Beglaubigte Abschrift

[redacted]

Landgericht Bonn

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

[redacted],

Klägers,

Prozessbevollmächtigte: Rechtsanwälte Wilde Beuger Solmecke Part. mbB,
Kaiser-Wilhelm-Ring 27 - 29, 50672 Köln,

gegen

die Meta Platforms Ireland Limited, 4 Grand Canal Square, Dublin, Irland,

Beklagte,

Prozessbevollmächtigte: Rechtsanwälte Freshfields Bruckhaus Deringer und Steuerberater PartnerGmbH,
Bockenheimer Anlage 44, 60322 Frankfurt,

hat die 10. Zivilkammer des Landgerichts Bonn
aufgrund mündlicher Verhandlung vom 12.05.2023
durch die Richterin am Landgericht [redacted] als Einzelrichterin

für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von 500 EUR nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 10.12.2022 zu zahlen.

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

3. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Anwaltskosten in Höhe von 220,27 EUR zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 10.12.2022 zu zahlen.

4. Im Übrigen wird die Klage abgewiesen.

5. Die Kosten des Rechtsstreits tragen der Kläger zu 40%, die Beklagte zu 60%.

6. Das Urteil ist vorläufig vollstreckbar. Der jeweilige Vollstreckungsschuldner kann die Vollstreckung durch Sicherheitsleistung i.H.v. 110% des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht der Vollstreckungsgläubiger vor der Vollstreckung Sicherheit i.H.v. 110% des jeweils zu vollstreckenden Betrages erbringt.

Tatbestand:

Die Parteien streiten um Auskunfts- Unterlassungs- und Schadensersatzansprüche nach einem behaupteten Verstoß der Beklagten gegen Vorschriften der Datenschutzgrundverordnung (im Folgenden: DSGVO).

Die Beklagte betreibt unter der Internetseite www.facebook.com eine Socialmedia-Plattform. Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen.

Bei der Registrierung wird der Nutzer auf die Datenrichtlinie der Beklagten hingewiesen, zu deren Gestaltung auf Anlage B 19 (dort Bl. 958 ff.) Bezug genommen wird. Den Nutzern werden zudem im „Hilfebereich", der unmittelbar auf der Facebook Homepage verlinkt ist, Informationen über die Privatsphäre-Einstellungen zur Verfügung gestellt (zu den Einzelheiten vgl. Anlagen B 3 bis B 11).

Bei der Eröffnung eines Facebook-Accounts muss der Nutzer zur Erstellung eines Nutzerprofils verschiedene Daten angeben. Der Vor- und Nachname, das Geschlecht und die von der Beklagten erstellte Nutzer-ID sind im Folgenden als Teil des

Nutzerprofils immer öffentlich einsehbar. Für die Nutzer besteht die Möglichkeit, weitere Angaben in ihrem Profil zu speichern, wie z.B. eine Handynummer oder E-Mail-Adresse. Diese Angaben sind für die Erstellung des Profils nicht zwingend.

Im Rahmen der Privatsphäre-Einstellungen der Plattform kann der Nutzer von verschiedenen Wahlmöglichkeiten Gebrauch machen: Bei der sogenannten „Zielgruppenauswahl" legt der Nutzer fest, wer einzelne Informationen auf seinem Profil, wie etwa Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse, einsehen kann. Die „Suchbarkeits-Einstellungen" legen hingegen fest, wer das Profil eines Nutzers anhand einer Telefonnummer finden kann.

Facebook bot in diesem Zusammenhang jedenfalls in den Jahren 2018-2019 die Funktion an, die im Smartphone eines Nutzers gespeicherten Personenkontakte mit Nutzern auf Facebook allein anhand der Telefonnummer zu synchronisieren (Contact-Import-Tool, CIT). Wenn ein Suchender in seinem Smartphone eine Telefonnummer als Kontakt eingespeichert hat, erlaubte es die Beklagte ihm, seine Kontakte mit den bei Facebook hinterlegten Telefonnummern abzugleichen, um die hinter den Nummern stehenden Personen als Freunde hinzuzufügen

Die Identifizierung eines Facebook-Profiles war dabei möglich, ohne dass die im Profil hinterlegte Nummer durch den betroffenen Nutzer für die Öffentlichkeit freigegeben war; eine Telefonnummer konnte damit einem Profil zugeordnet werden, ohne dass im Profil des Nutzers die Telefonnummer der Öffentlichkeit preisgegeben werden sollte.

Zwischen den Parteien ist streitig, ob eine solche Zuordnung zumindest dadurch ausgeschlossen werden konnte, dass der betroffene Nutzer nicht nur in der Zielgruppenauswahl seine Telefonnummer für die Öffentlichkeit „sperrte" sondern auch bei den Suchbarkeits-Einstellungen eine entsprechende aktive Auswahl vornahm. Die „Suchbarkeits-Einstellung" für Telefonnummern war auf der Plattform für die Nutzer jedenfalls standardmäßig auf „Alle" eingestellt.

Der Kläger eröffnete im Jahr 2008 einen Facebook-Account.

Im Zeitraum von Januar 2018 bis September 2019 sammelten Dritte mittels „Datenscrapings", also dem massenhaften automatisierten Abruf und Sammeln persönlicher Daten, verschiedene Daten von Facebook-Nutzern, die auf dem Facebook-Profil entweder „immer öffentlich" oder aber zu diesem Zeitpunkt aufgrund der Privatsphäreneinstellungen der Nutzer öffentlich einsehbar waren. Dieses

Sammeln von Daten mittels automatisierter Tools und Methoden war und ist nach den Nutzungsbedingungen der Beklagten untersagt.

