Landgericht Frankfurt am Main

Aktenzeichen: 2-18 O 114/22

Es wird gebeten, bei allen Eingaben das vorstehende Aktenzeichen anzugeben

Lt. Protokoll
verkündet am: 21.03.2023

[redacted], JAe
Urkundsbeamtin d. Geschäftsstelle

Im Namen des Volkes
Urteil

In dem Rechtsstreit

[redacted],

Kläger

Prozessbevollmächtigte: Rechtsanw. Wilde Beuger Solmecke, Kaiser-Wilhelm-Ring 27 - 29, 50672 Köln,
Geschäftszeichen: [redacted]

gegen

Meta Platforms Ireland LimitedFacebook Ireland Lt vertreten durch den Geschäftsführer (Director) Gareth Lambe, 4 Grand Canal Square, IRL Dublin 2,

Beklagte

Prozessbevollmächtigte: Rechtsanw. Freshfields Bruckhaus Deringer, Bockenheimer Anlage 44, 60322 Frankfurt am Main,
Geschäftszeichen: [redacted]

hat die 18. Zivilkammer des Landgerichts Frankfurt am Main
durch den Richter am Landgericht [redacted]
aufgrund der mündlichen Verhandlung vom 01.03.2023

für Recht erkannt:

Die Beklagte wird verurteilt, an den Kläger immateriellen Schadenersatz in Höhe von EUR 500,00 nebst Zinsen i.H.v. 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 17.9.2022 zu zahlen.

Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger 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.

Die Beklagte wird weiter verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000 €, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckende Ordnungshaft, oder an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu 6 Monaten, im Wiederholungsfall bis zu 2 Jahren, zu unterlassen, 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.

Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von EUR 627,13 nebst Zinsen i.H.v. 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 17. 9. 2022 zu zahlen.

Im Übrigen wird die Klage abgewiesen.

Die Kosten des Rechtsstreits werden gegeneinander aufgehoben.

Das Urteil ist für den Kläger hinsichtlich des Unterlassungsanspruchs gegen Sicherheitsleistung i.H.v. EUR 2.750,00, im Übrigen gegen Sicherheitsleistung i.H.v. 110 % des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

Tatbestand

Die Parteien streiten um mögliche Verstoße gegen die Datenschutzgrundverordnung durch die Beklagte im Zusammenhang mit der Nutzung der Social-Media-Plattform Facebook.

Die Beklagte ist ein international tätiges Unternehmen, das im Raum der Europäischen Union die Social-Media-Plattform www.facebook.com betreibt, auf der Nutzer mit anderen Nutzern u.a. kommunizieren und Fotos oder sonstige Beiträge miteinander teilen können. Auf der Website oder über eine Applikation können Nutzer persönliche Profile erstellen und diese mit Freunden teilen, wobei die persönlichen Profile je nach individueller Nutzereinstellung Angaben zu verschiedenen personenbezogenen Daten wie Name, Adresse, Geschlecht, Wohnort oder Geburtsdatum enthalten können. Die Plattform wird weltweit von etwa 2,5 Milliarden Menschen genutzt.

Die Beklagte ermöglicht es den Nutzern, bei der Registrierung und während der weiteren Nutzung darüber zu entscheiden, welche anderen Nutzer auf solche Daten zugreifen, d.h. diese einsehen können, z.B. ob der Zugriff auf als „Freunde“ kategorisierte Nutzer beschränkt oder für alle Nutzer sichtbar sein soll (sog. Zielgruppenauswahl). Dabei sehen die von Facebook vorgegebenen Standardeinstellungen ohne individuelle Anpassung grundsätzlich vor, dass alle anderen Nutzer von Facebook die jeweils vom Nutzer in seinem Profil offenbarten Daten einsehen können. Der Name, das Geschlecht und die Nutzer-ID sind stets öffentlich einsehbar, ohne dass ein Nutzer dies individuell verändern könnte. Die Telefonnummer eines Nutzers wird standardmäßig nicht als öffentlich einsehbar behandelt.

Daneben gibt es für Nutzer eine gesonderte „Suchbarkeitseinstellung“, mit der sie festlegen können, ob sie bzw. ihr Facebookprofil von anderen etwa über ihre Mobiltelefonnummer gefunden werden können. Grundsätzlich kann das Profil eines Nutzers dadurch z.B. anhand seiner angegebenen Telefonnummer gefunden werden, auch wenn der Nutzer die Telefonnummer bei der gesonderten Zielgruppenauswahl nicht für alle freigegeben hat. Diese Suchbarkeitseinstellung über die Telefonnummer ist standardmäßig auf „für alle“ suchbar eingestellt. Diese Einstellung konnte gesondert für bestimmte Zielgruppen eingeschränkt werden; ab Mai 2019 stand hierfür auch die Option „nur ich“ – also ein faktischer Ausschluss der Suchbarkeit – zur Verfügung. Die Standard-Suchbarkeitsoption war im streitgegenständlichen Zeitraum beim klägerischen Facebookprofil nicht individuell verändert worden.

Die individuellen Einstellungen zu der Sichtbarkeit persönlicher Daten und Suchbarkeit des Profils u.a. über die Mobilnummer können Nutzer im Rahmen des Anmeldeprozesses auf Facebook oder jederzeit im weiteren Verlauf individuell einstellen oder ändern. Nutzer werden zudem auf die Datenrichtlinie hingewiesen, für deren Inhalt auf Anlage B9 verwiesen wird; zudem wird ein „Hilfebereich“ zur Verfügung gestellt, der diverse Informationen über die Privatssphäreeinstellungen und Nutzung der Plattform enthält, für deren Inhalt auf Anl. B1 bis B8 sowie B19 und B20 verwiesen wird.

Facebook bietet zudem eine sog. Kontakt-Importfunktion an, mithilfe derer Nutzer ihre Kontakte von ihren jeweiligen Mobilgeräten auf Facebook hochladen können, um diese Kontakte auf der Facebook-Plattform zu identifizieren und mit Ihnen in Verbindung zu treten. Zweck dessen ist es, dass ein Nutzer auf Facebook schnell mit seinen persönlichen Kontakten entsprechend seines Handy-Adressbuchs verknüpft werden kann. Dabei kommt es zu einer Identifizierung von Facebookprofilen über die Telefonnummer, ohne dass die im Profil hinterlegte Nummer im Rahmen der Zielgruppenauswahl für die Öffentlichkeit freigegeben sein musste; für diese Verknüpfung greift nicht die Zielgruppenauswahl, sondern die Einstellungen zur Sucharbeit des Nutzers über seine Mobilnummer.

Die Beklagte bietet auch einen Facebook-Messenger-Dienst an. Hier können sich Facebooknutzer gegenseitig Nachrichten schreiben.

Zu einem nicht näher feststellbaren Zeitpunkt im Jahr 2019 kam es auf Facebook zu einem sog. „Datenscraping-Vorfall“, also einem massenhaften und automatisierten Abgreifen und Sammeln persönlicher Daten von Facebook-Nutzern durch unbekannte Dritte. Beim Scraping werden im Allgemeinen vornehmlich öffentlich einsehbare Daten und Informationen von Internetseiten mittels Softwareprogrammen massenhaft eingesehen und gesammelt und zu Datensätzen zusammengefügt. Die Beklagte untersagte solche automatisierten Datensammlungen in ihren Nutzungsbedingungen.

