Beglaubigte Abschrift

13 O 125/22

Landgericht Bonn

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

des

Klägers,

Prozessbevollmächtigte:

gegen

die Meta Platforms Ireland Ltd., vertreten durch den Director Gareth Lambe, 4 Grand Canal Sqaure, Dublin 2, Irland,

Beklagte,

Prozessbevollmächtigte:

hat die 13. Zivilkammer des Landgerichts Bonn
aufgrund mündlicher Verhandlung vom 03.03.2023
durch den Richter am Landgericht Sobotka als Einzelrichter

für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger 250,00 € nebst Jahreszinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 23.07.2022 zu zahlen.

Die Beklagte wird verurteilt, an den Kläger weitere 159,94 € nebst Jahreszinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 23.07.2022 zu zahlen.

Im Übrigen wird die Klage abgewiesen.

2. Die Kosten des Rechtsstreits werden dem Kläger auferlegt.
3. Das Urteil wird für vorläufig vollstreckbar erklärt. Der jeweilige Vollstreckungsschuldner kann die Vollstreckung des jeweiligen Vollstreckungsgläubigers durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht der jeweilige Vollstreckungsgläubiger vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrags leistet.
4. Die Berufung wird zugelassen.

Tatbestand:

Der Kläger nimmt die Beklagte wegen behaupteter datenschutzrechtlicher Verstöße im Zeitraum von Januar 2018 bis September 2019 in Anspruch.

Die Beklagte betreibt das sog. soziale (Internet-)Netzwerk "Facebook". Die Plattform ermöglicht es registrierten Benutzern, eine Profilseite mit personenbezogenen Daten einschließlich Lichtbildern zu erstellen und diese mit anderen registrierten Benutzern, aber auch der Allgemeinheit, zu teilen. Wer Zugriff auf welche Daten erhält, lässt sich nach einem vorgegebenen Schema ("Freunde", [auch] "Freunde von Freunden", "Öffentlich") in den von der Beklagten angebotenen Einstellungen zur Privatsphäre festlegen. Immer "Öffentlich" einzusehen sind dabei Name, Geschlecht und Profilidentifikationsnummer des Benutzers. Zu den der Profilseite hinzufügbaren personenbezogenen Daten gehört auch die Mobiltelefonnummer. Hat man diese seinem Profil hinzugefügt, gibt es eine zusätzliche Funktion, die es ermöglicht, einen Benutzer mit seiner Profilseite anhand der Mobiltelefonnummer aufzufinden. Für diese Funktion stellte die Beklagte eine Software namens "Contact-Import-Tool" (Werkzeug zum Hinzufügen von Kontakten) zur Verfügung. Gab man dort eine Zahlenfolge ein, prüfte die Software, ob es sich dabei um eine von einem Facebook-Benutzer hinterlegte Mobiltelefonnummer handelt und stellte eine Verknüpfung zu der entsprechenden Profilseite her. Die Software wurde üblicherweise so angeboten und eingesetzt, dass sie gemäß ihrer Funktionsweise automatisiert das Mobiltelefonadressbuch des Benutzers analysiert. Wer diese Suchfunktion nutzen kann ("Freunde", [auch] "Freunde von Freunden", "Alle", ab Mai 2019 außerdem:

"Nur ich"), konnte der Benutzer mittels einer von der oben beschriebenen Einstellungsmöglichkeit separaten Einstellung in den Privatsphäreeinstellungen festlegen. Über Funktion und Bedeutung der Privatsphäreeinstellungen informierte die Beklagte ihre Benutzer im sog. Hilfebereich gemäß der Anlagen B1 bis B7, auf deren Inhalt Bezug genommen wird.

Im April 2021 wurden im Internet frei zugänglich Datensätze mit den personenbezogenen Daten von ca. 533 Millionen Facebook-Benutzern veröffentlicht, wobei ein Datensatz grundsätzlich aus der Mobiltelefonnummer und den auf der Profilseite des jeweiligen Benutzers öffentlich einsehbaren Daten wie beispielsweise Name, Vorname, Geschlecht und Arbeitsplatz bestand. Die Datensätze wurden im Zeitraum von Januar 2018 bis September 2019 durch Unbekannte dergestalt generiert, dass in das Contact-Import-Tool automatisiert - und nach dem Vortrag des Klägers: wahllos - Zahlenfolgen eingegeben wurden. Stellte die Software - entsprechend ihrer Funktionsweise - fest, dass es sich dabei um die Mobiltelefonnummer eines registrierten Facebook-Benutzers handelte, griffen die Unbekannten - ebenfalls automatisiert - die auf der verknüpften Profilseite öffentlich zugänglichen personenbezogenen Daten ab (sog. Scraping) und kombinierten sie mit der - gemäß ihrem Vorgehen - "erratenen" Mobiltelefonnummer. Die entsprechende Funktion des Contact-Import-Tools wurde von der Beklagten im Nachgang an den Vorfall deaktiviert.