Den Daten der Facebook-Nutzer wurden dabei von den Scrapern mittels des Contact-Import-Tools die Handy- bzw. Telefonnummern der Nutzer zugeordnet. Dies geschah mittels „Telefonnummernaufzählung": Die „Scraper" luden mithilfe des „CIT" fiktive „Kontakte" hoch, welche automatisch generierte Telefonnummern enthielten, um festzustellen, ob diese Telefonnummern mit einem Facebook-Konto verbunden sind. Soweit sie feststellen konnten, dass eine Telefonnummer mit einem Facebook-Konto verknüpft war, kopierten sie die öffentlich einsehbaren Informationen aus dem betreffenden Nutzerprofil und fügten die Telefonnummer den abgerufenen, öffentlich einsehbaren Daten hinzu.

Anfang April 2021 veröffentlichten Unbekannte nach Angaben eines Artikels des „Business Insider" vom 03.04.2021 die Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern im Internet.

Wegen des Vorfalls verhängte die Irische Datenschutzbehörde DPC unter dem 28.11.2022 gegen die Beklagte aufgrund verschiedener Verstöße gegen die DSGVO eine Geldbuße in Höhe von 265 Mio. Euro.

Bereits im September 2020 löschte der Kläger seinen Facebook-Account.

Mit E-Mail vom 10.02.2022 forderte er die Beklagte durch seine Prozessbevollmächtigten zur Schadensersatzzahlung i.H.v. 500,00 EUR, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft darüber auf, welche konkreten Daten im Vorfeld der Veröffentlichung vom April 2021 abgegriffen und veröffentlicht worden waren (Anlage K1, Bl. 66).

Der Kläger behauptet, er habe bereits im Jahr 2020 vermehrt Spam- und Phishing-SMS sowie Robo-Calls erhalten. Auf der Seite ihavebeenpwnd.com habe er dann feststellen können, dass seine Facebook-Daten im Internet abrufbar seien – dies, obwohl er mit seinen Datenangaben bei Facebook immer sehr restriktiv umgegangen sei. Seine Handynummer habe er erst angegeben, als er den Messengerdienst zwingend zur Kommunikation mit anderen Nutzern gebraucht habe, da eine Kommunikation allein über den Browser nicht mehr möglich gewesen sei.

Seine persönlichen Daten wie Vor- und Nachname sowie Geschlecht und Facebook-ID seien auch auf dem Hackerforum raidforum.com veröffentlicht worden. Auch seine E-Mail-Adresse sei betroffen gewesen.

Aufgrund dieses Datenscraping-Vorfalls habe er das Vertrauen in die Fähigkeit der Beklagten, seine persönlichen Daten ausreichend zu schützen, vollkommen verloren und deshalb auch sein Facebook-Konto gelöscht. Seit dem Vorfall habe er den AB seines Handys ausgeschaltet, Anrufe von fremden Rufnummern beantworte er nicht mehr. Bei ihm verbleibe ein Zustand großen Unwohlseins und großer Sorge über einen möglichen Missbrauch der ihn betreffenden Daten.

Der Kläger ist der Ansicht, die Beklagte habe bei der Gestaltung ihrer Seite gegen diverse Vorschriften der DSGVO verstoßen. Insbesondere hätte sie nicht ausreichend die durch das CIT bestehende Sicherheitslücke geschlossen, durch die öffentlich abrufbare Daten mit einer Telefonnummer hätten korreliert und damit „veredelt" werden können. Selbst, wenn man eine Suchbarkeit des eigenen Accounts über die Telefonnummer in den Einstellungen ausgeschlossen hätte, hätte über das CIT eine Zuordnung des Accounts zur eigenen Handynummer durch Dritte vorgenommen werden können.

Es seien keine Sicherheitscapchas verwendet worden, um sicherzustellen, dass es sich bei der Anfrage zur Synchronisierung um die Anfrage eines Menschen und nicht um eine automatisch generierte Anfrage handele. Ebenso wenig sei ein Mechanismus zur Überprüfung der Plausibilität der Anfragen bereit gehalten worden. Der massenhafte Zugriff auf die Facebook-Profile durch Dritte mit auffälligen Telefonnummerabfragen wäre durch einfachste IP-Logs erkennbar und blockierbar gewesen.

Darüber hinaus seien aber auch bereits die Einstellungen zur Privatsphäre auf der Seite der Beklagten so undurchsichtig und kompliziert gestaltet, dass unsichere Einstellungen provoziert würden. Die Beklagte handle aufgrund der datenschutzunfreundlichen Standard-Voreinstellungen entgegen des Prinzips der Datenminimierung und des „privacy by default"-Grundsatzes. Die versteckte Option, dass der Nutzer nicht anhand seiner Telefonnummer von der Öffentlichkeit gefunden werden möchte, sei aufgrund der verworrenen Einstellungsmöglichkeiten nicht zu erreichen, wenn lediglich nach den Einstellungsmöglichkeiten für die Telefonnummer gesucht werde.

Durch die zahllosen Einstellungsoptionen werde ein Gefühl der Sicherheit für den Nutzer erzeugt, was im Ergebnis zu einer erheblichen Datengefährdung führe, da mit hoher Wahrscheinlichkeit zu erwarten sei, dass ein Nutzer die voreingestellten Standardeinstellungen behalte und nicht selbständig ändere. Diese

Undurchsichtigkeit setze sich bei der von der Beklagten betriebenen „Messenger"-App mit separaten Sicherheitseinstellungen fort.

Auch sei zumindest bei erstmaliger Eingabe der Telefonnummer des Nutzers ein expliziter Hinweis auf die offenen Standard-Einstellungen für die Suchbarkeit per Telefonnummer zu verlangen gewesen sowie eine Information über etwaige Risiken bei der Verwendung des CITs.

Hätte sich die Beklagte DSGVO-konform verhalten, wäre es mit an Sicherheit grenzender Wahrscheinlichkeit nicht möglich gewesen, mit einem automatisierten Verfahren Daten abzugreifen.

Ihm, dem Kläger stehe mithin gegen die Beklagte unter anderem ein Schadensersatzanspruch aus Art. 82 Abs. 1 DSGVO zu.

Der Kläger beantragt:

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

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

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

    a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, 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 Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat" noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.