Ursache und Ansatzpunkt des Scraping-Vorfalls bei Facebook war nach allgemeinem Verständnis – wobei Details und Einzelheiten zwischen den Parteien streitig sind –, dass unbekannte Dritte über die Nutzung der vorbeschriebenen Kontaktimport-Funktion Kontakte hochgeladen haben, welche mögliche Telefonnummern von Nutzern enthielten, um festzustellen, ob diese Nummern mit einem Facebook-Konto verbunden sind. Soweit sie feststellen konnten, dass eine Nummer mit einem Facebook-Konto verknüpft war, weil es dessen Sucharbeitseinstellung entsprechend erlaubt hatte, haben die Scraper jedenfalls die öffentlich einsehbaren Informationen auf dem jeweiligen Profil, abhängig von der Zielgruppenauswahl des Nutzers, exportiert und auf diese Weise die im Einzelfall ggf. nicht öffentlich freigegebene Telefonnummer eines Nutzers mit dessen öffentlich einsehbaren Daten zusammengebracht.

Die auf diese Weise gewonnen Daten wurden durch unbekannte Dritte im Internet veröffentlicht, wobei eine Vielzahl von Facebook-Nutzern und deren Datensätze betroffen waren. Umfasst waren z.B. Telefonnummer, Facebook-ID, Name oder Geschlecht. Die Beklagte gab daraufhin am 6.4.2021 einen Artikel heraus, in dem sie auf den Vorfall einging. Für den genauen Inhalt wird auf Anlage B10 verwiesen.

Die Beklagte informierte die zuständige Datenschutzbehörde hierüber nicht gesondert. Die irische Datenschutzbehörde erließ am 28.11.2022 eine Geldbuße in Höhe von EUR 265 Mio. wegen der streitgegenständlichen Scraping-Vorfälle gegen Facebook. Für den genauen In-

halt der Entscheidung wird auf Anlage K3 verwiesen. Die Entscheidung ist noch nicht rechtskräftig.

Der Kläger wandte sich mit vorgerichtlichem rechtsanwaltlichem Schreiben vom 2.6.2021 an die Beklagte und forderte sie wegen des Scraping-Vorfalls zur Zahlung von EUR 500,00 Schmerzensgeld nach Art. 82 Abs. 1 DSGVO auf. Hierauf antwortete die Beklagte mit Rückschreiben vom 30.8.2021. Für den genauen Inhalt der Schreiben wird auf Anl. K1 (Bl. 53 ff. d.A.) sowie auf Anlage B16 verwiesen. Hierin teilte die Beklagte unter anderem mit, dass nach ihren Informationen bei den von Scrapern abgerufenen Daten des Klägers jedenfalls dessen Nutzer-ID, Vor- und Nachname sowie Land, Geschlecht und Telefonnummer betroffen waren.

Der Kläger ist der Ansicht, die Beklagte habe gegen diverse Pflichten aus der DSGVO verstoßen und schulde ihm daher Schadensersatz nach Art. 82 Abs. 1 DSGVO. Im Übrigen nimmt er sie auf Unterlassung, Feststellung weitergehender Ersatzpflichten, Auskunft und Zahlung der vorgerichtlichen Rechtsanwaltskosten in Anspruch.

Er behauptet, von dem Scraping-Vorfall betroffen gewesen zu sein, da persönliche Daten von ihm wegen des Vorfalls nun im Darknet für jedermann abrufbar seien, wobei zusätzlich auch seine E-Mail-Adresse, der Wohnort, Geburtsdatum, Stadt und Beziehungsstatus des Klägers offenbart worden seien. Die im Rahmen von Scraping-Attacken gewonnenen Datensätze würden typischerweise und so auch hier von Dritten etwa zur Verwendung von Internetbetrügereien oder sog. „Phishing Attacken“ genutzt.

Er behauptet weiter, die Beklagte habe keine oder unzureichende Sicherheitsmaßnahmen vorgehalten, um ein unbefugtes Ausnutzen des bereitgestellten Kontaktimporttools zu verhindern. Die Beklagte habe insbesondere keine sog. „Sicherheitscaptchas“ (zur Erkennung automatisierter Abrufe) und keinen Mechanismus zur Überprüfung der Plausibilität von Anfragen implementiert. Derartige oder andere Vorkehrungen seien aber technisch möglich und auch erforderlich gewesen.

Er behauptet weiter, die Einstellungen zur Sicherheit der Telefonnummer auf Facebook seien (bewusst) so undurchsichtig gestaltet, dass Nutzer keine datensichere Einstellung erreichen könnten. Insbesondere die getrennte Behandlung der Suchbarkeitseinstellung hinsichtlich der hinterlegten Telefonnummer sei irreführend und würde regelmäßig dazu führen, dass Benutzer es bei der Standardeinstellung der allgemeinen Suchbarkeit belassen würden. Über die Verknüpfungsmöglichkeit zwischen Telefonnummer und Facebookprofil unter Ausnutzung des Kontaktimporttools sei er nicht bzw. unzureichend informiert worden. Zudem würden die von Facebook vorgegebenen Standardeinstellungen zum Datenschutz generell gegen das Prinzip „privacy by default“ verstoßen. Dies gelte auch bezüglich der Messenger-App, in Bezug auf die der Kläger behauptet, die dort getroffenen Nutzereinstellungen würden unabhängig von den Einstellungen auf der Facebook-Plattform funktionieren. Schließlich

habe die Beklagte auch gegen die Pflicht zur unverzüglichen Information der zuständigen Aufsichtsbehörde verstoßen.

Der Kläger behauptet sodann, ihm sei aufgrund des Scrapings ein kausaler Schaden entstanden; der erlittene Kontrollverlust über seine Daten habe ihn nämlich in einen Zustand großen Unwohlseins und großer Sorge versetzt, der sich in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern niederschlage. Der Kläger erhalte außerdem seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail, bei denen es sich um offensichtliche Betrugsversuche oder um Virenlinks handele. Er behauptet, er hätte seine Telefonnummer in Kenntnis der Umstände nicht angegeben bzw. nicht als „suchbar“ für alle eingestellt.

Der Kläger beantragt,

1. die Beklagte zu verurteilen, an den Kläger immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1000 € nebst Zinsen seit Rechtshängigkeit i.H.v. 5 Prozentpunkten über dem Basiszinssatz;

2. festzustellen, dass die Beklagte verpflichtet ist, dem Kläger 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 €, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckende Ordnungshaft, oder an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu 6 Monaten, im Wiederholungsfall bis zu 2 Jahren, zu unterlassen,

   a) personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

   b) die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Information darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht ex-

plizit hier für 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 durch 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 vorgerichtlicher 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 Klage sei bereits unzulässig, weil die Klageanträge unbestimmt seien und das Feststellungsinteresse fehle.