Der Kläger ist seit über 10 Jahren mit der Profilidentifikationsnummer bei Facebook angemeldet und hat dort auch seine Mobiltelefonnummer hinterlegt. Im Zeitraum des Scraping-Vorfalles hatte er die Datenschutzeinstellung betreffend die Sichtbarkeit seiner Mobiltelefonnummer so gesetzt, dass diese nur für ihn sichtbar war. Die Datenschutzeinstellung betreffend die Auffindbarkeit seiner Profilseite über seine Mobiltelefonnummer war so gesetzt, dass "Alle" ihn auffinden konnte (siehe Seite 36 der Klageerwiderung = Bl. 173 d.A.). Der betreffend den Kläger veröffentlichte Datensatz lautet wie folgt (siehe Seite 13 des Schriftsatzes vom 24.11.2022 = Bl. 328 d.A.):

Dabei handelt es sich um Mobiltelefonnummer, Profilidentifikationsnummer, Namen, Geschlecht und Arbeitsstätte des Klägers, welche er öffentlich einsehbar auf seiner Profilseite hinterlegt gehabt hatte.

Der Kläger beauftragte - zu Kosten von 887,03 €, bestehend aus einer 1,3 Geschäftsgebühr aus einem Gegenstandswert von 8.501,00 € zuzüglich 20 € Auslagenpauschale und 19 % Umsatzsteuer - seine jetzigen Prozessbevollmächtigten mit der vorgerichtlichen Rechtsverfolgung und ließ die Beklagte mit E-Mail-Schreiben vom 09.06.2021 (Anlage K1 = Bl. 52 ff. d.A.) im Wesentlichen gleichlautend mit den Klageanträgen in Anspruch nehmen. Betreffend den geltend gemachten Auskunftsanspruch heißt es dort:

> *Wir fordern Sie hiermit auf, unserer Mandantschaft nach Artikel 15 Absatz 1 DS-GVO unentgeltlich und schriftlich*
>
> ***A U S K U N F T***
>
> *darüber zu erteilen, ob Sie unsere Mandantschaft betreffende personenbezogene Daten unter der oben genannten E-Mail-Adresse im Zusammenhang mit dem im April 2021 bekannt gewordenen Datenschutzvorfall verarbeiten (Definition des Begriffs "Verarbeitung" siehe Art. 4 Nr. 2 DS-GVO).*
>
> *Sofern Sie dies bejahen, schließen wir **nachfolgende Fragen** an, welche von Ihnen ebenfalls unentgeltlich und schriftlich zu beantworten sind:*
>
> 1. *Welche, unsere Mandantschaft betreffenden, personenbezogenen Daten sind ganz konkret bei Ihnen abhanden gekommen?*
> 2. *Wo und zu welchem Zweck bzw. zu welchen Zwecken wurden diese, unsere Mandantschaft betreffende, personenbezogenen Daten verbreitet?*
> 3. *Wann - zu welchem Zeitpunkt oder in welchem Zeitraum - sind diese, unsere Mandantschaft betreffende, personenbezogenen Daten bei Ihnen abhandengekommen?*
> 4. *Wie oft wurden diese, unsere Mandantschaft betreffende personenbezogenen Daten abgefragt?*
> 5. *Wurde diese bei Ihnen bestehende Sicherheitslücke durch mehrere Unbefugte ausgenutzt? Sofern ja, von wem?*
> 6. *Welche zukünftigen Maßnahmen wurden und werden von Ihnen ergriffen, um eine Wiederholungsgefahr im Sinne des Bestehens von ähnlichen Sicherheitslücken auszuschließen?*
>
> (Hervorhebungen im Original)

Die Beklagte reagierte mit Schreiben vom 23.08.2021 (Anlage K2 = Bl. 80 ff. d.A.). Betreffend den Auskunftsanspruch heißt es dort:

> *Facebook Irland hält keine Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten enthalten. Auf Grundlage der bislang vorgenommenen Analysen ist es Facebook Ireland jedoch gelungen, der Nutzer ID Ihres*

Mandanten die folgenden Datenkategorien zuzuordnen, die nach unserem Verständnis in den durch Scraping abgerufenen Daten erscheinen und mit den auf dem Facebook-Profil Ihres Mandanten verfügbaren Informationen übereinstimmen (die "Datenpunkte"):

Nutzer ID

Vorname

Nachname

Land

Geschlecht

Darüber hinaus ist nach unserem Verständnis auch die Telefonnummer Ihres Mandanten in den durch Scraping abgerufenen Daten enthalten, wobei diese nach unserem Verständnis, wie oben beschrieben, von den Scrapern unter Anwendung der Methode der Telefonnummernaufzählung bereitgestellt und gerade nicht vom Facebook-Nutzerprofil Ihres Mandanten abgerufen wurde.