4. Die Beklagte wird verurteilt der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.

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

Die Beklagte beantragt,

die Klage abzuweisen.

Sie ist der Ansicht, die Klage sei in den Klageanträgen zu 1.) – 3). aufgrund der fehlenden Bestimmtheit bereits unzulässig, darüber hinaus aber auch unbegründet.

Ein Verstoß gegen die Vorschriften der DSGVO liege insgesamt nicht vor.

Der „Datenklau" beruhe nicht auf einer unzulässigen Sicherheitslücke ihrer Plattform. Die Scraper hätten lediglich rechtmäßige, gewöhnliche Nutzerfunktionen ausgenutzt. Ein Scraping öffentlich einsehbarer Daten könne nicht völlig verhindert werden, ohne dass dabei gleichzeitig der legitime Zweck der Plattform, eine Nutzervernetzung zu ermöglichen, unterlaufen würde. Es gebe allenfalls Mittel, um Scraping zu begrenzen. Entsprechende Sicherheitsvorkehrungen wie z.B. die Implementierung von Übertragungsbeschränkungen bei vermehrtem Datenabruf von einer bestimmten

IP-Adresse habe sie, die Beklagte auch getroffen. Auch Captcha-Abfragen kämen zum Einsatz.

Die Standard-Voreinstellungen orientierten sich am Hauptzweck der Facebook Plattform, andere Nutzer zu finden und mit diesen in Kontakt zu treten. Den Nutzern würden alle erforderlichen Informationen zur Datenverarbeitung zur Verfügung gestellt und umfassend über die Möglichkeiten der Anpassung der Einstellungen informiert. Die entsprechenden Einstellungen seien klar und leicht zu finden.

Sofern ein Nutzer eine Suchbarkeit des eigenen Accounts über die Telefonnummer ausgeschlossen habe, sei auch ein „Import" des Accounts über die CIT-Funktion nicht möglich gewesen.

Hinsichtlich der „Messenger"-App entsprächen die Sicherheitseinstellungen denjenigen im allgemeinen Facebook-Konto: Änderungen in den Privatsphäre-Einstellungen auf der Facebook-Plattform würden immer automatisch auch auf die Messenger-App übertragen.

Ein Schadensersatzanspruch nach Art. 82 DSGVO scheitere im Übrigen aber auch bereits daran, dass die Vorschriften, gegen die sie, die Beklagte, nach Ansicht der Klägerseite verstoßen haben soll, vom Anwendungsbereich des Art. 82 DSGVO nicht umfasst seien. Weiter habe die Klagepartei auch nicht dargelegt, dass sie einen immateriellen Schaden im Sinne einer spürbaren tatsächlichen Beeinträchtigung persönlichkeitsbezogener Belange von einigem Gewicht erlitten habe. Ein bloßes Unmutsgefühl wegen der Nichtbeachtung des Rechts durch einen anderen sei, wie auch der Generalanwalt Sánchez-Bordona in seinen Schlussanträgen vor dem EuGH im Verfahren C-300/21 (Österreichische Post) deutlich gemacht habe, für die Bejahung eines zum Ersatz verpflichtenden Schadens nicht ausreichend.

Auch sei zu berücksichtigen, dass vorliegend keine Klägerdaten betroffen seien, die ähnlich sensibel seien wie Kredit- und Bankkartennummern, nationale Ausweisnummern oder Kontopasswörter.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die zwischen den Parteien gewechselten Schriftsätze der Parteien nebst Anlagen sowie auf die Sitzungsniederschrift vom 12.05.2023 (Bl. 1252 ff. d.A.) Bezug genommen.

Entscheidungsgründe:

I.

Die Klage ist zulässig, insbesondere liegt hinsichtlich der Klageanträge 1.) – 3.) eine hinreichende Bestimmtheit i.S.d. § 253 Abs. 2 Nr. 2 ZPO vor.

Grundsätzlich kann eine hinreichende Bestimmtheit eines Antrags im Sinne des § 253 Abs. 2 Nr. 2 ZPO angenommen werden, wenn er den Anspruch konkret bezeichnet, den Rahmen der gerichtlichen Entscheidungsbefugnis erkennbar abgrenzt, den Inhalt und Umfang der materiellen Rechtskraft erkennen lässt, das Risiko des Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abwälzt und wenn er die Zwangsvollstreckung aus dem beantragten Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (BGH, Urteil vom 21. November 2017 - II ZR 180/15 -, juris, Rn. 8 m.w.N.). Der Klageantrag ist dabei der Auslegung zugänglich, wobei auch die Klagebegründung heranzuziehen ist (Zöller/Greger, ZPO, 33. Auflage 2022, § 253 Rn. 13 m.w.N.). Gemessen an diesen Voraussetzungen genügen die ersten drei Klageanträge dem Bestimmtheitsgebot:

Aus Klageschrift ergibt ein hinreichender Zusammenhang zwischen dem Zahlungsantrag in Klageantrag zu 1 und dem zugrundeliegenden Lebenssachverhalt, der – wenngleich er sich über einen längeren Zeitraum erstrecken mag – abgeschlossen ist.

Dem Klageantrag zu 2 lässt sich in Verbindung mit Klageschrift und Replik hinreichend bestimmt entnehmen, dass der Kläger festgestellt wissen will, dass die Beklagte verpflichtet ist, dem Kläger sämtliche zukünftige Schäden zu ersetzen, die dem Kläger aufgrund der missbräuchlichen Datenabgreifung noch entstehen werden.

Soweit die Beklagte in Bezug auf den Klageantrag zu 3 eine Unbestimmtheit der Formulierung „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen" rügt, ist dem nicht zu folgen. Denn eine weitergehende Konkretisierung der zu ergreifenden Sicherheitsmaßnahmen ist der Klägerseite schon deshalb nicht möglich bzw. zur Gewährung effektiven Rechtsschutzes abzulehnen, weil sie zu erwartende technische Weiterentwicklungen nicht hinreichend abbilden könnte (vgl. hierzu BGH GRUR 2017, 422). Weiter ist zu berücksichtigen, dass es der Beklagten selbst nach den gesetzlichen Vorschriften obliegt, Sicherheitsstandards einzurichten, die (weiteren) Scraping-Angriffen effektiv vorbeugen, so dass sie nicht von ihren Nutzern die Benennung konkreter Maßnahmen verlangen kann sondern selbst nach den effektivsten Mitteln forschen muss und diese dann einzusetzen hat.

