichfalls vor (s.o.). Insbesondere sind künftige materielle Schäden nicht schlechterdings ausgeschlossen, sollte es in Zukunft zu einer vermögensgefährdenden oder -schädigenden Nutzung der gewonnenen Daten kommen.

Antrag zu 3.
Die Unterlassungsansprüche nach §§ 1004 Abs. 1 S. 2, 823 Abs. 1 BGB, §§ 1004 Abs. 1 S. 2, 823 Abs. 2 BGB i.V.m. DSGVO bzw. aus Art. 17 DSGVO sind unbegründet.

Der Anspruch auf Unterlassung im Hinblick auf die fehlende Vorhaltung unzureichender technischer Maßnahmen hinsichtlich der Software zum Importieren von Kontakten besteht nicht, weil es an der Wiederholungsgefahr fehlt. Die Wiederholungsgefahr ist materielle Anspruchsvoraussetzung für den Unterlassungsanspruch. Sie ist die auf Tatsachen gegründete objektive ernsthafte Besorgnis weiterer Störungen. Eine vorangegangene rechtswidrige Beeinträchtigung wie sie vorliegend erfolgt ist, begründet grundsätzlich eine tatsächliche Vermutung für das Bestehen einer Wiederholungsgefahr, an deren Widerlegung durch den Störer hohe Anforderungen zu stellen sind (siehe BGH NJW 2004, 3701). Diese hohen Anforderungen sind durch die Beklagte erfüllt. Denn eine Vermutung kann nur so lange gelten, wie der ihr zugrunde liegende Sachverhalt unverändert fortbesteht (OLG Schleswig Urt. v. 28.2.2012 – 11 U 64/10, BeckRS 2013, 3123). Der Sachverhalt hat sich jedoch hier maßgeblich geändert. Die Beklagte hat dargelegt, dass die Kontakt-Importer-Funktion maßgeblich dahingehend verändert wurde, dass sie die Suchbarkeit von Nutzer:innen anhand ihrer Telefonnummer auf facebook abgeschaltet habe. Der Kläger bestreitet dies zwar. Dieses Bestreiten ist jedoch nicht ausreichend. Der Kläger ist selbst facebook-Nutzer. Es ist ihm sowohl

möglich als auch zumutbar, nachzuvollziehen, ob und ggf. wie die Kontakt-Importer-Funktion auf facebook noch vorhanden ist.

Die Klage ist gleichfalls unbegründet im Hinblick auf einen Unterlassungsanspruch, der gerichtet ist auf ein Unterlassen der Datenverarbeitung ohne Erfüllung der Informationspflichten gemäß Art. 13, 14 DSGVO. Insoweit lag bereits kein Verstoß vor. Eine unübersichtliche und unvollständige Information durch die Beklagte über die Verarbeitung der Telefonnummer des Klägers ist nicht erfolgt, Insoweit kann auf die Ausführungen zum Antrag zu 1. verwiesen werden.

Antrag zu 4.

Die Klage ist hinsichtlich des geltend gemachten Auskunftsanspruchs gemäß Art. 15 DSGVO unbegründet, da dieser Anspruch durch die Beklagte bereits erfüllt worden ist, § 362 Abs. 1 BGB. Die Beklagte hat mit ihrem Schreiben vom 14.1.2022 die erforderlichen Auskünfte erteilt. Insbesondere wurde dem Kläger mitgeteilt, welche Daten betroffen sind und auf welche Weise es zu deren Abgriff durch unbekannte Dritte gekommen ist.

Ob die Auskunft inhaltlich richtig und vollständig ist, ist für die Erfüllungswirkung unerheblich. Erfüllt ist die Auskunft bereits dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Umfang darstellen.

Auskunft über die Identität der Scraper schuldet die Beklagte nicht. Denn bei diesen handelt es sich nicht um „Empfänger“ im Sinne von Artt. 15, 4 Nr. 9 DSGVO. Der Empfang von Daten ist auf Empfängerseite ein passiver Vorgang. Entsprechend ist Voraussetzung für die Empfängereigenschaft, dass personenbezogene Daten offengelegt werden (Kühling/Buchner/Hartung, 3. Aufl. 2020, DS-GVO Art. 4 Nr. 9 Rn. 5). Dies ist vorliegend jedoch nicht geschehen. Vielmehr haben die Scraper Daten abgeschöpft.

Antrag zu 5.

Der Kläger hat Anspruch auf Zahlung vorgerichtlicher Rechtsanwaltskosten in Höhe von 159,94 €. Der Kläger kann aufgrund von Art. 82 Abs. 1 DSGVO den Ersatz vorgerichtlich aufgewendeter Rechtsanwaltskosten zur Anspruchsdurchsetzung als Schaden geltend machen (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 19). Die Gebühr berechnet sich aus einem gegenstandswert von bis 1000,00 € für die geltend gemachte Schadensersatzzahlung von 500,00 € sowie den Auskunftsanspruch.

Nebenentscheidungen

Die Kostenentscheidung folgt aus § 92 Abs. 1 ZPO.

Der Ausspruch zur vorläufigen Vollstreckbarkeit hat seine Grundlage in § 708 Nr. 11, 711 ZPO.

[redacted]

Vorsitzende Richterin am Landgericht

Beglaubigt
Frankfurt am Main, 04.08.2023

[redacted]
Urkundsbeamtin der Geschäftsstelle