Sie ist weiter der Ansicht, ein Verstoß gegen die DSGVO im Zusammenhang mit dem Scraping-Vorfall liege bereits deshalb nicht vor, weil sich das Scraping auf ohnehin öffentlich einsehbare Daten im Rahmen der Nutzung des Facebookprofils beziehe. Sie behauptet, Scraping nutze letztlich nur die normalen Benutzerfunktionen aus und sei nicht vollständig zu verhindern. Im Übrigen meint sie, die vermeintlichen Verstöße seien nicht von Art. 82 DSGVO erfasst; jedenfalls könne sie sich über Art. 82 Abs. 3 DSGVO exkulpieren.

Hinsichtlich der technischen Schutzanforderungen gegen Scraping behauptet sie, im Einklang mit der Marktpraxis während des relevanten Zeitraums über Übertragungsbegrenzungen sowie Bot-Erkennung verfügt zu haben. Zu den vorhandenen Schutzvorkehrungen hätten auch die von der Klägerseite genannten Mechanismen gehört. Diese Methoden würden ständig weiterentwickelt werden; man habe beim Kontaktimporttool etwa nach dem Vorfall einen sog. „Social Connection Check“ eingeführt sowie eine „Menschen, die Du kennen könntest“-Funktion zur Absicherung eingeführt. Zuletzt sei es auch zu generellen Einschränkung der Nutzung der Kontaktimporttechnik gekommen. Zudem würde die Beklagte mittels Unterlassungsaufforderung, Kontosperrungen und Gerichtsverfahren gegen Scraper vorgehen.

Entscheidungsgründe

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

I.

Die Klage ist zulässig, insbesondere ist das angerufene Gericht wegen des klägerischen Wohnsitzes gem. Art. 79 Abs. 2 S. 2 DSGVO international und sodann gem. §§ 12, 13 ZPO örtlich zuständig. Das Gericht ist auch sachlich zuständig, da der Streitwert über EUR 5.000,00 liegt, §§ 23, 71 GVG. Dabei werden der Klageantrag zu Ziffer 1.) entsprechend der klägerischen Bezifferung auf EUR 1.000,00 und der flankierende Feststellungsantrag hinsichtlich zukünftiger Schäden mit 20% des Hauptantrags, also auf weitere EUR 200,00 festgesetzt. Die Unterlassungsansprüche werden im Einklang mit § 23 Abs. 3 S. 2 RVG mit EUR 5.000,00 bewertet. Der Auskunftsanspruch gem. Klageantrag zu Ziffer 4.) bezieht seinen wirtschaftlichen Wert typischerweise daraus, dass mit ihm die Durchsetzung eines Hauptanspruchs vorbereitet werden soll. Der wirtschaftliche Zweck des Auskunftsverlangens besteht im Allgemeinen darin, eine der Grundlagen zu schaffen, die für den Anspruch auf die Hauptleistung erforderlich sind. Da die Auskunft die Geltendmachung des Leistungsanspruchs erst vorbereiten und erleichtern soll, beträgt der Wert des Auskunftsanspruchs in der Regel einen Bruchteil, nämlich 1/10-1/4 des Leistungsanspruchs (BGH NJW-RR 2018, S. 1265). Vor dem Hintergrund, dass die Auskunft in Zusammenhang mit den klägerischen Zahlungs- und Feststellungsanträgen zu Ziffern 1.) und 2.) zu verstehen ist, sind 10% ihres Wertes, also weitere EUR 120,00 festzusetzen. Daraus ergibt sich insgesamt ein Zuständigkeitsstreitwert von EUR 6.320,00.

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, durch den dieser hinreichend abgegrenzt wird und der die verschiedenen vorgeworfenen DSGVO-Verstöße umklammert. Entgegen der Auffassung der Beklagten sind aus diesem Grund nicht mehrere Streitgegenstände zu erkennen.

Auch der Antrag zu 2) begegnet vor diesem Hintergrund keinen Bedenken. Es ist hinreichend bestimmt und verständlich gemacht worden, 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 gem. § 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, S. 1431). Der Kläger hat hier hinreichend dargetan, dass sich aus dem Verlust persönlicher Daten in der Zukunft womöglich Vermögensschäden ergeben könnten, sollten Dritte mit den erlangten Daten missbräuchlich umgehen. Dass eine dahingehende Möglichkeit bei der Abgreifung personenbezogener Daten durch Dritte und deren Veröffentlichung im Internet 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, S. 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. Es obliegt im Übrigen gerade der Beklagten, die technisch erforderlichen Maßnahmen zu eruieren und zu implementieren. Dies kann nicht über die Formulierung des Unterlassungsbegehrens auf den Kläger abgewälzt werden.

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 eigens 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.

II.

Die Klage ist in dem aus dem Tenor ersichtlichen Umfang begründet. Der Kläger hat gegen die Beklagte einen Anspruch auf Schadensersatz gemäß Art. 82 Abs. 1 DSG VO i.H.v. EUR 500,00 und kann die begehrte Feststellung der Ersatzpflicht für weitere künftige Schäden verlangen. Zudem hat er Anspruch auf Unterlassung in dem aus dem Tenor ersichtlichen Umfang. Im Übrigen ist die Klage unbegründet.

1.

Der Kläger hat Anspruch gegen die Beklagte auf Ersatz seines immateriellen Schadens i.H.v. EUR 500,00 gemäß Art. 82 Abs. 1 DSGVO. Der für die Haftung erforderliche Verstoß gegen die DSGVO bei der Verarbeitung von Daten des Klägers durch die Beklagte und ein darauf beruhender kausaler Schaden des Klägers, von deren Haftung sich die Beklagte nicht gemäß Art. 82 Abs. 3 DSGVO exkulpieren kann, liegen vor.

a.

Die Beklagte ist für diesen Anspruch passivlegitimiert, da sie im Sinne des Art. 82 Abs. 2 S. 1 DSGVO die für die Verarbeitung personenbezogener Daten des Klägers Verantwortliche war. Dies ist gemäß Art. 4 Nr. 7 DSGVO u.a. eine juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, was die Beklagte als Anbieterin der streitgegenständlichen Social-Media-Plattform gewesen ist.

Eine Verarbeitung personenbezogener Daten lag ebenso vor. Bei den im hiesigen Fall zumindest betroffenen Informationen über den Kläger in Gestalt von Handynummer, Name, Facebook-ID und Geschlecht handelt es sich um personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO. Eine Verarbeitung ist gem. Art. 4 Nr. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Die Anmeldung, Registrierung und Speicherung der klägerischen Daten sowie deren Verwendung im Rahmen der Nutzung der Facebook-Plattform und des Kontaktimporttools stellen eine solche Verarbeitung dar.

b.

Die Beklagte hat bei der Verarbeitung der klägerischen Daten zur Überzeugung des Gerichts diverse Verstöße gegen die DSGVO begangen.

aa)

Die Beklagte hat gegen Art. 13 Abs. 1 lit. c) DSGVO verstoßen. Hiernach sind bei Erhebung personenbezogener Daten zum Zeitpunkt der Erhebung der betroffenen Person unter anderem die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, mitzuteilen. Dies soll dem Betroffenen ermöglichen, nicht nur über den Verarbeitungsvorgang als solchen informiert zu werden, sondern auch die Zwecke der Erhebung nachzuvollziehen. Gegen diese umfassende Informations- und Aufklärungspflicht hat die Beklagte bei der Erhebung und Verarbeitung der klägerischen Daten verstoßen, da sie den Kläger n cht bzw. nicht hinreichend über die Verwendung seiner Mobilnummer für das Kontaktimporttool aufgeklärt hat.

