Abschrift

EINGEGANGEN
22. FEB. 2023
WILDE BEUGER SOLMECKE
RECHTSANWÄLTE
450 3/21

Geschäfts-Nr.:
21 O 96/22

Verkündet am:
16. Februar 2023

[redacted]
als Urkundsbeamtin der Geschäftsstelle

Landgericht Stendal

Im Namen des Volkes!

Urteil

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., vertreten durch den Geschäftsführer (Director) Gareth Lambe, 4 Grand Canal Square, DUBLIN 2, IRELAND,

Beklagte,

Prozessbevollmächtigte: Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB, Bockenheimer Anlage 44, 60322 Frankfurt am Main,
Geschäftszeichen: [redacted]

hat die Zivilkammer 1 des Landgerichts Stendal durch

die Richterin am Landgericht [redacted] als Einzelrichterin

auf die mündliche Verhandlung vom 15. Dezember 2022

für **Recht** erkannt:

1. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadenersatz in Höhe von 500,00 Euro nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 02. August 2022 zu zahlen.
2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen materiellen Schäden zu ersetzen, die der Kläger durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Zeitraum Januar 2018 bis September 2019 erfolgte, noch entstehen.
3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihren gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren zu unterlassen,

   personenbezogenen 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.
4. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 287,98 Euro zu zahlen zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 02. August 2022.
5. Im Übrigen wird die Klage abgewiesen.
6. Die Kosten des Rechtsstreits werden gegeneinander aufgehoben.
7. Das Urteil ist gegen Sicherheitsleistung in Höhe von 110% des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

Tatbestand

Die Parteien streiten über Ansprüche auf Schadenersatz, Unterlassung und Auskunft wegen Verletzung des (Grund-) Rechts des Klägers auf Schutz personenbezogener Daten.

Die Beklagte ist die Betreiberin der Social-Media-Platform Facebook. Facebook-Nutzer können über verschiedene Kanäle auf den Facebook-Dienst zugreifen, einschließlich durch die Website-URL www.facebook.com sowie über Apps für Mobiltelefone und Tablet-PCs. Für Nutzer in der Europäischen Union wird die Facebook-Plattform von der Beklagten, einem Unternehmen nach dem Recht der Irischen Republik mit Sitz in Dublin, Irland, betrieben.

Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Auf diesen persönlichen Profilen können die Nutzer Angaben zu verschiedenen Daten zu ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können.

Der Kläger meldete sich mit der E-Mail-Adresse [redacted] bei Facebook an.

Damit Nutzer leichter mit anderen Nutzern auf der Facebook-Plattform in Kontakt treten können, müssen bestimmte Informationen bei der Registrierung angeben werden, die als Teil des Nutzerprofils immer öffentlich einsehbar sind. Dazu gehören Name, Geschlecht und Nutzer-ID. Dies wurde und wird im Hilfebereich erläutert. Die Einsehbarkeit weiterer Daten kann der Nutzer bestimmen.

Die Standardeinstellung für weitere persönliche Daten war im Zeitpunkt der Anmeldung des Klägers „Alle". Über Privatsphäre-Einstellungen konnte der Kläger Zielgruppen bestimmten, nämlich wer einzelne Informationen wie Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse im Facebook-Profil eines Nutzers sehen können sollte. Anstelle der Standardeinstellung „öffentlich" konnten der Nutzer „Freunde" oder „Freunde von Freunden" auswählen. Die Angabe der Handynummer war nicht zwingend. Entschied sich ein Nutzer aber diese anzugeben, so war die Standard-Einstellung für die Zielgruppenauswahl auf „Friends" voreingestellt, so dass nur Freunde des Nutzers, die seine Handynummer gespeichert hatten, die Telefonnummer auf dem Facebook-Profil des Nutzers sehen konnten.

Ländern im Internet auf der für jedermann abrufbaren Datenbank raidforums.com veröffentlicht worden.

Auf die Medienberichte stellte die Beklagte am 06.04.2021 den Nutzern Informationen über die durch Scraping abgerufenen Daten sowie weitere Informationen über maßgebliche Datenschutzeinstellungen zur Verfügung (Anlage B 10, Anlagenband zum Schriftsatz vom 08.11.2022). Am 07.04.2021 wurde im Facebook-Hilfebereich ein zusätzlicher Artikel bezüglich der durch Scraping abgerufenen Daten veröffentlicht, der auch Links zu Informationen in Bezug auf die Facebook-Privatsphäreneinstellung der Nutzer enthält. Am 15.04.2021 wurden im Facebook Newsroom weitere Informationen über die Maßnahmen von Facebook zur Bekämpfung von Scraping veröffentlicht. Am 19.05.2021 wurden ergänzende Informationen über die Bemühungen von Facebook zum Schutz vor Datenmissbrauch und Telefonnummern-Scrapingtechnik veröffentlicht (Anlage B 11, Anlagenband zum Schriftsatz vom 08.11.2022).