Für den Klageantrag zu 2.) ist weiter das gemäß § 256 Abs. 1 ZPO erforderliche Feststellungsinteresse ist gegeben. Ein solches liegt bei einer Rechtsgutsverletzung bereits dann vor, wenn künftige Schadensfolgen nicht von vornherein ausgeschlossen sind, mag ein Schadenseintritt auch ungewiss sein.

Unter Berücksichtigung des Umstandes, dass hier personenbezogene Daten des Klägers im Wege des Scrapings erlangt worden sind, erscheint es bei lebensnaher Betrachtung nicht ausgeschlossen, dass es bei dem Kläger künftig zu materiellen Schäden, etwa durch erfolgreiche betrügerische Anrufe, kommt. Der Vorrang der Leistungsklage steht einem Feststellungsinteresse vorliegend nicht entgegen, da es sich um noch ungewisse Schadensersatzansprüche handelt, die mit der Leistungsklage noch nicht einklagbar sind.

II.

In dem ausgeurteilten Umfang ist die Klage auch begründet.

1. Dem Kläger steht gegen die Beklagte einen Anspruch auf Schadensersatz i.H.v. 500,00 EUR aus Art. 82 Abs. 1 DSGVO zu (Klageantrag zu 1)).

   Nach dieser Vorschrift hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder den Auftragsverarbeiter.

   a) Die Beklagte hat als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO gegen Art. 13 DSGVO verstoßen, da sie der ihr auferlegten Informations- und Aufklärungspflicht nicht in vollständigem Umfang nachgekommen. Denn es ist nicht feststellbar, dass die Beklagte den Kläger zum Zeitpunkt der Datenerhebung seiner Mobilfunknummer hinreichend über sämtliche Zwecke der Verarbeitung seiner Mobilfunknummer aufgeklärt hat.

      Nach Art. 13 Abs. 1 c) DSGVO hat der Verantwortliche bei der Erhebung personenbezogener Daten der betroffenen Person bereits zum Zeitpunkt der Erhebung der Daten die Zwecke mitzuteilen, für die die personenbezogenen Daten verarbeitet werden sollen. Sinn und Zweck dieser Regelung ist es, den Betroffenen eines Datenverarbeitungsprozesses unter Berücksichtigung der Grundsätze einer fairen und transparenten Verarbeitung von

personenbezogenen Daten nicht nur über die Existenz des Verarbeitungsvorganges selbst, sondern darüber hinaus auch über die Zwecke der Verarbeitung zu unterrichten (Ehmann/Selmayr/Knyrim, 2. Aufl. 2018, DS-GVO Art. 13 Rn. 1).

Bei der Erhebung der Telefonnummer des Klägers hat die Beklagte insoweit nicht hinreichend über die Verwendung der Nummer im Rahmen des Contact-Import-Tools informiert und aufgeklärt. In der seitens der Beklagten mit Anlage B8 (Bl. 261 f) vorgelegten Information werden zwar verschiedene Zwecke angegeben (Nutzung für Werbung, für die Zwei-Faktor-Authentifizierung, zur Anmeldung bei Vergessen der Anmeldeinformationen, zum Vorschlag möglicher Bekannter), für die „möglicherweise" die Telefonnummer eine Verwendung findet.

Völlig außen vor bleibt bei der Darstellung der Verwendungszwecke jedoch das Contact-Import-Tool und seine Funktionsweise: Dass die Beklagte anderen Nutzern einen Abgleich ermöglicht, ob in seinem Smartphone gespeicherte Telefonnummern einem Facebook-Nutzer zugeordnet werden können und dieser Nutzer dann mithin die Möglichkeit hat, die Nutzer der erfolgreich abgeglichenen Facebook-Konten als „Freunde" hinzuzufügen, selbst wenn der Nutzer sich bei den Einstellungen gegen eine Sichtbarkeit seiner Telefonnummer für andere entschieden hat, wird dort nicht erwähnt. Verwiesen wird allein auf die Datenrichtlinie, in der ausgeführt werde, wer die eigene Telefonnummer sehen könne.

Auch diese enthält jedoch keine Ausführungen zum CIT (vgl. Anlage B11, Bl. 265 ff.), gleiches gilt für die Informationen im Bereich „Handy-Einstellungen" sowie die Unterverlinkung durch einen Klick auf „Mehr dazu".

Gerade weil das CIT einen automatisierten Abgleich einer Nummer mit einem Facebook-Konto ermöglicht und dieser Abgleich auch bei abgelehnter Sichtbarkeit der Handynummer für andere ermöglicht wird, war jedoch dieser Verarbeitungszweck für den Kläger als Nutzer der Plattform bedeutsam. Auch ohne Hinweis auf ein mögliches Missbrauchspotential dieser Funktion – zu dem die Beklagte wohl nicht zusätzlich verpflichtet gewesen wäre – hätte es für einen Nutzer bei entsprechender Information über die bloße Funktionsweise des CIT Anlass gegeben, über die (freiwillige) Angabe der Telefonnummer nachzudenken oder aber Einstellungen am Account

vorzunehmen, um den gewünschten Privatsphäre-Status dennoch zu erreichen.

b) Die Beklagte hat darüber hinaus gegen Art. 25 DSGVO verstoßen.

Nach Art. 25 Abs. 2 SDGVO muss der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Die Maßnahmen müssen dabei insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Dem ist die Beklagte hier nicht nachgekommen.