Für den Kläger war angesichts der in Anlagen B1 bis B9 dargelegten Informationen zwar – insoweit suffizient – ersichtlich und nachvollziehbar, dass sein Facebookprofil und damit auch die dort freigegebenen persönlichen Daten über seine Mobilfunknummer auffindbar sein würden, auch wenn die Nummer selbst nicht Teil der auf dem Profil veröffentlichen Daten war und sein musste; er wurde hierdurch grundsätzlich hinreichend darüber in Kenntnis gesetzt, dass er auch ohne veröffentlichte Mobilnummer über diese von anderen Nutzern gesucht werden kann, solange und soweit er die Einstellungen zur „Suchbarkeit“ über die Mobilnummer nicht abändern würde.

Allerdings fehlte eine verständliche Information darüber, dass die Mobilnummer konkret auch im Rahmen des Kontaktimporttools der Beklagten verwendet wird und Dritten somit eine Synchronisation von ihren im Mobiltelefon gespeicherten Telefonkontakten mit Facebookprofilen möglich war. Damit fehlte es zwangsläufig auch an einer Aufklärung darüber, dass auf diese Weise die Verknüpfung der nicht öffentlich gemachten Mobilfunknummer mit dem (öffentlichen) Facebookprofil auf automatisierte Weise bei Nutzung des Kontaktimporttools ermöglich wurde.

Auch wenn der dem zugrundeliegende Mechanismus der theoretisch herstellbaren Verknüpfung der eigentlich nicht auf dem Nutzerprofil freigegebenen Mobilnummer mit dem jeweiligen Profil grundsätzlich, wie beschrieben, erkennbar war aufgrund der Erläuterungen zu den Einstellungen zur Suchbarkeit des Profils, so hätte es hinsichtlich der Nutzung und Implementierung des Kontaktimporttools eines konkreten zusätzlichen Hinweises an den Kläger bedurft.

Dies gründet darin, dass mit der Verwendung der Importtechnik eine automatisierte Möglichkeit der Verknüpfung von Mobilnummer und Profil geschaffen wurde, die eine missbräuchliche, zumindest unbefugte Verwendung durch Dritte im Rahmen eines maschinellen Verfahrens – wie geschehen – erheblich und in signifikantem Ausmaße vereinfachte und die Gefahr eines möglichen Kontrollverlusts über die Daten auf diese Weise spürbar steigerte. Aus der Sicht eines durchschnittlichen Nutzers lag es nahe, die Verwendung der Suchbarkeitsoption nur als eine solche zu verstehen, die durch Individualpersonen, die dem Nutzer grundsätzlich im weiteren Sinne bekannt, jedenfalls aber

aus nachvollziehbaren Verbindungen heraus im Besitz seiner Mobilnummer sind, genutzt werden würde, indem diese im Rahmen eines Einzelvorgangs die Mobilnummer in eine Suchmaske eingeben, um einen Kontakt auf Facebook herzustellen. Dagegen handelt es sich bei der Verwendung der Mobilnummer im Rahmen des Kontaktimporttools um eine automatisierte Abgleichung von (beliebigen) Mobilnummern aus einem Handyadressbuch mit möglichen Facebookprofilen. Dieser Vorgang war und ist geeignet, dem Betroffenen die Übersicht und Kontrolle über die Weitergabe und Verwendung seiner Daten in erhöhtem Maße zu nehmen oder diese zumindest zu erschweren, und bot Dritten ein Einfallstor an, auf einfachste Weise über Softwareprogramme zweckwidrig umfangreiche Datensätze zu erstellen.

Eine solche Verwendung der Mobilnummer musste sich einem Nutzer des Dienstes der Beklagten auch nicht ohne weiteres aufdrängen, insbesondere musste er auf Basis des Mechanismus der grundsätzlichen Suchbarkeit über die ggf. nicht eigens veröffentlichte Mobilnummer nicht auf eine solche automatisierte Abgleichungsmöglichkeit im Rahmen des Kontaktimporttools und die damit einhergehende auf der Hand liegende Missbrauchsgefahr schließen. Das auch bei Individualnutzung der Suchbarkeitsoption grundsätzlich vorhandene Risiko des unbefugten Abgleichens beliebiger Mobilnummern über die Suchmaske wurde gerade durch die Automatisierung im Rahmen des Kontaktimporttools gesteigert und die damit verbundene Missbrauchsgefahr entscheidend geprägt. Die Beklagte hätte jedoch ohne Weiteres Informationen über das ihr seinerzeit bereits bekannte „gängige“ Verfahren des unbefugten Scrapings durch Dritte mitteilen können, um dem Nutzer die Tragweite der Folgen der automatisierten Synchronisation von Telefonnummer und Facebookprofil zu offenbaren. Damit war den Nutzern eine fundierte Risikoabschätzung hinsichtlich der Möglichkeiten – und Missbrauchsgefahren – des automatisierten Abgleichs von Mobilnummern mit Facebookprofilen im Rahmen des Kontaktimporttools nicht möglich.

Dem steht nicht entgegen, dass durch das Scraping womöglich nur diejenigen Daten zusammengestellt werden, die der betroffene Nutzer ohnehin auf seinem Profil freigegeben hat und im Hinblick auf die sich daher nur ein allgemeines Lebensrisiko verwirklicht. Denn Kernpunkt der Verletzung der Informationspflicht der Beklagten ist die durch das Kontakt-Tool ermöglichte automatisierte Verknüpfung der nicht freigegebenen Nummer mit dem Profil und den darin enthaltenen (freigegebenen) Angaben zur Person und Erstellung von Datensätzen mit den damit verbundenen Folgen und Risiken.

Eine solche Aufklärung ist vorliegend nicht erfolgt. Aus den insoweit seitens der Beklagten vorgelegten Anlagen B1 bis B9 sowie B19 und B20 findet sich kein ausdrücklicher Hinweis auf das Kontaktimporttool und die Verwendung der Mobilnummer hierfür bei im Übrigen auf „privat“ geschaltetem Account. Insbesondere die Hinweise auf die „Zwei-Faktor-Authentifizierung“ unter Verwendung der Mobilfunknummer enthält keine dahingehende Information. Im Übrigen betreffen die Informationen weitgehend nur die Privatssphäereeinstellungen im Hinblick auf die Veröffentlichung

persönlicher Daten – also die Zielgruppenauswahl –, nicht aber die Verwendungsarten der Mobilfunknummer.