Mit E-Mail seiner Prozessbevollmächtigten vom 24.08.2021 forderte der Kläger die Beklagte wegen Verstößen gegen die DSGVO zu Schadenersatz, Auskunft und Unterlassen auf (Anlage K 1, Bd. I Bl. 52 ff d.A.).

Mit Anwaltsschreiben vom 17.09.2021 wies die Beklagte die Ansprüche zurück (Anlage B 16, Anlagenband zum Schriftsatz vom 08.11.2022).

Die Irische Datenschutzbehörde DPC verhängte am 28.11.2022 gegen die Beklagte im Hinblick auf den streitgegenständlichen Scraping-Vorfall wegen Verstößen gegen die DSGVO eine Geldbuße in Höhe von 265 Mio. Euro. Wegen der Einzelheiten wird auf die im Internet veröffentliche Entscheidung verwiesen (https://www.dataprotection.ie/sites/default/files/uploads/2022-12/Final%20Decision_IN-21-4-2_Redacted.pdf).

Der Kläger behauptet, das Scraping sei möglich gewesen, weil die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten CIT zu verhindern, und andererseits, weil die Einstellungen zur Sicherheit der Telefonnummer auf Facebook so undurchsichtig und kompliziert gestaltet sind, dass ein Nutzer tatsächliche keine sichere Einstellung habe erreichen können. Die Einstellungen seien entgegen der Vorgaben der DSVO datenschutz-unfreundlich eingestellt gewesen, so dass eine hohe Wahrscheinlichkeit bestehe, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte. Die Sicherheit und

Vertraulichkeit seiner Telefonnummer sei für einen Nutzer besonders relevant. Es seien von der Beklagten keine Sicherheitscapchas verwandt worden, um sicherzustellen, dass es sich bei der Anfrage zur Synchronisierung, um die Anfrage eines Menschen und nicht um eine automatisch generierte handele. Ebenso wenig sei ein Mechanismus zur Überprüfung der Plausibilität der Anfragen bereitgehalten worden, etwa indem ungewöhnlich viele Anfragen derselben IP-Adresse auf einmal geblockt worden oder Adressbücher mit auffälligen Telefonnummerabfolgen automatisch abgelehnt worden seien. Auf der Datenbank raidformums.com im Darknet seien folgende Daten des Klägers enthalten: [redacted],6/ [redacted],". Die Veröffentlichung der Daten habe weitreichende Folgen für den Kläger gehabt. Die Zuordnung von Telefonnummern zu weiteren Daten wie Mail-Adresse oder Anschrift eröffne böswilligen Akteuren eine weite Bandbreite an Möglichkeiten wie Identitätsdiebstahl, die Übernahme von Accounts oder gezielte Phishing-Nachrichten. Insbesondere sogenannte „Sim-Swap"-Angriffe würden durch die Verknüpfung von Telefonnummern zu weiteren Nutzer-Accounts eröffnet. Durch derartige Angriffe sei es Kriminellen möglich, Passwörter zu ändern, die durch telefonnummernbasierende Authentifizierung geschützt seien. Der Kläger habe einen erheblichen Kontrollverlust über seine Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch seiner Daten verblieben. Er habe seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail erhalten, die Nachrichten mit offensichtlichen Betrugsversuchen und potentiellen Virenlinks enthielten. Die Beklagte habe es unterlassen, ihn und die Datenschutzbehörde über den Vorfall zu informieren. Die bisherige Auskunftserteilung sei unzureichend.

Der Kläger meint, ihm stünden wegen Verletzung von Vorschriften der DSGVO, insbesondere Art. 5 Abs. 1 lit. a), 13, 14, 25 Abs. 2, 33, 34 DSGVO, ein Anspruch auf Schadenersatz gemäß § 82 DSGVO zu. Die Beklagte trage die vollständige Darlegungs- und Beweislast, soweit die Einhaltung der DSGVO in Streit stehe. Bereits die Verletzung der DSGVO führe zu einem auszugleichenden immateriellen Schaden. Der Schadensbegriff nach der DSGVO sei weit auszulegen. Die Haftung des Verantwortlichen sei verschuldensunabhängig. Eine Kausalität sei haftungsbegründend gegeben, aber nicht erforderlich. Für die Datenschutzverstöße im Zusammenhang mit dem Datenleck sei ein immaterieller Schadenersatz in Höhe

von 500,00 Euro und für die zeitlich danach liegende unzureichende Auskunft ein weiterer Schadenersatz in gleicher Höhe angemessen. Der Feststellungsantrag sei nicht auf künftige immaterielle Schäden gerichtet. Der Auskunftsanspruch gemäß § 15 DSGVO sei begründet, da Angaben zu den konkreten Empfängern der Daten fehlten. Die Beklagte gehe gegen Scraper nach eigenen Angaben, die sich der Kläger hilfsweise zu eigen mache, per Unterlassungsverfügung vor, so dass die Beklagte diese konkret benennen könne. Der Unterlassungsanspruch ergebe sich wegen der Wiederholungsgefahr aus Art. 17 DSGVO, § 1004 analog iVm § 823 BGB.