Unstreitig waren (auch) beim Facebook-Account des Klägers die Suchbarkeitseinstellungen für die Nutzer automatisch so eingestellt, dass die Telefonnummer für jeden Dritten für einen Abgleich via CIT offenstand. Ohne Zutun des einzelnen Nutzers hat die Beklagte diese personenbezogenen Daten daher einer unbestimmten Vielzahl unbeteiligter Dritter zugänglich gemacht.

Die Beklagte kann sich auch nicht darauf berufen, dass eine Suchbarkeit der einzelnen Nutzer für die Ausübung der Plattform zwingend notwendig gewesen wäre. Ebenso wäre eine Kontakt-Suche der Nutzer allein über den Namen als solches möglich gewesen, was wesentlich weniger missbrauchsanfällig gewesenwäre und darüber hinaus allein an einer Information angesetzt hätte, die nach den zumindest in diesem Punkt den Nutzern transparent kommunizierten Bedingungen der Plattform stets öffentlich zugänglich war. Gerade für die Telefonnummer, die zum automatischen Kontakte-Import genutzt wurde, galt dies jedoch nicht.

Erschwerend kommt hinzu, dass die Privatsphäre-Einstellungen für die Telefonnummer auf der Plattform an zwei verschiedenen, miteinander nicht unmittelbar verlinkten Stellen vorgenommen werden mussten und die Datenschutzeinstellungen nach den vorgelegten Ausdrucken der

verschiedenen Hilfe- und Informationsseiten (vgl. die Anlagen B 1 ff.) insgesamt unübersichtlich und verwirrend gestaltet waren. Auch durch diese datenschutzunfreundliche Gestaltung hat die Beklagte das Risiko erhöht, dass Nutzer eine von ihnen eigentlich intendierte Plattformeinstellung, die auf die maximal mögliche Einhaltung der Privatsphäre ausgerichtete gewesen wäre, nicht vornahmen.

c) Zudem hat die Beklagte als Verantwortliche aufgrund unzureichender Sicherheitsmaßnahmen bezüglich der Nutzung des CIT auch gegen die Art. 32, 24, 5 DSGVO verstoßen.

Nach Art. 32 Abs. 1 Hs. 1 DSGVO haben der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Diesen Anforderungen genügten die beklagtenseits behaupteten Schutzmaßnahmen nicht.

Das Gericht verkennt dabei nicht, dass die Gewährleistung eines absoluten Schutzniveaus unmöglich und von der Beklagten mithin auch nicht verlangt werden konnte. Das Schutzniveau, welches vom Verantwortlichen eingehalten muss, ist jedoch jeweils an Größe und Eintrittswahrscheinlichkeit des Risikos zu bemessen, welches für die verarbeiteten personenbezogenen Daten besteht.

Sowohl Größe als auch Eintrittswahrscheinlichkeit sind vorliegend als erheblich zu bewerten. Das CIT ermöglicht einen unbefugten Zugang i.S.d. Art. 32 Abs. 2 DSGVO zu den personenbezogenen Daten der Nutzer. Bei einem solchen Zugang geht die entscheidende Aktivität vom Empfänger der Daten aus. Der Verantwortliche ermöglicht den unbefugten Abruf der Daten jedoch durch die Ausgestaltung der technischen Bedingungen des Datenabrufs durch Dritte, z.B. durch das Einräumen von Zugriffsrechten im Rahmen von Netzwerken oder durch die Einstellung in eine Datenbank, auf die auch Dritte zugreifen können (vgl. dazu Kühling/Buchner/Jandt,

Datenschutz-Grundverordnung, 3. Aufl. 2020, Art. 32 Rn. 34). So liegt der Fall hier, da das CIT zweckwidrig nicht nur zum Auffinden von persönlichen Kontakten auf Facebook, sondern auch zu einem automatisierten Abgleich einer Vielzahl von künstlich generierten Telefonnummern mit den Facebook-Konten zu Missbrauchszwecken genutzt werden konnte.

Dass diese Funktion ein „Einfallstor" für Scraping-Versuche darstellte, musste der Beklagten im Hinblick auf die weite Verbreitung von Datenscraping und auch im Hinblick auf die Bedeutung, die personenbezogene Daten bei kriminellen, technologie-gestützten Betrugsmachenschaften immer mehr einnehmen, klar gewesen sein. Insoweit trägt sie selbst vor, dem Scrapingrisiko durch diverse Maßnahmen Rechnung getragen haben zu wollen. Gerade im Hinblick auf den Schaden, der bei einem unbefugten Gebrauch der durch das CIT zusammengeführten Telefonnummer mit den öffentlich abrufbaren Daten des Facebook-Nutzers durch Phishing-Attacken, Identitätsdiebstahl und weiteren Missbrauch drohte, wäre es jedoch an der Beklagten gewesen, die CIT-Funktion effektiv und mithin auch zu Lasten des „Komforts" bei einer „legalen" Nutzung der Funktion weiter einzuschränken.

Dass eine solche Einschränkung möglich gewesen wäre, zeigt sich bereits an der Beschreibung, die die Beklagte selbst zu den von ihr über den Zeitverlauf ergriffenen Anti-Scraping-Maßnahmen liefert. Danach wurden Übertragungsbeschränkungen erst nach und nach angepasst; noch augenfälliger ist jedoch, dass tatsächlich effektive Maßnahmen erst, wie die Beklagte formuliert, „im Nachgang", also ex post ergriffen wurden. So wurden bei einem Telefonnummernabgleich nach dem Scraping-Vorfall „Trefferkonten" erst dann angezeigt, wenn der importierende Nutzer neben der abgefragten Telefonnummer einen Namen der Nummer zuordnen konnte, der dem Nutzernamen zumindest ähnelte oder der betroffene Nutzer den importierenden Nutzer bereits in seinen Kontakten führte. Wiederum später erfolgte eine Überarbeitung der CIT-Funktion dergestalt, dass nach Abgleich der Telefonnummern mit der Facebook-Datenbank nur noch eine Liste von Kontaktvorschlägen („People you may know-Funktion, PYMK-Funktion) angezeigt wurde, ohne dass eine Zuordnung zu den Telefonnummern vorgenommen wurde (Einzelheiten Beklagtenschriftsatz vom 04.05.2023, S. 22, Bl. 905 f.).