Der Kläger behauptet, die Beklagte habe sich in Ansehung des Scraping-Vorfalles datenschutzrechtlicher Verstöße schuldig gemacht. Sie habe es unterlassen, sowohl dem Stand der Technik entsprechende Sicherheitsvorkehrungen zu ergreifen, um den automatisierten Missbrauch des Contact-Import-Tool zu verhindern, als auch ihn - den Kläger - ausreichend über Existenz und datenschutzrechtliche Bedeutung der Suchfunktion anhand der Mobiltelefonnummer sowie die Funktionsweise des Contact-Import-Tool aufzuklären. Durch den streitgegenständlichen Vorfall habe er einen spürbaren Kontrollverlust über seine Daten erlitten. So sei es zu einem massiven Anstieg von betrügerischen Kontaktversuchen per E-Mail, ferner auch per SMS und Telefon gekommen. Wegen der Einzelheiten wird auf den schriftsätzlichen Vortrag einschließlich der zugehörigen Lichtbilder sowie die Ausführungen des Klägers im Rahmen der persönlichen Anhörung (Sitzungsprotokoll vom 03.03.2023 = Bl. 1039 ff. d.A.) Bezug genommen.

Der Kläger beantragt,

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

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

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

   a. seine personenbezogenen Daten, 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 zu verurteilten, ihm Auskunft über die ihn betreffenden personenbezogenen Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten,

5. die Beklagte zu verurteilen, an ihn 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 aus unterschiedlichen Gründen, wegen derer auf die schriftsätzlichen Ausführungen Bezug genommen wird, bereits unzulässig, jedenfalls aber unbegründet.

Schadensersatzansprüche des Klägers seien ausgeschlossen, weil Art. 82 Abs. 1 DSGVO seinem Anwendungsbereich nach eine unzulässige Datenverarbeitung voraussetze, welche ebenso wenig vorliege wie ein sonstiger Verstoß gegen Vorschriften der DSGVO. Hierzu behauptet sie, keine unzureichenden technischen Sicherungsmaßnahmen ergriffen zu haben. So beschäftige sie ein Team von Experten, das Aktivitätsmuster und Verhaltensweisen, die typischerweise mit automatisierten Computeraktivitäten in Zusammenhang stehen, identifizieren, unterbrechen und nach Möglichkeit verhindern soll. Eine der Maßnahmen seien Übertragungsbeschränkungen, die die Anzahl von Anfragen von bestimmten Daten reduzieren, welche pro Nutzer oder von einer bestimmten IP-Adresse in einem bestimmten Zeitraum gemacht werden können. Es kämen außerdem sog. Captcha-Abfragen zum Einsatz. Sie gehe außerdem mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren gegen sog. Scraper vor. Die Anfragen über das Contact-Import-Tool hätten vor diesem Hintergrund nicht wahllos erfolgen können, weil sie dann durch die Sicherungsmaßnahmen abgeblockt worden wären. Im Übrigen könne - was unstreitig ist - technisch kein 100%iger Schutz vor Vorfällen wie dem streitgegenständlichen sichergestellt werden. Wegen der Einzelheiten wird auf den Sachvortrag auf Seiten 29 bis 32 der Klageerwiderung (Bl. 166 bis 169 d.A.) Bezug genommen.

Die Beklagte ist weiter der Ansicht, dem Kläger sei kein Schaden entstanden, da - insoweit unstreitig - die veröffentlichten, der Profilseite des Klägers entnommenen Daten ohnehin öffentlich einsehbar gewesen seien und die Mobiltelefonnummer von den Unbekannten generiert und nicht von der Beklagten zur Verfügung gestellt worden sei. Vor diesem Hintergrund sei ein "Kontrollverlust" nicht ersichtlich. Auskunftsansprüche des Klägers seien durch das vorgerichtliche Schreiben vom 23.08.2021 erfüllt worden.

