– Beglaubigte Abschrift –

Landgericht Göttingen

Im Namen des Volkes

Urteil

10 O 41/22

Verkündet am 29.09.2023

[redacted], Justizsekretärin
als Urkundsbeamtin der Geschäftsstelle

In dem Rechtsstreit

[redacted]

- Kläger -

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

gegen

Meta Platforms Ireland LimitedFacebook Ireland Ltd. vertr.d.d.Geschäftsführer (Director) Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland, Irland

- Beklagte -

Prozessbevollmächtigter:
Rechtsanwalt Freshfields Bruckhaus Deringer, Bockenheimer Anlage 44, 60322 Frankfurt am Main
Geschäftszeichen: [redacted]

hat das Landgericht Göttingen – 10. Zivilkammer – durch die Vizepräsidentin des Landgerichts [redacted] als Einzelrichterin auf die mündliche Verhandlung vom 18.08.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger 400,00 € nebst Zinsen in Höhe von 5 Prozentpunkten über den jeweiligen Basiszinssatz seit dem 14.08.2022 zu zahlen.

2. Die Beklagte wird darüber hinaus verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 159,94 € nebst Zinsen in Höhe von 5 Prozentpunkten über den jeweiligen Basiszinssatz seit dem 14.08.2022 zu zahlen.

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

4. Im Übrigen wird die Klage abgewiesen.

5. Von den Kosten des Rechtsstreits hat der Kläger ¾ und die Beklagte ¼ zu tragen.

6. Das Urteil ist vorläufig vollstreckbar. Die Parteien dürfen die Vollstreckung durch Sicherheitsleistung in Höhe von 120 % des aufgrund des Urteils vollstreckbaren Betrages abwenden, wenn nicht die jeweils andere Partei vor der Vollstreckung Sicherheit in Höhe von 120 % des jeweils zu vollstreckenden Betrages leistet.

7. Der Streitwert wird auf 6.000 € festgesetzt.

Tatbestand

Die Parteien streiten um Ansprüche auf Schadensersatz, Unterlassung und Auskunftserteilung im Zusammenhang mit einem sogenannten „Scraping“-Vorfall.

Der Kläger meldete sich 2016 bei dem von der Beklagten betriebenen Plattform „Facebook“ an und unterhielt ein Nutzerkonto. Die Plattform ermöglicht als soziales Netzwerk die Kommunikation mit anderen Nutzern sowie das Teilen von Inhalten. Bei der Registrierung auf der Plattform müssen Name und Geschlecht angegeben werden.

Vor dem Abschluss der Registrierung befindet sich ein Informationsfeld mit dem Inhalt: „Indem du auf „Registrieren“ klickst, stimmst du unseren Nutzungsbedingungen zu. In unserer Datenrichtlinie erfährst du, wie wir deine Daten erfassen, verwenden und teilen (…)“.

Die Plattform teilt dem Nutzer nach der Registrierung eine entsprechende ID zu. Die ID, der Name und das Geschlecht sind für alle Nutzer offen einsehbar. Die Nutzer können auch weitere Informationen, wie Geburtstag, Beziehungsstatus oder Wohnort angeben. Bei diesen zusätzlichen Angaben können die Nutzer jeweils selbst über die Einstellungen entscheiden, ob und gegebenenfalls von welchem Adressatenkreis diese Daten angesehen werden können (sogenannte „Zielgruppenauswahl“). Eine Eingabe der Handynummer ist nicht erforderlich, kann aber beispielsweise angegeben werden, um eine 2-Faktor-Authentifiziereung zu ermöglichen. Weiter können die Nutzer festlegen, ob das Nutzerprofil von Dritten anhand von Daten wie beispielsweise der Telefonnummer aufgefunden werden kann (sogenannte „Suchbarkeit“).

Die Datenrichtlinie der Beklagten beinhaltete Informationen zu den öffentlich sichtbaren Inhalten, der Zielgruppenauswahl und der Suchbarkeit. Den Nutzern stehen im „Hilfebereich“ weitere Informationen über die Privatsphäreeinstellungen zur Verfügung.