All diese Maßnahmen mögen das „Nutzererlebnis“ eingeschränkt haben, da durch diese Einschränkungen nicht mehr in jedem Fall sichergestellt wird, dass ein Telefonkontakt auch einer Facebook-Konto-Seite zugeordnet werden kann; ein „eingeschränktes Nutzererlebnis“ mag sich mittelbar auch negativ für die Beklagte auswirken, die auf eine extensive Nutzung der Konten angewiesen ist, an der sich Werbeeinnahmen als maßgebliche Einnahmequelle für sie ausrichten. In jedem Fall wären diese Maßnahmen aber auch vorher möglich und im Hinblick darauf auch zumutbar gewesen, dass sich das System der Datenabfrage allein über künstlich leicht generierbare „Telefonnummern“ von Anfang an als besonders missbrauchsanfällig darstellte, die einem Abgreifen potentiell ausgesetzten Daten ein erhebliches Betrugspotenzial aufwiesen, geeignete technisch-organisatorische Maßnahmen auch nach dem damaligen Stand der Technik zur Verfügung standen und sich die potenziellen Kosten für eine zusätzliche Sicherungsstufe im zumutbaren Rahmen hielten.

d) Soweit die Beklagte darüber hinaus auch gegen Art. 33 und 34 DSGVO verstoßen hat, sind diese Normverstöße für den geltend gemachten Schadensersatzanspruch des Klägers insoweit unbeachtlich, als dass auch eine Einhaltung der Informationspflichten (Meldung an die zuständige Aufsichtsbehörde / Unterrichtung des Klägers) den Schadenseintritt nicht mehr verhindert hätte, da der konkrete Scraping-Vorfall schon abgeschlossen war und lediglich im Hinblick auf zukünftige Verstöße früher Maßnahmen hätten ergriffen werden können.

e) Die Verletzung der Art. 13, 25 und 32 DSGVO ist auch vom Anwendungsbereich des Schadensersatzanspruches des Art. 82 DSGVO erfasst.

Nach Art. 82 Abs. 2 DSGVO besteht ein Schadenersatzanspruch, wenn nach ein Schaden durch eine nicht dieser Verordnung entsprechenden Verarbeitung verursacht wurde. Entsprechend der Legaldefinition des Art. 4 Ziffer 2 DSGVO zählt bereits das Erheben von Daten zur „Verarbeitung“ im Sinne der Verordnung; bereits mit der Erhebung personenbezogener Daten entstehen aber die Informations- und Aufklärungspflichten des Art. 13

DSGVO. Bereits zu diesem Zeitpunkt hat der Verantwortliche gegenüber dem Betroffenen umfangreiche Informationspflichten zu erfüllen; ein Verstoß gegen diese Vorschriften begründet mithin auch eine Schadensersatzpflicht nach Art. 82 Abs. 2 DSGVO.

Die in den Art. 25 und 32 DSGVO aufgeführten Verpflichtungen betreffen bereits nach ihrem Wortlaut die Datenverarbeitung als solche, ohne dass auf die Vorverlagerung der Legaldefinition des Art. 4 DSGVO zurückgegriffen werden müsste.

Nach der Formulierung des Art. 82 Abs. 2 DSGVO haftet der Verantwortliche für jede „nicht dieser Verordnung entsprechende Verarbeitung" (Abs. 2 S. 1). Mithin wird eine umfassende Haftung bei jedem noch so kleinen Verstoß statuiert, solange dieser nur kausal für den Schaden ist. Auf einen spezifisch drittschützenden Charakter der Norm kommt es nicht an. Da die Norm erkennbar einen umfassenden Schutz bezweckt, werden nicht nur materielle Rechtmäßigkeitsanforderungen sondern auch formale Vorschriften umfasst (Kühling/Buchner/Bergt, a.a.O., Art. 82 Rn. 22, m.w.N.).

f) Die Beklagte kann sich auch nicht gemäß Art. 82 Abs. 3 DSGVO exkulpieren. Danach wird der Verantwortliche von der Haftung nach Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Eine Verantwortlichkeit wäre nur dann nicht gegeben, wenn die Beklagte Sorgfaltsanforderungen erfüllt hätte und ihr nicht die geringste Fahrlässigkeit vorzuwerfen wäre (Kühling/Buchner/Bergt, a.a.O., Art. 82 Rn. 54).

   Wie oben dargelegt wäre der Beklagten jedoch sowohl eine ausreichende Aufklärung hinsichtlich der Verwendungszwecke der abgefragten Daten als auch das Ergreifen effektiver Sicherheitsmaßnahmen zum Ausschluss des Datenscrapings möglich gewesen. Dass diese Maßnahmen erforderlich gewesen wären, war für sie auch erkennbar.

g) Die dargelegten Verstöße gegen die DSGVO sind auch kausal für das Datenscrapping geworden.

Zur Überzeugung der Kammer sind auch die Telefonnummer des Klägers sowie die von ihm bei Facebook öffentlich einsehbaren persönlichen Daten „gescrapt" und ins Internet eingestellt worden. Soweit die Beklagte diesen Umstand noch im Schriftsatz vom 09.06.2023 (dort S. 3, Bl. 1262) mit Nichtwissen bestritten hat, ist dieses Bestreiten unbeachtlich. Der Beklagten – die im Rahmen des „Datenskandals" umfangreiche eigene Untersuchungen angestellt hat – ist es möglich ist, die vorgetragene Behauptung anhand ihrer eigenen Erkenntnisse zu verifizieren, so dass ein Bestreiten mit Nichtwissen unzulässig ist, vgl. § 138 Abs. 4 ZPO.