Die Klageschrift vom 03.06.2022 ist der Beklagten am 22.07.2022 zugestellt worden. Mit - von der Beklagten mit Rechtsmitteln angefochtener - Entscheidung vom 25.11.2022 (Anlage K4 = Bl. 465 ff. d.A.) hat die irische Datenschutzbehörde wegen des streitgegenständlichen Vorfalls Verstöße der Beklagten gegen Art. 25 Abs. 1 und 2 DSGVO festgestellt.

Entscheidungsgründe:

Die Klage ist nur teilweise zulässig und, soweit sie zulässig ist, nur teilweise begründet.

I.

Die Klage ist nur teilweise zulässig.

Der Klageantrag zu Ziffer 1 ist zulässig, insbesondere ist der Streitgegenstand hinreichend bestimmt und steht - entgegen der Ansicht der Beklagten - nicht in einem unzulässigen Alternativverhältnis zu sich selbst. Der Kläger trägt einen einheitlichen Lebenssachverhalt vor, aus welchem er einen Anspruch auf ein einheitliches Schmerzensgeld geltend macht. Dadurch, dass er sich auf mehrere datenschutzrechtliche Verstöße der Beklagten beruft, behauptet er keine alternativen Geschehensabläufe, auf die er seinen Anspruch wahlweise stützt und die er in eine bestimmte Reihenfolge bringen muss, sondern Umstände, die ggf. als Bemessungsfaktoren im Rahmen des Schmerzensgeldanspruches zu berücksichtigen sind.

Der Klageantrag zu Ziffer 2 ist unzulässig, da der Kläger nicht dargelegt hat, dass ihm künftige Schäden drohen, für welche die Beklagte rechtlich einzustehen hat. Wegen Einzelheiten wird auf die Ausführungen zur Zurechnung im Rahmen der Begründetheit des Klageantrags zu Ziffer 1 Bezug genommen.

Der Klageantrag zu Ziffer 3 ist insgesamt unzulässig.

Der Teilantrag nach a) ist als Unterlassungsantrag unzulässig, weil in der Sache kein Unterlassungsanspruch, sondern ein Leistungsanspruch geltend gemacht wird. Der Kläger begehrt dort bei verständiger Würdigung nicht, dass die Beklagte es gänzlich unterlässt, die dort genannten Daten Dritten zugänglich zu machen, sondern er begehrt, dass sie zu diesem (grundsätzlich gewünschten) Zweck die "nach dem Stand der Technik möglichen Sicherheitsmaßnahmen [vorsieht]". Aber auch als Leistungsantrag ist er unzulässig, weil er nicht im Sinne des § 253 Abs. 2 Nr. 2 ZPO hinreichend bestimmt ist. Der gewählten Formulierung lässt sich nicht entnehmen, welche konkreten Maßnahmen die Beklagte im Verurteilungsfalle zu treffen hätte. Eine Zwangsvollstreckung wäre vor dem geschilderten Hintergrund nicht möglich.

Dem Teilantrag nach b) fehlt es am allgemeinen Rechtsschutzbedürfnis. Soweit der Kläger dort begehrt, dass die Beklagte seine Mobiltelefonnummer nicht auf

Grundlage seiner aktuellen, von ihm unwirksamen gehaltenen Einwilligung verwendet, mag er diese zurückziehen bzw. die von ihm gewünschten Einstellungen, die er im Detail selbst in der Klageschrift beschreibt, vornehmen. Eine hierauf gerichtete Unterlassungsklage stellt sich vor dem geschilderten Hintergrund als rechtsmissbräuchlich dar.

Der Klageantrag zu Ziffer 4 ist unzulässig, weil er nicht im Sinne des § 253 Abs. 2 Nr. 2 ZPO hinreichend bestimmt ist. Der gewählten und als unglücklich zu bezeichnenden Formulierung lässt sich nicht - auch nicht durch wohlwollende Auslegung - entnehmen, was tatsächlich gewollt ist.

Der Hauptaussagesatz lautet: "Die Beklagte wird verurteilt[,] der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen [...].". Diese Formulierung ist zu allgemein gefasst und entspricht offensichtlich nicht dem Rechtsschutzziel des Klägers, dem die von der Beklagten verarbeiteten Daten bekannt sein dürften, da er sie ihr selbst im Rahmen der Anmeldung und Pflege seines Benutzerprofils zur Verfügung gestellt hat.

Zwar schränkt er den Hauptsatz sodann durch einen Nebensatz ein ("[...] namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten"). Schon das Wort "namentlich" passt von seinem Sinngehalt her allerdings nicht zu dem vorangegangenen Satzteil. Es wird auch kein Bezug zu dem streitgegenständlichen Scraping-Vorfall hergestellt; ob dies gewollt ist oder nicht, lässt sich auch der Klagebegründung nicht zweifelsfrei entnehmen. Unklar bleibt schließlich, was mit "Empfänger" gemeint ist. Unstreitig ist der Scraping-Vorfall durch Unbekannte verübt worden. Welche Auskunft erwartet der Kläger an dieser Stelle?