Die Verletzung des Art. 13 DSGVO führt auch zu einer grundsätzlichen Ersatzpflicht nach Art. 82 DSGVO, da sie im vorliegenden Fall unmittelbar auf die Rechtmäßigkeit der Datenerhebung ausstrahlt. Zwar ist bei einem Verstoß gegen Art. 13 Abs. 1 DSGVO die Datenerhebung nicht zwangsläufig auch rechtswidrig; vielmehr kommt es auf eine Einzelfallbetrachtung an. Diese führt vorliegend indes dazu, dass die Datenerhebung insgesamt als rechtswidrig anzusehen ist. Etwas anderes gilt nämlich vor allem dann, wenn die betroffene Person verpflichtet war, die Datenerhebung zu dulden oder an ihr mitzuwirken, so dass sich die Verletzung von Aufklärungs- und Informationspflichten im Ergebnis nicht ausgewirkt hätte (vgl. Bäcker in: Kühling/Buchner, Art. 13 DSGVO, Rn. 64). So liegt der Fall hier allerdings nicht. Der Kläger war unstreitig nicht gehalten, seine Suchbarkeitseinstellungen unverändert zu lassen und konnte die Datenerhebung daher insgesamt beeinflussen. Die Nutzung der Plattform war auch nicht davon abhängig, dass der Kläger eine bestimmte Suchbarkeitseinstellung vornimmt. Vielmehr konnte der Kläger bei der Suchbarkeitseinstellung selbst entscheiden, ob und in welchem Umfang er sich über seine Mobilnummer suchbar machen will. Die dahingehende Willensbekundung des Klägers war infolge unvollständiger Information allerdings defizitär, so dass der Vorgang der Datenerhebung als solcher fehlerhaft war (vgl. Bäcker in: Kühling/Buchner, aaO.; Schmidt-Wudy in: BeckOK, Art. 13 DSGVO, Rn. 19).

bb)

Die Beklagte hat zudem gegen Art. 32 Abs. 1 DSGVO verstoßen. Hiernach sind 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. Dies dient der Absicherung der Datenschutzgrundsätze der Vertraulichkeit und Integrität (Art. 5 Abs. 1 lit. f) DSGVO). Gemäß Art. 32 Abs. 2 DSGVO sind bei der Beurteilung des angemessenen Schutzniveaus insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch unbefugten Zugang zu personenbezogenen Daten.

Angesichts des Umstands, dass im vorliegenden Fall das Risiko unbefugten Zugangs zu personenbezogenen Daten durch Scraping-Aktionen schon nach dem eigenen Vorbringen der Beklagten vergleichsweise hoch lag, da es sich um „gängige“ Techniken unbefugter Dritter zur Datenabgreifung im Internet handele, und die Nutzung des Kontaktimporttools, wie gezeigt, 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.

Den Anforderungen des Art. 32 Abs. 1 und 2 DSGVO ist die Beklagte nicht hinreichend nachgekommen. Dies hat die Klägerin unter Aufzeigung verschiedener technischer Möglichkeiten substantiiert vorgetragen. Die Beklagte trifft insoweit eine sekundäre Darlegungslast, zu den getroffenen Schutzmaßnahmen im Übrigen vorzutragen (vgl. OLG Stuttgart, Urteil v. 31.03.2021 – 9 U 34/21). Der hierzu getätigte Sachvortrag vermag nicht zu belegen, dass hinreichende Maßnahmen zur Vermeidung des unbefugten Zugriffs Dritter auf Daten getroffen wurden, so dass die entsprechende Behauptung der Klägerseite gem. § 138 Abs. 3 ZPO als zugestanden gilt.

Die Beklagte trägt zum Teil Mechanismen und Maßnahmen vor, die ersichtlich und/oder nach ihrem eigenen Vorbringen erst nach dem streitgegenständlichen Vorfall ergriffen wurden. Hierzu gehören sämtliche von ihr beschriebenen Fortentwicklungen vorhandener Maßnahmen bis hin zu der behaupteten generellen Einschränkung des Kontaktimporttools. Auch der von ihr dargelegte „Social Connection Check“ oder das „Freunde, die du kennen könntest“-System, ist nach ihrem Vorbringen erst im Nachgang zum Scraping-Vorfall implementiert worden. 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 auch dies ersichtlich keine präventiven Schutzmaßnahmen zur Verhinderung eines Vorfalls wie dem streitgegenständlichen, sondern es stellen Reaktionen auf bereits eingetretene Vorfälle dar. Das unbefugte Abgreifen von persönlichen Daten ist zu diesem Zeitpunkt bereits erfolgt. Soweit die Beklagte weiter vorträgt, sie habe die Suche von Nutzern anhand der Telefonnummer in der Facebook-Suchfunktion beschränkt, hat dies mit den technischen Vorkehrungen beim Kontaktimporttool nichts zu tun. 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 Kontaktimportfunktion im streitgegenständlichen Zeitpunkt.

Einzig relevant ist der Beklagtenvortrag, wonach 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-Anfragen oder Bot-Erkennungen sowie Übertragungsbeschränkungen. Auch dieses Vorbringen war jedoch zur Anspruchsverteidigung unzureichend, da es keinen Vortrag dazu enthält, 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 bzw. womöglich umgangen worden sind. Ohne eine solche Auseinandersetzung bleibt die Behauptung, man habe seinerzeit alle technisch erforderlichen Maßnahmen ergriffen, substanzlos, da sie das eigentliche Ereignis nicht erklären können.

Dabei mag es zutreffen, dass ein Scraping-Vorgang nicht schlechterdings zu vermeiden ist. Jedoch hätte die Beklagte die seinerzeit technisch realisierbaren und zumutbaren Möglichkeiten aufzeigen und deren Unfähigkeit, gerade den hiesigen Vorfall zu verhindern, darlegen müssen. Auch an einer hinreichenden Auseinandersetzung mit der Möglichkeit der Kombination verschiedener einzelner technischer Maßnahmen fehlt es.

Die Beklagte hat, wie ausgeführt, dargelegt, welche Techniken im Nachgang implementiert wurden. Ihr Vortrag lässt allerdings eine substantiierte Auseinandersetzung damit vermissen, weshalb diese Techniken nicht vorher schon vorhanden waren. Dies gilt etwa für die behauptete Einschränkung des Kontaktimporttools im Nachgang zum hiesigen Vorfall sowie für den „Social Connection Check“. Auch weitere Maßnahmen, wie sie die Beklagten ihrer Anlage B11 vom 19.5.2021 in Bezug auf neue Schutzvorkehrungen gegen Attacken gegenüber Nutzern dargelegt hat, etwa Datenbeschränkungen oder Begrenzungen der abgleichbaren Rufnummern bei ihrem Kontaktimporttool, lassen nicht erkennen, weshalb sie auch bei der notwendigen Einnahme einer ex-ante-Perspektive nicht schon vor dem streitgegenständlichen Vorfall implementiert waren. Für die Beklagte lag das Risikopotenzial bei der Implementierung das Kontaktimporttools in Kombination mit den Grundeinstellungen zur Sucharbeit eines Nutzers über dessen Telefonnummer aus technischer Sicht, anders als für den individuellen Nutzer, 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. Für den „Social Connection Check“ oder eine zahlenmäßige Begrenzung der abgleichbaren Rufnummern liegt das Potenzial zur Verhinderung von Scraping-Vorfällen auf der Hand. Dabei handelt es sich auch um technisch einfach umzusetzende flankierende Maßnahmen, die in einem angemessenen Verhältnis zum Risiko stehen.