Bei einer ausreichenden Information des hiesigen Klägers hinsichtlich der Funktionsweise des CIT ist zur Überzeugung der Kammer davon auszugehen, dass der Kläger andere Einstellungen in seinem Benutzerprofil bezüglich der Suchbarkeit über seine Telefonnummer vorgenommen hätte. Gleiches gilt für einen Verstoß der Beklagten gegen die „Privacy-by-default"-Vorgabe des Art. 25 DSGVO: Hätte die Beklagte hier keine automatische Voreinstellung dergestalt vorgenommen, dass eine Suche über die Telefonnummer grundsätzlich jedem Dritten offensteht oder eine transparentere und leichter zugängliche Gestaltung der Einstellungsmöglichkeiten angeboten, hätte der Kläger im hiesigen Verfahren zur Überzeugung der Kammer eine solche Einstellung im späteren Verlauf selbst nicht aktiv eingestellt.

Der Kläger hat vorgetragen, nur wenige personenbezogene Rahmendaten in seinen Account eingepflegt zu haben und bezüglich der Sichtbarkeit seiner Daten die jeweils „privateste Option" ausgewählt zu haben. Diesen Vortrag hat die Beklagte in ihrem nachgelassenen Schriftsatz vom 09.06.2023 nicht bestritten, obgleich ihr als Plattformbetreiberin die jeweiligen Accounteinstellungen zugänglich waren. Nach lebensnaher Auslegung hätte der Kläger daher auch bei der Suchbarkeit entsprechende Einstellungen aktiviert. Den Vortrag der Beklagten zugrunde gelegt, dass bei Einstellung der Suchbarkeitsoptionen über die Telefonnummer auf „just me" ein Abgleich im Rahmen des CIT nicht mehr hätte vorgenommen werden können, hätte eine entsprechend angepasste Einstellung des Klägers das Datenscrapping verhindert, so dass auch hier eine Kausalität zu bejahen ist.

Eine Kausalität ist darüber hinaus aber insbesondere für den Verstoß der Beklagten gegen Art. 32 DSGVO zu bejahen. Wäre der Abruf der Facebook-Kontakte über das CIT frühzeitig an die Angabe eines weiteren Merkmals – wie später der Name des Nutzers – geknüpft gewesen, wäre es zum massenweisen unbefugten Abgriff der öffentlich einsehbaren Daten und ihrer Verknüpfung mit nicht freigegebenen Telefonnummern nicht gekommen.

h) Auch ein Schaden des Klägers ist vorliegend zu bejahen.

Der Begriff des Schadens ist nach Erwägungsgrund 146 Satz 3 der DSGVO weit und unter Berücksichtigung der Ziele der Verordnung auszulegen. Er umfasst sowohl materielle als auch immaterielle Schäden. Der Anspruch soll einen vollständigen und wirksamen Ersatz des erlittenen Schadens sicherstellen. Unter Berücksichtigung der Rechtsprechung des EuGH, die unter Bezugnahme auf den Effektivitätsgrundsatz verlangt, dass nationale Schadensersatzvorschriften zur Umsetzung europäischer Vorgaben über einen rein symbolischen Schadensersatz hinausgehen und eine abschreckende Wirkung aufweisen, ist er so zu bestimmen, dass Verstöße gegen die europarechtlichen Normen „unattraktiv" werden (Kühling/Buchner/Bergt, a.a.O., Art. 82 Rn. 17).

In der Rechtssache C-300/21 („Österreichische Post") hat der EuGH unter dem 04.05.2023 ferner entschieden, dass Art. 82 ABs. 1 DSGVO dahin auszulegen ist, dass er einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens im Sinne der Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grand an Erheblichkeit erreicht hat (EuGH, a.a.O., Rz. 51). Dabei sei insbesondere zu berücksichtigen, dass die DSGVO ausweislich ihres zehnten Erwägungsgrundes namentlich darauf abziele, innerhalb der Union ein gleichmäßiges und hohes Niveau des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten und zu diesem Zweck für eine unionsweit gleichmäßige und einheitliche Anwendung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten dieser Personen bei der Verarbeitung personenbezogener Daten zu sorgen. Die Annahme einer Erheblichkeitsschwelle stünde der bezweckten Kohärenz der Regelungen entgegen, da die Festlegung einer Schwelle je nach Beurteilung

durch die angerufenen Gerichte unterschiedlich hoch ausfallen könne (vgl. EuGH, a.a.O., Rz. 48f.)

Gleichzeitig hat der EuGH in seiner Entscheidung aber auch festgehalten, dass die Verhängung eines „Strafschadenseresatzes" nicht erforderlich ist, um eine auf Art. 82 DSGVO gestützte finanzielle Entschädigung als „vollständig und wirksam" anzusehen, wenn sie es nur im Übrigen ermöglicht, den aufgrund des Verstoßes gegen die Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen (EuGH, a.a.O., Rz. 58).

In Anbetracht dieser europarechtlichen Vorgaben und des hier konkret vorliegenden Sachverhalts liegt ein immaterieller Schaden des Klägers zur Überzeugung der Kammer vor. Unstreitig hat der Kläger seinen Face-Book-Account aufgrund des Datenscraping-Vorfalls nicht nur deaktiviert sondern – unter Inkaufnahme des Verlustes der Zugriffsmöglichkeit auf seine bei Facebook gespeicherten Daten – vollständig gelöscht. Bereits unter Berücksichtigung des Umstands, dass der Kläger den Account zum Zeitpunkt des Löschens über 10 Jahre in Gebrauch hatte und sich im Account bei lebensnaher Betrachtung eine erhebliche Daten- und „Erinnerungsmenge" gesammelt haben dürfte, lässt dieser Schritt eine spürbare Betroffenheit des Klägers erkennen.

Zur Überzeugung der Kammer sind ferner die vom Kläger angeführten, vermehrten Robocalls und Spam-SMS zumindest auch auf den Datenscraping-Vorfall zurückführbar. Im Übrigen dürfte aber allein die reelle Möglichkeit solcher betrügerischen Anrufe, die durch die unautorisierte Veröffentlichung der Klägerdaten im Darknet geschaffen wurde, ein Gefühl des Kontrollverlustes und des Ausgeliefertseins verursachen, das nach den Erwägungsgründen der DSGVO im Rahmen der Bestimmung eines immateriellen Schadens zu berücksichtigen ist.