Eine Zwangsvollstreckung wäre vor dem geschilderten Hintergrund insgesamt nicht möglich. Im Übrigen sei erwähnt, dass die Beklagte durch das vorgerichtliche Schreiben vom 23.08.2021 das wesentliche berechtigte Informationsinteresse des Klägers - und sei es durch die Auskunft, dass ihr keine (weiteren) Informationen vorliegen - bedient haben dürfte.

Der Klageantrag zu Ziffer 5 ist als allgemeiner Leistungsantrag zulässig.

II.

Soweit die Klage zulässig ist, ist sie nur teilweise begründet.

1.

(Klageantrag zu Ziffer 1)

Der Kläger hat gegen die Beklagte einen Anspruch auf Schadensersatz in Form eines Schmerzensgeldes in Höhe von 250,00 € (Art. 82 Abs. 1 DSGVO).

a.

Nach dieser Vorschrift steht einer Person, der wegen eines Verstoßes gegen die Vorschriften der DSGVO ein immaterieller Schaden entstanden ist, ein Anspruch auf Schadensersatz gegen die Verantwortliche zu. Diese Voraussetzungen liegen vor.

Indem die Beklagte es unterlassen hat, das Contact-Import-Tool technisch so abzusichern, dass automatisierte Abrufe mit beliebigen Ziffernfolgen ausgeschlossen gewesen sind, hat sie gegen ihre Pflicht zur "Integrität und Vertraulichkeit" gemäß Art. 5 Abs. 1 Buchst. f), Art. 25 Abs. 1 und 2 sowie Art. 32 Abs. 1 DSGO verstoßen. Danach müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Hierzu trifft die Verantwortliche 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, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Derartige Maßnahmen hat die Beklagte nicht (in ausreichendem Maß) ergriffen. Die entsprechende Behauptung des Klägers hat das Gericht diesem Urteil als unstreitig zugrunde zu legen, da die Beklagte ihr nicht in einer den prozessualen Substantiierungsanforderungen genügenden Weise entgegengetreten ist (§ 138 Abs. 2 ZPO).

Die Behauptung des Klägers ist zunächst schlüssig. Der Umstand, dass es zu dem streitgegenständlichen Vorfall überhaupt gekommen ist, begründet nach der Lebenserfahrung zumindest den Verdacht, dass unzureichende technische und organisatorische Maßnahmen ergriffen worden waren. Zwar ist auch nach der DSGVO kein absoluter Schutz gefordert; die Beklagte behauptet jedoch selbst nicht, und erst recht nicht mit der gebotenen prozessualen Substanz, dass der

streitgegenständliche Vorfall technisch nicht zu verhindern gewesen wäre. Die Behauptung des Klägers stellt sich vor diesem Hintergrund und eingedenk der Erwägung, dass der Kläger keine Einsicht in die technischen Maßnahmen der Beklagten hat, nicht als "ins Blaue hinein" aufgestellt dar.

Der Beklagten hätte es vor diesem Hintergrund oblegen darzulegen, welche konkreten technischen Maßnahmen in Bezug auf die Zweckentfremdung des Contact-Import-Tools in dem hier gegenständlichen Zeitraum ergriffen gewesen waren. Dem ist die Beklagte nur unzureichend nachgekommen. Zwar führt sie aus, dass sie u.a. die Prüfung von IP-Adressen vorgenommen und sog. Captcha-Abfragen eingesetzt habe. Diese Ausführungen sind jedoch zu allgemein gehalten. Es bleibt unklar, in welchem konkreten Zeitraum welche konkreten Maßnahmen konkret in Bezug auf das Contact-Import-Tool verwendet wurden. Wie sind diese Maßnahmen technisch konkret umgesetzt worden? Nach wie vielen Anfragen wurde eine IP-Adresse für wie lange gesperrt? Wie viele Anfragen waren nach der erfolgreichen Bewältigung einer Captcha-Abfrage möglich? Wie viele Anfragen pro Zeitraum ließ die Beklagte allgemein zu? Vortrag zu diesen naheliegenden Fragen fehlt, zumal auffällt, dass die Ausführungen unter dem Gliederungspunkt "Reaktion der Beklagten auf den Scraping-Sachverhalt" (Hervorhebung durch das Gericht) erfolgen und auch deshalb zweifelhaft ist, ob und ggf. in welchem Umfang welche Maßnahmen überhaupt bereits im Zeitpunkt des streitgegenständlichen Scraping-Vorfalls implementiert gewesen waren. Die von der Beklagten angeführten Maßnahmen "Unterlassungsaufforderungen", "Kontosperrungen" und "Gerichtsverfahren gegen sog. Scraper" können ihrer Natur erst nach dem Beginn eines Scrapings erfolgen und stellen, wenngleich sie abschreckenden Wirkung entfalten können mögen, keine technischen Abwehrmaßnahmen dar.