Die Verletzung von Art. 32 DSGVO ist vom Schutzbereich des Art. 82 DSGVO auch umfasst; ein Verstoß kann die Schadensersatzpflicht auslösen (Jandt in: Kühling/Buchner, Art. 32, Rn. 40a m.w.N.).

cc)

in der Konsequenz aus den beiden vorgenannten Verstößen folgt auch eine Verletzung der Meldepflicht aus Art. 33 DSGVO durch die Beklagte. Denn hiernach hat der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung der zuständigen Aufsichtsbehörde zu melden. Etwas anderes

gilt nur, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen geführt hat. Eine Meldung hat die Beklagte unstreitig nicht veranlasst.

Die für die Meldepflicht erforderliche Verletzung des Schutzes personenbezogener Daten im Sinne einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (Art. 4 Nr. 12 DSGVO), hat es nach dem Vorgesagten gegeben. Es ist zu einem unbefugten Zugang zu personenbezogenen Daten gekommen, der in der zweckwidrigen Ausnutzung des – nicht hinreichend erklärten und nicht hinreichend abgesicherten – Kontaktimporttools zur Verknüpfung von nicht veröffentlichter Mobilnummer und Facebookprofil zu erkennen ist. Eine Einschränkung der Meldepflicht nach Art. 33 Abs. 1 S. 1 DSGVO lag nicht vor.

Der Verstoß gegen Art. 33 des GVO kann auch zu einer Haftung nach Art. 82 DSGVO führen (Kühling/Büchner/Jandt, Art. 33 DSGVO, Rn. 27; vgl. OLG Frankfurt am Main, GRUR 2022, S. 1252).

Das vorstehend Gesagte gilt auch hinsichtlich eines Verstoßes gegen Art. 34 Abs. 1 DSGVO, nachdem die Beklagte auch den Kläger als betroffene Person unverzüglich hätte benachrichtigen müssen. Ein hohes Risiko für die Rechte des Betroffenen im Normsinne lag nach dem Vorgesagten vor. Die von der Beklagten insoweit herausgegebene Information vom 6.4.2021 stellte dabei keine hinreichende individuelle Information des Klägers dar. Der Beklagten wäre es wegen der ihr bekannten E-Mail-Adresse des Klägers und sämtlicher weiterer betroffener Nutzer ohne weiteres möglich gewesen, individuelle Benachrichtigungen per E-Mail oder jedenfalls solche auf der individuellen Profilseite eines jeden Nutzers zu versenden. Das Schreiben der Beklagten vom 30.8.2021 war sodann nicht mehr unverzüglich im Sinne des Art. 34 Abs. 1 DSGVO. Ein Ausschlussgrund nach Art. 34 Abs. 3 DSGVO liegt nicht vor. Insbesondere ist ein Ausschluss des Risikos für die Zukunft nach dem eigenen Beklagtenvorbringen im Sinne von Art. 34 Abs. 3 lit. b) DSGVO im Hinblick auf Scraping-Attacken weiterhin nicht ausgeschlossen.

dd)

Im Übrigen kann es dahinstehen, ob der Beklagten auch ein Verstoß gegen Art. 25 DSGVO vorzuwerfen ist, da ein solcher jedenfalls für sich genommen keinen Anspruch aus Art. 82 DSGVO auslösen könnte, weil die Anforderungen des Art. 25 DSGVO schon vor der eigentlichen Verarbeitung von Daten anknüpfen (vgl. Kühling/Buchner/Hartung, Art. 25 DSGVO, Rn. 31; Matz in: Sydow/Marsch, Art. 25 DSGVO, Rn. 77).

Gleiches gilt für einen möglichen Verstoß gegen Art. 15 DSGVO, da es sich hierbei nicht um einen Verstoß gegen Pflichten bei der Verarbeitung von personenbezogenen Daten handelt. Die Auskunft dient allenfalls der Vorbereitung eines Schadensersatzanspruchs bzw. der allgemeinen Information über die Datenerhebung. Zudem würde es an der Kausalität des Verstoßes für den ver-

meintlichen Schaden in Gestalt des Datenverlustes fehlen, denn dieser liegt in einer ggf. rechtswidrigen Datenverarbeitung begründet, nicht jedoch in einer unterlassenen oder verspäteten Auskunft über die erhobenen Daten als solche (vgl. Bienemann in: Sydow/Marsch, Art. 15 DSGVO, Rn. 77). Insoweit unterscheidet sich das Auskunftsrecht aus Art. 15 DSGVO von der – bei Verstoß von Art. 82 DSGVO umfassten – Meldepflicht gegenüber dem Betroffenen aus Art. 34 DSGVO. Letztere hängt unmittelbar mit einem konkreten Verletzungsereignis zusammen und ermöglicht dem Betroffenen ggf. eine Einflussnahme auf das Ausmaß des Schadens oder dessen Verhinderung, wohingegen Art. 15 DSGVO ein allgemeines Informationsrecht regelt.

c.

Der Beklagten gelingt sodann nicht die Entlastung gem. Art. 82 Abs. 3 DSGVO. Voraussetzung hierfür wäre, dass sie nachweist, in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich zu sein. Erforderlich ist deshalb der Nachweis, dass der Anspruchsgegner sämtliche Sorgfaltsanforderungen erfüllt hat und ihm nicht die geringste Fahrlässigkeit vorzuwerfen ist (vgl. Kühling/Buchner/Bergt, Art. 82 DSGVO, Rn. 54 m.w.N.). Dies ist hier nicht der Fall, was sich bereits aus den Ausführungen zur Verletzung der DSGVO-Pflichten ergibt, da diese ein zumindest fahrlässiges Handeln belegen. Insbesondere das Fahlen von weiteren – erst im Nachgang zum streitgegenständlichen Ereignis vorgenommenen – technischen Schutzmaßnahmen war sorgfaltspflichtwidrig. Dabei fällt ins Gewicht, dass die Methode des Scrapings nach dem eigenen Beklagtenvorbringen sowie ihren Mitteilungen an ihre Nutzer (etwa in Anlage B11) 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, Art. 82 DSGVO, Rn. 15). Außergewöhnliche Kausalverläufe oder ein Fall höherer Gewalt liegt weder vor, noch wurde derartiges vorgetragen.

d.

Der Kläger hat auch einen immateriellen Schaden im Sinne der Norm erlitten. Der Begriff des Schadens ist nach dem Erwägungsgrund 146 S. 3 weit auszulegen. Es soll ein vollständiger und wirksamer Ersatz des erlittenen Schadens sichergestellt werden. Dies beinhaltet auch eine Abschreckungswirkung des Schadensersatzes zur Wahrung des Effektivitätsgrundsatzes (vgl. Bergt in: Kühling/Buchner, Art. 82 DSGVO, Rn. 17 m.w.N.). Auf eine schwer wiegende Persönlichkeitsrechtsverletzung kommt es wegen der notwendigen unionsrechtlichen Auslegung des Schadensbegriffs nicht an. Allerdings erfordert die Ersatzpflicht das Vorhandensein eines konkreten Schadens über den bloßen Verstoß gegen die Vorschriften des DSGVO hinaus (OLG Frankfurt, GRUR 2022, S. 1252). Zu solchen immateriellen Beeinträchtigungen können etwa Ängste, Stress sowie Komfort- und Zeiteinbußen gehören (OLG Frankfurt, aaO.).