Der Kläger beantragt,

1. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadenersatz in Höhe von 1.000,00 Euro nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz zu zahlen;
2. es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen Schäden zu ersetzen, die der Kläger durch den unbefugten Zugriff Dritter auf das Datenarchiv der Eklagten, 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 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihren gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren zu unterlassen,
    a. personenbezogenen 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 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 einer Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird;

4. die Beklagte wird verurteilt, dem Kläger Auskunft über die Klägerseite betreffende personenbezogenen Daten, welche die Beklagte verarbeitet, zu erteilten, 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 den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 Euro zu zahlen zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 02. August 2022.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte stellt Datenschutzverstöße in Abrede. Sie behauptet, der Sachverhalt und Vorgang zum sog. Scraping sei falsch wiedergegeben. Der klägerische Vortrag beruhe auf einem Missverständnis zum Scraping als solchen. Es sei unschlüssig und unsubstantiiert vorgetragen, welche Daten des Klägers genau gescrapt worden sein sollen. Sie bestreite mit Nichtwissen, dass der Kläger einen authentischen Auszug aus den durch Scraping abgerufenen Daten aus einer Datenbank im Darknet handelt. Es seien lediglich automatisch gesammelte öffentlich einsehbare Daten entweder von der APP oder der Website gescraped worden, was nach den Nutzungsbedingungen untersagt gewesen sei und noch untersagt sei. Sie habe alle nach Art. 13 und 14 DSGVO festgelegten Informationen zur Datenverarbeitung zur Verfügung gestellt gehabt. Gegen die Entscheidung der Datenschutzbehörde habe die Beklagte Rechtsmittel eingelegt.

Die Beklagte ist der Ansicht, die Klage sei teilweise nicht zulässig. Die Beklagte habe nicht gegen die Datenschutzvorschriften der DSGVO verstoßen. Es fehle an einem Verstoß gegen § 82 DSGVO: Ein kompensationsfähiger Schaden sei auch nicht dargelegt. Ein Kontrollverlust über personenbezogene Daten wäre ihr nicht zuzurechnen, weil die öffentliche Einsehbarkeit den Privatsphäre-Einstellungen des

Klägers entsprochen habe. Schließlich fehle es an einer schlüssigen Darlegung der Kausalität. Mangels Verstoßes sei der unzulässige Feststellungsantrag unbegründet. Der Unterlassungsanspruch scheitere an einer Erstbegehungs- und einer Wiederholungsgefahr.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen verwiesen.

Die Kammer hat den Kläger in der mündlichen Verhandlung persönlich angehört. Wegen der Einzelheiten wird auf die Leseabschrift des Sitzungsprotokolls, Bd. III Bl. 4 ff d.A., Bezug genommen.

Entscheidungsgründe

Die Klage hat im tenorierten Umfange Erfolg.

A. Die Klage ist nur teilweise zulässig.

I. Der Klageantrag zu 1) ist zulässig, insbesondere ist er hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO. Die zur Auslegung des Klageantrags heranzuziehende Klagebegründung ergibt einen einheitlichen Lebenssachverhalt, den Scraping-Vorfall, von dem der Kläger behauptet, betroffen zu sein. Dargelegt wird eine Mehrheit von Datenschutzverstößen der Beklagten im Zusammenhang mit dem Scraping-Vorfall, die einen einheitlichen Schmerzensgeldanspruch begründen (vgl. Grüneberg in: Grüneberg, BGB, 82. Aufl., § 253 Rn 15).

II. Der Feststellungsantrag zu 2) ist unzulässig, soweit mit ihm die Feststellung begehrt wird, dass die Beklagte dem Kläger zukünftige Schäden, die bereits entstanden sind, zu ersetzen hat. Der Antrag ist insoweit wegen Widersprüchlichkeit nicht hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO.

Der Antrag ist indes hinreichend bestimmt, soweit mit ihm daneben die Feststellung begehrt wird, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen materiellen Schäden zu ersetzen, die dem Kläger durch den unbefugten Zugriff auf das Datenarchiv der Beklagten, der nach der Aussage der Beklagten im Jahr 2019 erfolgte, noch entstehen werden.