Solche Maßnahmen hätten aber ergriffen werden müssen, um eine angemessene Sicherheit der von der Beklagten verarbeiteten Daten des Klägers vor unbefugter und unrechtmäßiger Verarbeitung zu gewährleisten (siehe die nachstehenden Ausführungen). Das Missbrauchspotential der beschrieben Funktion hat für die Beklagte auch schon vor dem streitgegenständlichen Vorfall auf der Hand liegen müssen, was sie durch ihren - wenn auch unzureichenden - Vortrag selbst einräumt (Gliederungspunkt "Scraping ist im Internet allgegenwärtig" auf Seite 25 der Klageerwiderung). Soweit die Beklagte in diesem Zusammenhang bestreitet, dass bei dem Scraping-Vorfall wahllose Ziffernfolgen verwendet worden seien, weil in diesem Fall die Anfragen durch die getroffenen Sicherheitsvorkehrungen verhindert worden wären, ist dieser Vortrag schon deshalb unbeachtlich, weil er - wegen des unzureichenden Vortrags zu den getroffenen Sicherheitsvorkehrungen, siehe oben -

zirkelschlüssig ist. Unabhängig davon hat sich die Beklagte nicht dazu erklärt, ob - und ggf. warum nicht - ihr insoweit Protokolle vorliegen, aus denen die Anfragen konkret hervorgehen. Auch insoweit ist die Beklagte ihrer Darlegungslast nicht nachgekommen.

b.

Durch den Verstoß ist es zu einer unzulässigen Datenverarbeitung i.S.d. Art. 6 Abs. 1 DSGVO gekommen.

Personenbezogene Daten i.S.d. Art. 4 Nr. 1 DSGVO liegen vor, da sich die Mobiltelefonnummer des Klägers und die auf seiner Facebook-Profilseite öffentlich einsehbaren Daten auf eine namentlich identifizierte bzw. identifizierbare natürliche Person beziehen.

Die Daten sind i.S.d. Art. 4 Nr. 2 DSGVO "verarbeitet" worden, da eine "Verknüpfung" (von Mobiltelefonnummer mit den auf der Facebook-Profilseite öffentlich einsehbaren Daten) vorliegt. Der Annahme einer Verknüpfung steht nicht entgegen, dass aus Sicht der Beklagten sämtliche Daten einschließlich der Mobiltelefonnummer ohnehin bereits mit der Person des Klägers verknüpft gewesen waren. Denn maßgeblich ist insoweit die Sichtweise der verarbeitenden Person - bei der es sich unstreitig nicht um eine der Beklagten "unterstellte" natürliche Person gehandelt hat (vgl. § 32 Abs. 4 DSGVO) -, die die Verknüpfung aus ihrer Sicht erst erzeugt hat.

Die Verarbeitung ist unzulässig gewesen. Dies setzt voraus, dass mindestens einer der im Katalog des Art. 6 Abs. 1 DSGVO aufgeführten Rechtfertigungstatbestände erfüllt ist. Daran fehlt es. Für die Buchstaben d) bis e) ist dies offensichtlich. Der Kläger hat auch keine Einwilligung zu der Verarbeitung gemäß Buchstabe a) erteilt, denn unstreitig sind die Privatsphäreeinstellungen bezüglich der Sichtbarkeit der Mobiltelefonnummer des Klägers so gesetzt gewesen, dass sie nicht öffentlich einsehbar gewesen ist.