Im relevanten Zeitraum war die Voreinstellung bei der Eingabe der Telefonnummer zur 2-Faktor-Authetifizierung auf „nur ich“ voreingestellt, wohingegen sie bezüglich der Suchbarkeit auf “alle“ voreingestellt war. Die Suchbarkeit des Klägers über die Telefonnummer war dementsprechend ab dem 10.03.2016 auf „alle“ eingestellt.

Nach Medienberichten aus dem April 2021 war es bei der von der Beklagten betriebenen Plattform zu einem sogenannten „Scraping“-Vorfall gekommen. „Scraping“ ist eine Vorgehensweise, bei der unbekannte Dritte eine Telefonnummer benutzten, um über die „Kontakt-Importer-Funktion“ das Facebook-Konto anderer Nutzer anzusehen und auf diese Weise umfangreiche Datensätze zu generieren. Soweit der Nutzer eine Suchbarkeit über die Telefonnummer erlaubt hatte, ist es den unbekannten Dritten so möglich, die immer öffentlich einsehbaren Nutzerdaten mit der Telefonnummer zu verknüpfen. Sind noch weitere Daten des Nutzers für alle einsehbar, können auch diese Daten der Telefonnummer und den bereits erlangten Daten zugeordnet werden. Ob vorliegend die Telefonnummern, mit denen die Datensätze aufgebaut wurden, von den unbekannten Dritten zufällig ausprobiert oder gezielt angekauft wurden, ist zwischen den Parteien streitig.

Nach den Nutzungsbedingungen der Beklagten ist das serielle Auslesen der Kontaktdaten untersagt. Die Beklagte setzt als Maßnahme zu dessen Verhinderung eine Bot-Erkennung sowie technische Übertragungsbegrenzungen ein. Die irische Datenschutzaufsicht wurde von der Beklagten nicht über den Vorfall informiert.

Um „Scraping“ weiter zu bekämpfen, deaktivierte die Beklagte im April 2018 die Suche von Nutzern anhand der Telefonnummer. Als weitere Maßnahme überarbeitete die Beklagte die „Kontakt-Importer-Funktion“ grundlegend, sodass nur noch eine Liste der „Menschen, die du kennen könntest“ angezeigt wird. Ein direkter Import von Kontakten nur über die Handynummer war nicht mehr möglich.

Die Beklagte wies durch ihren jetzigen Prozessbevollmächtigen mit Schreiben vom 23.08.2021 den Kläger nach dessen Auskunftsbegehren darauf hin, dass es im April 2021 einen „Scraping“-Vorfall gegeben hatte. In dem Schreiben gab die Beklagte Angaben zu möglichen Datenpunkten an, die aufgrund der gewählten Einstellungen ausgelesen werden konnten. Ferner wies sie darauf hin, dass ihr keine Rohdaten zu den abgerufenen Daten vorlägen. Die Beklagte gab dem Kläger zudem Informationen, wie eine Änderung der Einstellungen vorgenommen und eine Kopie aller Facebook-Informationen heruntergeladen werden kann.

Mit E-Mail vom 28.10.2021 wiesen die jetzigen Prozessbevollmächtigten des Klägers die Beklagte darauf hin, dass aus ihrer Sicht Verstöße gegen die DSGVO bestanden haben, und forderten die Beklagte vergeblich zur Zahlung von 500 € Schmerzensgeld sowie von vorgerichtlichen Rechtsanwaltskosten in Höhe von 887,03 € bis zum 29.11.2021 auf.

Die irische Datenschutzbehörde verhängte gegen die Beklagte wegen des Abflusses der Daten am 28.11.2022 eine Geldbuße in Höhe von 265 Mio. Euro.

Der Kläger behauptet, bei ihm sei es nach dem Scraping-Vorfall zu unerwünschten Spam-Anrufen gekommen. Im Darknet sei ein Datensatz mit den verknüpften Daten seines Namens, Vornamens, Handynummer, Facebook-ID und Geschlecht zu finden.