Das Gericht ist hier nach § 286 ZPO unter Zugrundelegung allgemeiner Lebenserfahrung bei dem hier zu beurteilenden Fall in hinreichendem Umfang davon überzeugt, dass die Verknüpfung der

Mobilnummer des Klägers mit dessen Facebookprofil durch den Scraping-Vorfall und dadurch die unbefugte Zusammenstellung und gesonderte Veröffentlichung von personenbezogenen Daten, jedenfalls von Name, Land, Telefonnummer und Geschlecht sowie Facebook-ID durch unbefugte Dritte mit der dem immanenten Gefahr der zweckwidrigen, illegalen und vor allem potenziell vermögensgefährdenden Verwendung der Daten durch Dritte einen Schaden in Gestalt von empfundenem Stress, Unwohlsein und Komforteinbußen hervorruft. Es ist nach allgemeiner Lebenserfahrung hinreichend sicher, dass der Kontrollverlust und der Umstand, dass personenbezogene Daten über die Verknüpfung zur Mobilnummer unbefugten Dritten bekannt geworden und von diesen in Zukunft womöglich zweckwidrig und/oder zu illegalen Zwecken benutzt werden, ein für den immateriellen Schaden bereits ausreichendes „ungutes Gefühl“ auslösen (vgl. Dickmann, r+s 2018, S. 345). Dass es sich bei den abgerufenen Daten um solche gehandelt hat, die der Kläger auf seinem Profil ohnehin freigegeben hatte, steht dem nicht entgegen, da Anknüpfungspunkt der Haftung die Verknüpfung dieser Daten mit der – nicht freigegebenen – Mobilnummer unter Ausnutzung des Kontaktimporttools darstellt.

Letzteres spielt indes bei der Bemessung der Höhe des Schadensersatzanspruchs eine Rolle. Die Höhe bemisst das Gericht vorliegend insgesamt mit EUR 500,00, wobei es dies für angemessen, aber auch ausreichend hält, um der Ausgleichsfunktion für den erlittenen immateriellen Schaden und eine Abschreckungswirkung nachzukommen, zugleich jedoch die besonderen Umstände des Falles zu würdigen. Dem Gericht steht insoweit gemäß § 287 ZPO ein Ermessen zu. Zu berücksichtigen sind Art, Umfang und Zweck der betreffenden Verarbeitung, der Verschuldensgrad, Maßnahmen zur Minderung des Schadens und die Intensität des erlittenen Schadens.

Vorliegend fällt ins Gewicht, dass die Beklagte, wie aufgezeigt, mehrere Verstöße gegen die DSGVO zu verantworten hat. Hinzu kommt der beachtliche Umfang des Scraping-Vorfalls sowie die beim Kläger grundsätzlich erlittenen Nachteile. Gleichwohl handelt es sich bei dem erlittenen Schaden um einen solchen im Bagatellbereich; die erlittenen Einschränkungen gehen nicht signifikant über alltägliche zumutbare Beeinträchtigungen hinaus. Außerdem ist, wie angesprochen, zu berücksichtigen, dass im Ergebnis zwar eine Verknüpfung von Telefonnummer und persönlichen Daten des Klägers, die so nicht gewollt war, stattgefunden hat, jedoch im wesentlichen ohnehin von diesem veröffentlichte Daten betroffen waren und sich in gewisser Weise ein abstrakt vorhandenes allgemeines Risiko der sozialen Bewegungen im Internet verwirklicht hat. Zu einer konkreten Vermögensgefährdung oder Schädigung ist es infolge des Vorfalls (bislang) nicht gekommen. Ferner ist der Beklagten allenfalls Fahrlässigkeit hinsichtlich der Datenschutzverstöße vorzuwerfen. Zudem sind ihre Bemühungen um die Eindämmung und zukünftige Verhinderung solcher Schäden zu berücksichtigen.

Nicht in die Bewertung mit einzubeziehen war indes die Behauptung des Klägers, es sei bei ihm zu einer größeren Skepsis bei Anrufen von unbekannten Nummern oder E-Mail-Absendern gekommen sowie, dass es vermehrt zu Kontaktversuchen via SMS und E-Mail durch unbekannte Dritte

gekommen sei. Hierzu ist schon nicht feststellbar, dass es eine belastbare kausale Verknüpfung zum streitgegenständlichen Scraping-Vorfall gegeben hat. Das gesteigerte Misstrauen des Klägers stellt im Übrigen keine Komforteinbuße im eingangs beschriebenen Sinne oder eine zum Schadensersatz führende Gefühlslage dar.

e.

Die der Beklagten vorzuwerfenden DSGVO-Verstöße sind für den Schaden im Übrigen kausal, wobei eine Mitursächlichkeit ausreicht (vgl. Bergt in: Kühling/Buchner, Art. 82 DSGVO, Rn. 44).

Bei einer ordnungsgemäßen umfänglichen Information des Klägers über die Implementierung des Kontaktimporttools hätte eine Einschränkung der Suchbarkeit des Profils und damit eine Umgehung der Verknüpfung von Mobilnummer und Profil stattfinden können. Nach gegenwärtigem allgemeinen Verständnis – entsprechend des Beklagtenvorbringens – waren Daten von Nutzern, deren Suchbarkeit eingeschränkt oder ausgestellt war, nicht vom Scraping-Vorfall betroffen. Dass der Kläger eine solche Einstellung bei umfassender Aufklärung vorgenommen hätte, ist nach seinem Vorbringen unter Würdigung nach allgemeiner Lebenserfahrung anzunehmen. Dass der Kläger seine Suchbarkeitseinstellung nach Kenntnis vom Scraping-Vorfall womöglich nicht oder nicht gleich geändert hat, steht dem nicht entgegen. Denn zu diesem Zeitpunkt hatte die Beklagte bereits neue, verbesserte Schutzvorkehrungen implementiert und kommuniziert, so dass die Entscheidung eines Nutzers auf einer neuen und fundierten Grundlage erfolgte.

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. Insbesondere die Einschränkungen der Nutzung des Kontaktimporttools (etwa durch Begrenzung abrufbarer Nummern) oder die Einführung des „Social Connection Checks“ hätten das automatisierte Datenabgreifen ersichtlich verhindern können, da sie die uneingeschränkte und unkontrollierte Verknüpfung von wahllos zusammengestellten Mobilnummern mit jeweiligem Facebookprofil unattraktiv oder gar unmöglich gemacht hätte. Dies entspricht nicht zuletzt dem Beklagtenvorbringen zu der Effektivität der von ihr – im Nachgang zum hiesigen Vorfall – ergriffenen Maßnahmen.

Gleiches gilt für die Verletzung der Meldepflichten, nachdem diese jedenfalls im Sinne einer Mitursächlichkeit bei rechtzeitiger Einhaltung eine Risikominimierung ermöglicht hätten, dies etwa durch zeitige Änderung von Telefonnummern, Passwörtern oder Profildaten.

f.

Insgesamt steht dem Kläger nach alledem der beantragte Schadensersatzanspruch aus Art. 82 Abs. 1 DSGVO in Höhe von EUR 500,00 zu.

2.