Der Kläger hat auch keine Einwilligung dadurch erteilt, dass die für sein Benutzerkonto geltende Privatsphäreeinstellung betreffend die Auffindbarkeit seines Profils mittels Mobiltelefonnummer auf "Alle" gesetzt gewesen ist. Denn der Kläger hat diese Einstellung unstreitig nicht willentlich selbst gesetzt, sondern es hat sich dabei um die Standardeinstellung im Zeitpunkt der Angabe der Mobiltelefonnummer

gehandelt. Hierdurch hat die Beklagte gegen ihre Pflicht zu datenschutzfreundlichen Voreinstellungen gemäß Art. 25 Abs. 2 DSGVO verstoßen. Danach trifft die Verantwortliche geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden, insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Hierfür spielt es keine Rolle, ob der "Zugang" dadurch erfolgt, dass die Daten originär abgerufen werden können (hier bezüglich der Mobiltelefonnummer nicht der Fall) oder ob die Beklagte die Zugehörigkeit einer geratenen Telefonnummer zu einem bestimmten Benutzer gegenüber "Allen" bestätigt (so der Fall hier).

Unabhängig davon hätte sich eine Einwilligung nicht darauf erstreckt, auch Personen, denen nicht bereits zuvor bekannt gewesen ist, wem die verwendete Mobiltelefonnummer "gehört", zu gestatten, die Suchfunktion des Contact-Import-Tools zu nutzen. Denn es ist unstreitig nicht der Zweck des Contact-Import-Tools gewesen, eine Mobiltelefonnummer neu mit einer Person zu verknüpfen, sondern bereits bestehende Kontakte darauf zu prüfen, ob sie über eine Facebook-Profilseite verfügen. Wäre dies anders gewesen, so wäre eine unterstellte Einwilligung des Klägers auch deshalb unwirksam, weil die Beklagte den Kläger nicht ausreichend über diese Möglichkeit aufgeklärt gehabt hätte, wie sich den beklagtenseits vorgelegten Anlagen B1 bis B7 entnehmen lässt. Daran ändert es nichts, dass die entsprechende Datenschutzeinstellung sprachlich auf "Alle" lautet, da einem durchschnittlichen Benutzer nicht ohne weiteres bewusst sein muss, dass das Contact-Import-Tool auch mit von ihm nicht bekannten Personen "erratenen" Mobiltelefonnummern genutzt werden kann.

c.

Sowohl für die Verletzung der Integritäts- und Vertraulichkeitspflicht als auch die hierdurch ermöglichte unzulässige Datenverarbeitung ist die Beklagte i.S.d. Art. 82 Abs. 2 und 3 DSGVO "verantwortlich". Maßgeblich hierfür ist, wem die Verstöße zuzurechnen sind. Dabei erfolgt die Zurechnung der Verletzung der Integritäts- und Vertraulichkeitspflicht bereits daraus, dass es das eigene Unterlassen der Beklagten gewesen ist, das die Pflichtverletzung begründet. Die unzulässige Datenverarbeitung ist zwar nicht unmittelbar durch die Beklagte erfolgt, sondern stellt ein Verhalten der Unbekannten dar. Dieses ist der Beklagten jedoch infolge des Verstoßes gegen die Integritäts- und Vertraulichkeitspflicht zurechenbar, da durch deren Verletzung die unzulässige Datenverarbeitung unmittelbar ermöglicht worden ist. Es ist gerade Sinn

und Zweck der Integritäts- und Vertraulichkeitspflicht, unzulässige Datenverarbeitungen zu verhindern. Nicht mehr zuzurechnen sind der Beklagten nach diesem Maßstab die durch die Unbekannten und ggf. sonstige Dritte weitergehenden Datenverarbeitungen, wie etwa die im April 2021 erfolgte Veröffentlichung der verknüpften Daten und deren Weiterverwendung. Die Klägerseite hat insoweit nicht ausreichend dargelegt, dass diese durch der Beklagten mögliche und zumutbare Maßnahmen, deren Unterlassen ihrerseits Verstöße gegen die DSGVO dargestellt hätten, hätten verhindert werden können.

d.

Dem Kläger ist auch ein Schaden in Form eines Kontrollverlustes über seine Daten entstanden. Bei der Verknüpfung einer Mobiltelefonnummer mit sonstigen personenbezogenen Daten handelt es sich um eine sensible Kombination, da zum einen dem Mobiltelefon heutzutage eine besondere Funktion bei der Erstellung und Absicherung von Benutzerkonten bzw. allgemein der Abwicklung von geschäftlichen Kontakten zukommt und damit das Risiko u.a. von sog. Identitätsdiebstahl erhöht wird, und die Verknüpfung zum anderen eine deutlich zielgerichtetere Kontaktaufnahme mit dem Kläger zu unlauteren Zwecken ermöglicht.

e.

Als Rechtsfolge kann der Kläger ein angemessenes Schmerzensgeld verlangen, welches das Gericht mit 250,00 € bemisst.