Der Kläger meint, zu einem Auslesen seiner Daten im Rahmen des „Scrapings“ habe es nur kommen können, weil die Voreinstellungen der Beklagten auf „alle“ gesetzt gewesen seien. Dies widerspreche dem Grundsatz der Datenminimierung und Datensicherheit. Zudem seien die Datenschutzhinweise der Beklagten schwer verständlich sowie wenig transparent und daher ungeeignet. Der Kläger lebe seither mit dem Gefühl des „Kontrollverlustes“ in Bezug auf die den Unbekannten zugänglich gemachten Daten.

Der Kläger beantragt,

1. die Beklagte zu verurteilen, an ihn immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessend es Gerichts gestellt wird, mindestens jedoch 1.000,00 EUR 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 verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzendes Ordnungsgeldes bis zu 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, es zu unterlassen,

a. personenbezogene Daten des Klägers, 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 des Klägers 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 wird und, im Falle der Nutzung der Facebook-Messenger-App, hier ebenfalls explizit die Berechtigung verweigert wird,

4. die Beklagte zu verurteilen, ihm Auskunft über den ihn betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten,

5. die Beklagte zu verurteilen, ihm 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.

Die Beklagte bestreitet das Vorhandensein eines Datensatzes zu dem Kläger im Darknet, den Erhalt von Spams sowie eine Ursächlichkeit des „Scraping“-Vorfall hierfür mit Nichtwissen. Die

Beklagte ist der Ansicht, anders als bei einem Hackerangriff seien bei dem „Scraping“-Vorfall Daten erlangt worden, die von jedem Dritten ohne Überwinden von Hindernisschranken hätten erlangt werden können. Ein Abgreifen der Daten beim Verarbeiter sei gerade nicht erfolgt. Die Datenschutzinformationen auf der Plattform seien auch verständlich. Eine Auskunft sei entweder erfolgt oder nicht möglich, weil eine Übermittlung an die unbekannten Dritten nicht von der Beklagten veranlasst worden sei. Ein Verstoß gegen die DSGVO liege insofern nicht vor.

Hinsichtlich der Einzelheiten des Vorbringens der Parteien wird auf die zur Akte gereichten Schriftsätze nebst Anlagen Bezug genommen.

Entscheidungsgründe

Die Klage ist überwiegend zulässig, aber nur teilweise begründet.

I.

Die Klage ist überwiegend zulässig.

Das Landgericht Göttingen ist international, sachlich und örtlich zuständig.

Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 Alt. 2 EGVVO sowie auch aus Art. 79 Abs. 2 Satz 2 DSGVO. Die sachliche Zuständigkeit ergibt sich aufgrund des 5.000 EUR übersteigenden Wert der geltend gemachten Ansprüche aus §§ 23 Nr. 1, 71 Abs. 1 GVG, § 5 ZPO. Die örtliche Zuständigkeit ergibt sich nach § 44 Abs. 1 Satz 2 BDSG aus dem besonderen Gerichtsstand des gewöhnlichen Aufenthaltsortes des Klägers im Bezirk.

Der Antrag zu 1) ist zulässig, insbesondere nach § 253 Abs. 2 Nr. 2 ZPO hinreichend bestimmt. Danach muss die Klageschrift die bestimmte Angabe des Gegenstandes und des Grundes des erhobenen Anspruchs, sowie einen bestimmten Antrag enthalten. Damit werden der Streitgegenstand abgegrenzt, die Grenze der Rechtshängigkeit und Rechtskraft festgelegt sowie Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts bestimmt.

Der zugrundeliegende Lebenssachverhalt ist hier hinreichend bestimmt. Aus der Klagebegründung wird deutlich, dass es um das „Scraping“ und die Veröffentlichung des Leak-Datensatzes geht. Soweit der Kläger auch auf die aus seiner Sicht unzureichende Informationen der Beklagten zuvor und die unterbliebene Meldung an die Datenschutzaufsicht danach anführt, handelt es sich dabei bloß um Bemessungsfaktoren für die Höhe der Entschädigung und nicht um eine Ausdehnung des haftungsbegründenden Ereignisses.