Der Kläger kann von der Beklagten auch die Feststellung der Ersatzpflicht für mögliche künftige Schäden verlangen. Die für eine solche Feststellung erforderliche Möglichkeit künftiger Schäden, liegt, wie beschrieben, hier vor. Insbesondere sind künftige materielle Schäden nicht schlechterdings ausgeschlossen, sollte es in Zukunft zu einer vermögensgefährdenden oder –schädigenden Nutzung der gewonnen Daten kommen. Die grundsätzliche Ersatzpflicht aus Art. 82 Abs. 1 DSG VO liegt, wie gezeigt, vor.

3.

Der Kläger hat gegenüber der Beklagten jedenfalls aus §§ 823 Abs. 1, 1004 BGB analog i.V.m. Art. 6 DSGVO Anspruch auf Unterlassung im Hinblick auf die fehlende Vorhaltung unzureichender technischer Maßnahmen, mithin im Hinblick auf den Verstoß gegen Art. 32 Abs. 1 DSGVO.

Es ist, wie gezeigt, zu einer schuldhaften, kausalen Verletzung der Persönlichkeitsrechte des Klägers gekommen. Die Datenverarbeitung erfolgte entgegen den Vorgaben des Art. 6 Abs. 1 DSGVO, da es wegen des Versäumnisses der Beklagten zu hinreichenden Information an einer rechtmäßigen Einwilligung im Sinne des Art. 6 Abs. 1 S. 1 lit. a) DSGVO fehlte und im Weiteren, namentlich im Hinblick auf Art. 6 Abs. 1 S. 1 lit. b) DSGVO, auf den sich die Beklagte wegen der Zwecke des Betriebs einer social media Plattform beruft, die Rechtmäßigkeit der Datenverarbeitung immanent vorausgesetzt hätte, dass technisch ausreichende Schutzmaßnahmen im Sinne des Art. 32 DSGVO vorlagen. Da dies nicht der Fall war, erfolgte die Datenverarbeitung rechtswidrig. Der Kläger kann vor diesem Hintergrund von der Beklagten grundsätzlich verlangen, dass dies in Zukunft unterlassen wird.

Das Bestehen des Verstoßes indiziert die für den Unterlassungsanspruch erforderliche Wiederholungsgefahr. Das Rechtsschutzziel des Klägers ist auch auf ein Unterlassen gerichtet, da die Beklagte die personenbezogenen Daten in Zukunft nicht erneut ohne ausreichende Sicherheitsvorkehrungen verarbeiten soll.

Der Kläger hatte den Datenschutzverstoß auch nicht zu dulden. Dass die Daten zum Teil vom Kläger selbst auf seinem Profil veröffentlicht wurden, steht dem Anspruch, wie zuvor bereits behandelt, nicht entgegen.

Einem Unterlassungsanspruch aus nationalem Recht steht Art. 79 DSGVO nicht entgegen; solche Ansprüche sind nicht gesperrt (LG Frankfurt a.M., Beschluss v. 15.10.2020 – 2/3 O 356/20, GRUR-RS 2020, 28899 m.w.N.). Darauf, ob Art. 17 DSGVO einen Unterlassungsanspruch begründet, kommt es daher nicht an.

Die Klage war allerdings unbegründet im Hinblick auf einen Unterlassungsanspruch, der gerichtet ist auf ein Unterlassen der Datenverarbeitung ohne Erfüllung der Informationspflichten gemäß Art. 13, 14 DSGVO. Zwar lag ein solcher Verstoß, wie ausgeführt, vor. Es fehlt allerdings an einer noch bestehenden Wiederholungsgefahr, die Voraussetzung für einen Unterlassungsanspruch wäre. Zwar indiziert die Erstbegehung grundsätzlich die Gefahr von Wiederholungen; im hiesigen Fall ist allerdings zu berücksichtigen, dass sich das der Beklagten konkret vorzuwerfende Versäumnis der nicht ausreichenden Information des Klägers über die Datenverarbeitung im Hinblick auf die Verwendung seiner Mobilnummer im Rahmen des Kontaktimporttools bei verständiger Würdigung des Sachverhalts nicht wiederholen dürfte. Der Kläger ist, wie seine Klage zeigt, mittlerweile hinreichend über diese Vorgänge informiert und aufgeklärt und kann seine persönlichen Datenschutzeinstellungen bei der Nutzung der Facebook-Plattform entsprechend anpassen. Eine ähnlich gelagerte zukünftige Konstellation, die eine unzureichend informierte Datenverarbeitung über die Nutzung des Kontaktimporttools befürchten lassen würde, ist nicht ersichtlich.

4.

Die Klage war des Weiteren 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 bereits mit Ihrem Schreiben vom 30.8.2021 die erforderlichen Auskünfte erteilt. Insbesondere wurde dem Kläger hier mitgeteilt, welche Daten betroffen sind und auf welche Weise es zu deren Abgriff durch unbekannte Dritte gekommen ist.

Soweit der Kläger an der inhaltlichen Richtigkeit und Vollständigkeit der Auskünfte zweifelt, steht dies der Erfüllungswirkung nicht entgegen. Erfüllt ist die Auskunft bereits dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Umfang darstellen.

Weitergehende Auskünfte schuldete die Beklagte nicht, insbesondere war ihr wegen Unmöglichkeit im Sinne von § 275 Abs. 1 BGB nicht aufzuerlegen, mitzuteilen, welche Empfänger zu welchem Zeitpunkt welche Daten im Detail durch den Vorfall erhalten haben. Es ist nicht erkennbar, dass der Beklagten eine solche Auskunft möglich wäre.

V.

Der Kläger kann aufgrund von Art. 82 Abs. 1 DSGVO den Ersatz vorgerichtlich aufgewendeter Rechtsanwaltskosten zur Anspruchsdurchsetzung als Schaden geltend machen (vgl. Bergt in: Kühling/Bruchner, Art. 82 DSGVO, Rn. 19). Der Höhe nach beträgt die einschlägige 1,3 RVG-Gebühr EUR 627,13 brutto. Zu berücksichtigen sind für die Wertermittlung die Schadensersatzhöhe von EUR 500,00 sowie die geltend gemachten Unterlassungsansprü-

che. Soweit die Klage darüber hinausging, wurde ein unzutreffend hoher Streitwert für die Berechnung zugrunde gelegt.

VI.

Der Kläger hat unter dem Gesichtspunkt des Verzugs gem. §§ 286, 288, 291 BGB Anspruch auf Ersatz von Zinsen aus EUR 500,00 in Höhe von 5 Prozentpunkte über dem Basiszinssatz seit Rechtshängigkeit, vorliegend seit dem 17.9.2022. Denn die Beklagte hat ausweislich der Verteidigungsanzeige vom 16.9.22 spätestens zu diesem Zeitpunkt die Klage zugestellt bekommen. Für die Zinsen aus dem Anspruch auf Zahlung der vorgerichtlichen Rechtsanwaltskosten gilt dasselbe.

VII.

Die Kostenentscheidung beruht auf § 92 Abs. 1 S. 1 ZPO. Die Entscheidung zur vorläufigen Vollstreckbarkeit beruht auf § 709 ZPO.

Der nicht nachgelassene Schriftsatz der Beklagten vom 13.03.2023 war, soweit er Angriffs- und Verteidigungsmittel enthält, gem. § 296a ZPO verspätet. Eine Wiedereröffnung gem. § 156 ZPO war nicht angezeigt.

[redacted]