Insgesamt erscheint im vorliegenden Einzelfall damit ein Schmerzensgeld in Höhe von 500 EUR für angemessen, um der Ausgleichs- und Genugtuungsfunktion sowie dem generalpräventiven Zweck des immateriellen Schadensersatzes hinreichend Rechnung zu tragen. Dabei war zum einen zu berücksichtigen, dass die Beklagte gegen mehrere Vorschriften der DSGVO verstoßen hat und – aufgrund der vorgenommenen Accountlöschung durch

den Kläger – auch eine deutliche Betroffenheit des Klägers belegt ist, die er im Rahmen seiner persönlichen Anhörung schlüssig vortragen konnte. Zu berücksichtigen war dabei auch, dass der Kläger ausweislich der von der Beklagten selbst vorgelegten Einstellungen des klägerischen Facebook.-Accounts eine besondere Vorsicht bei der Freigabe seiner Daten walten ließ.

Andererseits war aber auch mit in die Wertung einzustellen, dass sich ein durch das Scraping gesetzte Betrugsrisiko bislang unstreitig nicht realisiert hat und aufgrund des seit dem Vorfalls liegenden Zeitablaufs an Wahrscheinlichkeit verliert. Die festgesetzten 500 EUR erscheinen damit insgesamt auch ausreichend.

2. Auch der mit dem Klageantrag zu 2 geltend gemachte Feststellungsantrag ist begründet. Gemäß vorstehender Ausführungen hat der Kläger gegenüber der Beklagten wegen Verletzung der DS-GVO einen Anspruch auf Schadensersatz nach Art. 82 DSGVO. Die jeweiligen Gesetzesverletzungen sind - wie bereits erörtert - zudem kausal für den unkontrollierten Datenverlust des Klägers. Dass es in der Folgezeit zu erfolgreichen Betrugsanrufen o.ä. unter Ausnutzung der gescrapten Daten kommen kann, ist zumindest nicht sicher ausgeschlossen.

3. Der mit dem Klageantrag zu 3. geltend gemachte Unterlassungsanspruch steht dem Kläger hingegen nicht zu. Unstreitig hat der Kläger seinen Facebook-Account bereits gelöscht, so dass es an der für die Bejahung eines Unterlassungsanspruchs gem. §§ 823 Abs. 2, 1004 BGB notwendigen Wiederholungsgefahr fehlt.

4. Dem Kläger steht auch der mit dem Klageantrag zu 4 verfolgte Auskunftsanspruch nach Art. 15 DS-GVO nicht zu. Ihm ist nämlich einerseits bekannt, welche Daten durch den Scraping-Vorfall erlangt wurden und zum anderen hat die Beklagte mehrfach versichert keine „Rohdaten" des Scraping-Vorfalls zu halten. Mit Schriftsatz vom 09.06.2023 hat die Beklagte weiter in angemessener Seite mitgeteilt, welche Daten im Rahmen des Scrapings abgegriffen werden konnten. Weitergehende Auskunft kann der Kläger nicht verlangen.

5. Die vorgerichtlichen Rechtsanwaltskosten sind als Teil des zu ersetzenden Schadens gemäß Art. 82 Abs. 1 DSGVO zu erstatten. Aufgrund der Schwierigkeit der Sach- und Rechtslage war die Hinzuziehung eines Rechtsanwalts zur effektiven Durchsetzung der klägerischen Ansprüche erforderlich und notwendig. Ausgehend von einem Wert des berechtigten Verlangens des Klägers zum Zeitpunkt der außergerichtlichen Tätigkeit in Höhe von 1.500 EUR (vgl. hierzu die untenstehende Streitwertfestsetzung und die Verteilung auf die einzelnen Klageanträge) ergibt dies Kosten in Höhe von 220,27 EUR (1,3-fache Geschäftsgebühr in Höhe von 165,10 EUR nebst Auslagenpauschale Nr. 7001 und 7002 VV RVG zzgl. 19% MwSt.).

III.

Die Kostenentscheidung beruht auf § 92 ZPO, die Entscheidung zur vorläufigen Vollstreckbarkeit auf den §§ 708 Nr. 11, 711, 709 ZPO.

Der Streitwert wird gem. § 63 Abs. 2 ZPO auf 2.500 EUR festgesetzt und auf die einzelnen Klageanträge wie folgt neu verteilt:

Der Streitwert für den Klageantrag zu 1.) ist nach der Höhe des geltend gemachten immateriellen Schadensersatzanspruchs auf 1.000 EUR festzusetzen.

Der Wert des Feststellungsantrags zu Ziffer 2. der Klageschrift ist an der Höhe eines denkbaren zukünftigen materiellen (Betrugs-)Schadens durch die weiterhin bestehende Missbrauchsmöglichkeit der unbefugt veröffentlichten Daten zu orientieren und ebenfalls auf 1.000 EUR festzusetzen.

Dem Unterlassungs-Antrag zu Ziffer 3. der Klageschrift ist hingegen kein eigener Wert beizumessen, da das Facebook-Konto im Zeitpunkt der Klageeinreichung bereits fast ein Jahr gelöscht war und die Beklagte seitdem mithin auch keine Daten des Klägers mehr vorhält oder verarbeitet.

Bezüglich des Auskunftsanspruchs in Ziffer 4. der Klageschrift geht die Kammer unverändert von einem Streitwert von 500,00 EUR aus. Der hälftige Wert des behaupteten immateriellen Schadensersatzanspruchs erscheint dabei angemessen.

[redacted]

Beglaubigt
Urkundsbeamter/in der Geschäftsstelle
Landgericht Bonn

LANDGERICHT NORDRHEIN-WESTFALEN