Wegen der im materiellen Recht angelegten Rechtsfolge des Ersatzes immaterieller Schäden, ist es auch ausreichend, dass der Kläger die Höhe des nach seiner Vorstellung auszusprechenden Entschädigungsbetrages mit einem Gesamtbetrag von mindestens 1.000,00 EUR angibt (OLG Hamm GRUR-RS 2023, 22505 Rn. 43; ferner Roth, in: Stein/Jonas, ZPO, 23. Aufl. 2016, § 253 Rn. 43 ff.).

Auch der Feststellungsantrag zu 2) ist zulässig.

Es liegt keine Überschneidung mit dem Klagantrag zu 1) vor, die zu einer unzulässigen doppelten Rechtshängigkeit führte. Der Kläger hat im Klageschriftsatz hinreichend deutlich gemacht, dass durch den Antrag nur materielle Schaden erfasst sein sollen.

Das nach § 256 Abs. 1 ZPO erforderliche Feststellungsinteresse besteht. Ein solches liegt vor, wenn die Schadensentwicklung noch nicht abgeschlossen ist und der Kläger seinen Anspruch deshalb ganz oder teilweise nicht beziffern und insoweit keine Leistungsklage erheben kann.

Der Kläger hat dargetan, dass eine Haftung der Beklagten aus Datenschutzrecht wegen des in Rede stehenden „Scraping"-Vorfalls zumindest möglich erscheint. Aufgrund der vom Kläger behaupteten Spam-Anrufe und des Darknet-Auszugs erscheint es ferner zumindest möglich, dass sich daraus materielle Vermögenseinbußen entwickeln können oder sich schon entwickelt haben und dem Kläger wegen des heimlichen Datenabgriffs bisher unbekannt geblieben sind und dass ohne den Feststellungsantrag die Verjährung der Ansprüche droht.

Der Unterlassungsantrag zu 3) ist hingegen unzulässig. Bei dem Antrag handelt es sich um einen verdeckten Leistungsantrag. Ob ein Leistungs- oder ein Unterlassungsantrag vorliegt, ist im Wege der Auslegung mit Blick auf den Schwerpunkt der jeweils in Rede stehenden Verpflichtung zu beurteilen (BGH NJW-RR 2021, Rn. 11 m.w.N).

Der Schwerpunkt liegt hier im aktiven Tun. Hier verlangt der Kläger mit seinen Anträgen, dass die Beklagte es unterlässt, Daten (…) zugänglich zu machen (…) ohne dass vorgesehen wird (…) bzw. die Telefonnummer (…) zu verarbeiten (…) ohne eindeutige Informationen darüber (…). Damit verlangt der Kläger, dass die Beklagte unter bestimmten näher gefassten Bedingungen eine Handlung in einer bestimmten Weise ausübt (vgl. auch OLG Hamm GRUR-RS 2023, 22505 Rn. 206 f.).

Der danach vorliegende Leistungsantrag ist aber ebenfalls unzulässig. Da die Beklagte unstreitig aktuell eine Kontaktimportfunktion nicht betreibt, verlangt der Kläger eine künftige Leistung. Eine Klage auf künftige Leistung kann nach § 259 ZPO erhoben werden, wenn den Umständen nach die Besorgnis gerechtfertigt ist, dass der Schuldner sich der rechtzeitigen Leistung entziehen werde. Dis ist hier nicht der Fall. In dem Übergang der Beklagten zur Anzeige nur noch von „Menschen, die du kennen könntest" liegt eine Abkehr von der Kontaktimportfunktion (OLG Hamm GRUR-RS 2023, 2250,5 Rn. 209 f.). Ein Übergang hin zur vorherigen Praxis liegt angesichts der deswegen verhängten Geldbuße der irischen Datenschutzbehörde eher fern (so auch OLG Hamm GRUR-RS 2023, 22505, Rn. 210). Jedenfalls hat der Kläger in diese Richtung nichts Konkretes vorgetragen.