Das Schmerzensgeld muss nach Sinn und Zweck der DSGVO abschreckend sein und sich an Ausgleichs- und Genugtuungsfunktion orientieren, wobei es auf die konkreten Umstände des Einzelfalls ankommt und der Katalog des Art. 83 Abs. 2 DSGVO Berücksichtigung finden kann.

Hierbei ist *schmerzensgelderhöhend* zu berücksichtigen, dass es sich bei der streitgegenständlichen Verknüpfung - wie im Rahmen des Schadens ausgeführt - um eine sensible Kombination mit hohem Missbrauchspotential handelt.

Das Gericht verkennt dabei nicht, dass sämtliche Daten des Klägers - mit Ausnahme der Mobiltelefonnummer - ohnehin für Dritte öffentlich einsehbar und damit beliebig kopierbar, weiterverwendbar und missbrauchbar gewesen sind. Maßgeblicher Anknüpfungspunkt für das Schmerzensgeld ist demgemäß nicht ein Kontrollverlust

über diese Daten (der Kontrolle hatte sich der Kläger insoweit bereits freiwillig begeben), sondern der Kontrollverlust über seine Mobiltelefonnummer einerseits und die Möglichkeit der Verknüpfung dieser Nummer mit seinen übrigen Daten andererseits. Hierfür ist es ohne Belang, dass die Mobiltelefonnummer nicht von der Beklagten "gestellt", sondern von den Unbekannten per Zufallsgenerator "erraten" worden ist. Denn die Beklagte hat die Nummer jedenfalls validiert (siehe oben).

Schmerzensgeldmindernd ist zu berücksichtigen, dass es sich sämtlich um Daten aus der - grundsätzlich am wenigstens schutzwürdigen - Sozialsphäre des Klägers nach der insoweit maßgeblichen Rechtsprechung des Bundesverfassungsgerichts zum allgemeinen Persönlichkeitsrecht handelt. Weiter ist zu berücksichtigen, dass sich der Kläger seiner Daten in Kenntnis des Geschäftsmodells der Beklagten und damit - anders als etwa im Falle von Gesundheitsdaten, die im Zuge ärztlicher Behandlungen notwendigerweise erhoben werden - freiwillig begeben hat (wenn auch - wie ausgeführt - nicht zu dem Zweck der streitgegenständlichen Verarbeitung).

Nicht in die Schmerzensgeldbemessung eingeflossen sind konkrete Folgen, die den Kläger nach seinem Vortrag durch den streitgegenständlichen Vorfall getroffen haben sollen, wie etwa vermehrte missbräuchliche Kontaktaufnahmen per E-Mail und Mobiltelefon. Der Kläger hat insoweit bereits nicht in einer den prozessualen Substantiierungsanforderungen genügenden Weise dargelegt, dass derartige Kontaktaufnahmen (allein) auf den streitgegenständlichen Vorfall zurückzuführen sind, hierfür im Übrigen auf das - zulässige - Bestreiten der Beklagten auch keinen tauglichen Beweis angeboten. Es ist auch nicht ohne weitere Erläuterung ersichtlich, wieso es durch den streitgegenständlichen Vorfall, der die E-Mail-Adresse des Klägers unstreitig nicht betroffen hat, zu der von dem Kläger im Rahmen der persönlichen Anhörung geschilderten Flut an gerade Spam-E-Mails gekommen sein soll.

f.

Der Zinsanspruch folgt aus Rechtshängigkeit ab dem Tag nach Zustellung der Klageschrift (§§ 291, 288 Abs. 1 S. 2 BGB).

2.

(Klageantrag zu Ziffer 5)

Der Kläger hat gegen die Beklagte unter Schadensersatzgesichtspunkten einen Anspruch auf Ersatz der ihm entstandenen vorgerichtlichen Rechtsverfolgungskosten wegen der o.g. Datenschutzverletzung in Höhe einer 1,3 Geschäftsgebühr aus einem Gegenstandswert in Höhe der seinerzeit berechtigten Ansprüche (= 750,00 € gesamt, bestehend aus 250,00 € Schmerzensgeld + 500,00 € berechtigtes Auskunftsverlangen) zuzüglich 20 € Auslagenpauschale und 19 % Umsatzsteuer, insgesamt 159,94 €.

III.

Die prozessualen Nebenentscheidungen folgen aus §§ 92 Abs. 2 Nr. 1, 708 Nr. 11, 711 ZPO. Auf die Streitwertfestsetzung gemäß Beschluss vom 08.07.2022 wird Bezug genommen.

Beglaubigt
Urkundsbeamter/in der Geschäftsstelle
Landgericht Bonn

Verkündet am 29.03.2023

Justizsekretärin
als Urkundsbeamtin der Geschäftsstelle