Die Leistungsanträge zu 4) und 5) sind zulässig.

II.

Die Klage ist nur teilweise begründet.

Der Klageantrag zu 1.) ist teilweise begründet.

Der Kläger hat einen Anspruch auf Zahlung eines Schmerzensgeldes in Höhe von 400 € aus Art. 82 DSGVO. Danach hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein

materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen.

Die DSGVO ist sachlich anwendbar. Der Betrieb eines sozialen Netzwerkes durch Sammlung bzw. Speicherung jedenfalls des Namens und Geschlechts von Mitgliedern und die automatisierte Vernetzung der Mitglieder fällt in den sachlichen Anwendungsbereich der DSGVO, vgl. Art. 2 Abs. 1 DSGVO (OLG Hamm GRUR-RS 2023, 22505 Rn. 67).

Als Betreiberin der Plattform Facebook ist die Beklagte Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO.

Es liegt auch ein Verstoß gegen die DSGVO vor.

Zwar fallen der Beklagten im Hinblick auf den ursprünglichen Registrierungsprozess und die ursprüngliche Angabe der Telefonnummer keine Verstöße zur Last. Der Kläger hat sich im Jahr 2016 registriert und hat seine Telefonnummer auch in diesem Jahr zu angegeben. Nach Art. 99 Abs. 2 DSGVO gilt die DSGVO aber erst ab dem 25.5.2018.

Ein Datenschutzverstoß ergibt sich aber aus der Voreinstellung in Bezug auf die (weitere) Speicherung der Telefonnummer ab dem 25.5.2018.

Im Fall einer Datenerhebung vor dem 25.05.2018 unterfällt ausschließlich die Weiterverarbeitung der Daten ab dem 25.05.2018 den Anforderungen der DSGVO; denn aus Erwägungsgrund 171 Satz 2 DSGVO, aus Art. 4 Nr. 2 DSGVO sowie Art. 24 Abs. 1, insbesondere Satz 2 DSGVO ergibt sich die Pflicht, die Datenverarbeitungen, die zum Zeitpunkt der Anwendung der DSGVO bereits begonnen hatten, bis zum 25.05.2018 in Einklang mit der Verordnung zu bringen (OLG Hamm GRUR-RS 2023, 22505 Rn. 61; GA Pitruzzella Schlussanträge v. 27.4.2023 – C-340/21, BeckRS 2023, 8707 Rn. 43; LAG Baden-Württemberg Urt. v. 25.2.2021 – 17 Sa 37/20, ZD 2021, 436 = juris Rn. 63).

Bei der Telefonnummer handelt es sich um personenbezogene Daten im Sinne der Art. 5 Abs. 1 lit. a Var. 1, Art. 6 Abs. 1 Unterabs. 1 lit. a, Art. 7, Art. 2 Abs. 1 in Verbindung mit Art. 4 Nr. 1 DSGVO.

Es liegt ein Verstoß gegen Art. 25 DSGVO bei der Datenverarbeitung vor.

Zwar kann ein Verstoß gegen Art. 25 DSGVO unmittelbar nicht zur Auslösung der Haftung nach Art. 82 DSGVO führen, da Art. 25 DSGVO in erster Linie eine organisatorische Verpflichtung für den Verantwortlichen darstellt (Nolte/Werkmeister, in: Gola/Heckmann, DSGVO BDSG, 3. Aufl. 2022, Art. 25 Rn. 34). Eine Datenverarbeitung liegt aber unzweifelhaft mit dem andauernden weiteren Vorhalten der Telefonnummer vor.

Hierbei liegt auch kein Erlaubnistatbestand nach Art. 6 DSGVO vor. Buchst. a muss schon mangels aktiver Einwilligung in die voreingestellte Preisgabe ausscheiden. Buchst. b. scheitert daran, dass die Preisgabe der Telefonnummer an alle zur Auffindung auch nach weitestgehender Auslegung des von den Parteien bezweckten Ziels eines sozialen Netzwerks nicht mehr der Erfüllung des Vertrags dient (so auch OLG Hamm GRUR-RS 2023, 22505 Rn. 82 ff.).

Nach Art. 25 Abs. 1 Satz 1 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur

personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Man könnte annehmen, dass für den Verwendungszweck eines sozialen Netzwerkes die Eingabe möglichst vieler personenbezogene Daten wie Telefonnummer, Geburtsort, Hobbies usw. erforderlich wäre (in eine ähnliche Richtung LG Stuttgart GRUR-RS 2023, 14394, Rn. 34; LG Essen ZD 2023, 292, Rn. 66). Art. 25 Abs. 1 Satz 3 DSGVO stellt aber insofern eine grundsätzliche Regel für den Umgang auch mit solchen für den Vertragszweck erforderlichen Daten auf. Danach müssen die Maßnahmen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Die Vorschrift ist ersichtlich auf soziale Netzwerke zugeschnitten und soll den betroffenen Nutzern ermöglichen, den Kreis der Empfänger ihrer Nachrichten oder sonstigen Aktivitäten selbst zu steuern (Nolte/Werkmeister, in: Gola/Heckmann, DSGVO BDSG, 3. Aufl. 2022, Art. 25 Rn. 27; ferner Hansen, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 25 Rn. 53; Hartung, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 25 Rn. 26).

Als Voreinstellung ist deshalb der kleinstmögliche Empfängerkreis vorzusehen (Nolte/Werkmeister, in: Gola/Heckmann, DSGVO BDSG, 3. Aufl. 2022, Art. 25 Rn. 27). Gemeint ist damit insbesondere die Verpflichtung von sozialen Netzwerken bzw. ähnlichen Internet-Diensten, dass die von Nutzern veröffentlichten Informationen nicht ohne Einschränkungen der allgemeinen Öffentlichkeit zugänglich gemacht werden dürfen, sondern dies aktiv (vergleichbar einem „Opt-In“) erst in den Privatsphäreeinstellungen durch den Nutzer eingerichtet werden muss (Hartung, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 25 Rn. 26).

Dass der Anbieter den Nutzern nur die Möglichkeit eröffnet, Datenschutzeinstellungen des Dienstes jederzeit selbst zu ändern, genügt nach der Idee des Gesetzgebers dem normativen Auftrag des Art. 25 Abs. 2 DSGVO nicht (Martini, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 25 Rn. 46).

Nach diesem Maßstab stellt die Voreinstellung bei eingegebener Telefonnummer auf sichtbar für „alle“ einen Verstoß gegen Art. 25 DSGVO dar (so auch OLG Hamm GRUR-RS 2023, 22505 Rn. 97 ff., Rn. 112 f.; LG Paderborn GRUR-RS 2022, 39349, Rn. 107). Die „Suchbarkeits-Einstellungen“ sahen in ihrer Standard-Voreinstellung unabhängig von der Einsehbarkeit der Telefonnummer vor, dass alle Personen mittels dieser die hinter den Nummern stehenden Profile finden konnten. Die Nutzer mussten von sich aus aktiv werden, um ihre Daten Dritten weniger zugänglich zu machen.

Infolge der Voreinstellungen kam es bei dem Kläger zu – vermehrten - unerwünschten Spam-Anrufen. Das Gericht ist hiervon aufgrund der vorgelegten Screen-Shots sowie der persönlichen Anhörung des Klägers überzeugt. Der persönlich angehörte Kläger hat nachvollziehbar geschildert, dass es nach dem Vorfall bei ihm zu Spam-Anrufen kam, teilweise sogar mehrfach täglich. Er hat dabei ohne Weiteres eingeräumt, dass es auch zuvor vereinzelt Spam-Anrufe gegeben hatte, dies dann aber ab einem bestimmten Zeitpunkt deutlich mehr geworden war, ohne dass hierfür eine andere Ursache als der Scraping-Vorfall, von demm der Kläger erst später erfahren hat, ersichtlich ist.

Auf die Veröffentlichung des Datensatzes im „Darknet“ kommt es hingegen nicht entscheidungserheblich an. Dieses Phänomen vertieft den Primärschaden in Form der Spam-Anrufe nicht, sondern geht diesem voraus.

Die Frage, ob das bloße Gefühl eines „Kontrollverlustes“ für die Bejahung eines Anspruchs auf immateriellen Schadensersatz schon ausreicht, bedarf hier daher keiner Entscheidung (insoweit ablehnend OLG Hamm GRUR-RS 2023, 22505, Rn. 139 ff, Rn. 146 ff.).

Der eine Haftung ausschließende Nachweis nach Art. 82 Abs. 3 DSGVO ist der Beklagten nicht gelungen. Danach wird der Verantwortliche von der Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Dass die Beklagte nicht für die Spam-Anrufe verantwortlich ist, liegt auf der Hand. Erforderlich wäre aber die Nichtverantwortlichkeit für die Umstände, die dazu geführt haben. Dies waren aber gerade die von der Beklagten gewählten Voreinstellungen in Bezug auf die eingegebenen Telefonnummern.

Ein weiterer haftungsbegründender bzw. haftungsverschärfender Datenschutzverstoß ergibt sich nicht daraus, dass der genannte Verstoß gegen Art. 25 DSGVO, der sich im April 2018 realisiert hatte, entgegen Art. 33, 34 DSGVO nicht der Datenschutzaufsicht gemeldet worden ist. Es ist vom Kläger nicht dargetan und auch sonst nicht ersichtlich, dass der Kläger im Falle rechtzeitiger Unterrichtung der Datenschutzaufsicht weniger Spam-Anrufe bekommen hätte. Insbesondere ist nicht ersichtlich, dass die Datenschutzaufsicht, auf die unbekannten Dritten oder auf diejenigen, denen die Datensätze für die Spam-Anrufe überlassen worden sind, hätte einwirken können.

Der Höhe nach ist ein Betrag von 400 € zum Ausgleich der erlittenen und zu erwartenden immateriellen Schäden angemessen (ähnlich auch LG Stuttgart ZD 2023, 278 (300 €); LG Paderborn GRUR-RS 2022, 39349 (500 €)). Bei der Bestimmung des vom Kläger in das Ermessen des Gerichts gestellten Höhe des Schadenersatzes gem. § 287 Abs. 1 ZPO waren auf der einen Seite die Unannehmlichkeiten durch die Spam-Anrufe und damit einhergehend der Zugriff der Anrufer auf Nummer und Namen des Klägers zu berücksichtigen. Auf der anderen Seite war die Möglichkeit des Klägers, seine Handynummer zu wechseln, zu berücksichtigen sowie der (nur) fahrlässige Datenschutzverstoß. Zudem war das Maß an Pflichtwidrigkeit herabgesetzt wegen der von der Beklagten ergriffenen - wenn auch nicht ausreichenden - Maßnahmen in Gestalt der Bot-Erkennung und technischen Übertragungsbeschränkung. Ferner handelt es sich bei den abgegriffenen Daten zwar um personenbezogene Daten, aber nicht um personenbezogene Daten einer besonderen Kategorie nach Art. 9 DSGVO.

Ein Mitverschulden des Klägers durch Beibehaltung der Voreinstellung liegt nicht vor. Es ist gerade der Zweck des Art. 25 Abs. 1 Satz 3 DSGVO, Voreinstellungen datenminimierend auszugestalten, weil Nutzer typischerweise wenig Veranlassung haben, diese später noch einmal zu verändern (ähnlich auch LG Stuttgart ZD 2023, 278, Rn. 93).

Nachdem dem Kläger der Schadensersatzanspruch aus Art. 82 DSGVO dem Grunde nach zusteht, ist auch auf den Klageantrag zu 2) begründet, da es ohne Weiteres möglich ist, dass der Kläger neben immateriellen Schäden künftig auch materielle Einbußen erleiden kann. Eine darüber hinausgehende gewisse Wahrscheinlichkeit des Schadenseintritts ist nicht erforderlich (so auch OLG Stuttgart, Urteil vom 21.6.2018, 13 U 18/18, Rn 46, zitiert nach juris)

Der Kläger hat dagegen keinen Auskunftsanspruch.

Zwar steht dem Kläger im Ausgangspunkt ein Auskunftsanspruch nach Art. 15 DSGVO zu. Denn nach Art. 15 Abs. 1 Hs. 1 DSGVO hat die betroffene Person gegen den Verantwortlichen einen Anspruch, ihm zu bestätigen, ob ihn betreffende personenbezogene Daten verarbeitet werden. Verarbeitet der Verantwortliche personenbezogene Daten der betroffenen Person, so

hat die betroffene Person gem. Art. 15 Abs. 1 Hs. 2 DSGVO ein Recht auf Auskunft über diese personenbezogenen Daten. Gemäß Art. 15 Abs. 3 Satz 1 DSGVO stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.

Der Anspruch des Klägers ist jedoch durch Erfüllung untergegangen, § 362 BGB. Erfüllt im Sinne des § 362 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die - gegebenenfalls konkludente - Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (BGH GRUR 2021, 110, Rn. 43). Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll (OLG Hamm GRUR-RS 2023, 22505 Rn. 233; LG Paderborn GRUR-RS 2022, 39349, Rn. 165).

Dies ist hier der Fall gewesen. Mit Schreiben vom 23.08.2021 hat die Beklagte in angemessener Weise mitgeteilt, welche personenbezogenen Daten verarbeitet werden, indem sie den Kläger auf die Selbstbedienungstools verwiesen hat. Eine Auflistung der Datenpunkte wurde erteilt. Dies war als Erfüllungshandlung ausreichend.

Ein darüberhinausgehender Auskunftsanspruch in Bezug darauf, welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten, besteht nicht. Die Beklagte hat vorgetragen, über die Verarbeitungstätigkeiten Dritter (hier: „Scraper“), keine Angaben machen zu können. Das ist auch ohne Weiteres nachvollziehbar. Unabhängig davon, ob die erteilte Auskunft unrichtig oder unvollständig ist, begründet die erteilte Auskunft jedenfalls keinen (weiteren) Auskunftsanspruch, da die Beklagte hiermit zum Ausdruck gebracht hat, das Auskunftsbegehren des Klägers vollständig erfüllt zu haben (so auch für einen parallel liegenden Fall: LG Paderborn GRUR-RS 2022, 39349, Rn. 167 f.).

Weitere Anspruchsgrundlagen, die auf Auskunftserteilung gerichtet sind, sind weder ersichtlich noch vom Kläger vorgetragen.

Als weiteren Posten des ihm zustehenden materiellen Schadensersatzanspruchs nach Art. 82 DSGVO kann der Kläger auch die Erstattung angefallener vorgerichtlicher Rechtsanwaltsgebühren beanspruchen. Ausgehend von den Gegenstandswerten für die erfolgreichen Klageanträge 1) und 2) sind 900 € anzusetzen. Insgesamt ergeben sich damit ersatzfähige Gebühren nach Ziff. 2300, 7002, 7008 VV-RVG in Höhe von 159,94 Euro.

Der Zinsanspruch ergibt sich aus §§ 291, 288 Abs. 1 Satz 2 ZPO.

III.

Die prozessualen Nebenentscheidungen resultieren aus §§ 92 Abs. 1, 708 Nr. 11, 711 ZPO.

Die Streitwertfestsetzung resultiert aus § 3 ZPO. Der Schadenersatzanspruch ist mit 1.000 € zu bemessen, hinsichtlich des Feststellungsantrags sind 500 € anzusetzen, der Unterlassungsantrag ist mit 4.000 € zu bemessen, der Auskunftsantrag mit 500 €.

[redacted]
Vizepräsidentin des Landgerichts

Beglaubigt
Göttingen, 11.10.2023

[redacted], Justizsekretärin
als Urkundsbeamtin der Geschäftsstelle