Der Kläger hat mit Schriftsatz vom 30.11.2022 insoweit klargestellt, dass der Feststellungsantrag nicht immaterielle, sondern nur zukünftige materielle Schäden

umfasse, so dass es keine Überschneidung mit den Schmerzensgeldanträgen zu Ziffer 1. gebe. Ein Feststellunginteresse gemäß § 256 ZPO ist für diesen Antrag gegeben. Der Kläger macht die Verletzung von Datenschutzvorschriften und damit die Verletzung seines durch Art. 2 Abs. 1 GG geschützten Anspruchs auf informationelle Selbstbestimmung, einem absoluten Recht im Sinne von § 823 Abs. 1 BGB, geltend. Bei der Verletzung absoluter Rechte genügt zur Annahme eines Feststellungsinteresses die bloße Möglichkeit eines künftigen Schadenseintritts (vgl. BGH, Urteil vom 29. Juni 2021 – VI ZR 52/18 –, Rn 30, juris). Von der Möglichkeit künftiger materieller Schäden ist auszugehen, auch wenn der Kläger auch nach seinem Vortrag bisher keine materiellen Schäden durch den Scraping-Vorfall erlitten hat. Es ist nicht ausgeschlossen, dass er durch die Veröffentlichung seiner Daten im Internet bzw. Darknet einen materiellen Schaden, z.B. durch betrügerische Anrufte, erleiden wird.

III. Der Unterlassungsantrag zu 3), insbesondere die Formulierungen „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen" und „unübersichtlicher oder unvollständiger Information" genügen dem Bestimmtheitserfordernis gemäß § 253 Abs. 2 Nr. 2 ZPO, da ein gewisses Maß an Verallgemeinerung zu gestatten ist, auch wenn dies dazu führt, dass das Vollstreckungsgericht Wertungen vornehmen muss (vgl. BGH NJW 2004, 2080).

Der Antrag zu Ziffer 3 a) ist auch nicht widersprüchlich. Die Beklagte ging selbst davon aus, dass „böswillige Akteure" (vgl. Anlage B 16) und damit unbefugte Dritte das von ihr den Nutzern zur Verfügung gestellte CIT genutzt haben, um die Daten der Nutzer abzuschöpfen. Der Antrag des Klägers ist darauf gerichtet, der Beklagten das Bereitstellen des CIT ohne hinreichende Sicherheitsmaßnahmen aus diesem Grund zu untersagen.

Dem Klageantrag zu 3 a) fehlt auch nicht das Rechtsschutzbedürfnis. Das Rechtsschutzbedürfnis ist gegeben, wenn der Rechtssuchende ein berechtigtes Interesse daran hat, gerichtliche Hilfe in Anspruch zu nehmen, d.h. sein Ziel nicht auf einfacheren, billigeren Weg erreichen kann. Zwar kann der Kläger durch die Anpassung der Einstellungen die Suchbarkeit über die Telefonnummer deaktivieren. Dieses genügt aber nicht, um eine zukünftige unrechtmäßige Datenverarbeitung durch die Beklagte zu verhindern, da der Kläger keinen Einfluss auf die durch die Beklagte

ergriffenen Sicherheitsmaßnahmen und damit das vorgehaltene Schutzniveau hat (vgl. LG Paderborn, Urteil vom 13. Dezember 2022 – 2 O 212/22 –, Rn 49 f, juris).

Der Antrag zu 3 b) genügt unter Heranziehung der Klagebegründung den Bestimmheitsanforderungen des § 253 Abs. 2 Nr. 2 ZPO.

B. Die Klage – soweit sie zulässig ist – ist teilweise begründet.

I. Klageantrag zu 1.

1. Der Kläger hat gegen die Beklagte wegen des streitgegenständlichen Scraping-Vorfalls einen Anspruch auf Schadensersatz in Höhe von 500,00 EUR gemäß Art. 82 Abs. 1 DSGVO.

Gemäß Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Diese Voraussetzungen sind vorliegend gegeben.

1.1. Verstoß gegen Art. 25 DSGVO

Zur Überzeugung des Gerichts hat die Beklagte als Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO hinsichtlich des streitgegenständlichen Scraping-Vorfalls gegen Art. 25 Abs. 1 und 2 DSGVO verstoßen. Die Kammer teilt insoweit die rechtliche Einschätzung der DPC in ihrer Entscheidung vom 22.11.2022, die Gegenstand der mündlichen Verhandlung war und deren Inhalt den Prozessbevollmächtigten der Parteien bekannt ist. Die Kammer geht im Ergebnis der Erörterung davon aus, dass sich der Kläger den für ihn günstigen Tatsachenvortrag der DPC in ihrer Entscheidung zu eigen gemacht hat.

Art. 25 Abs. 1 DSGVO verpflichtet den Verantwortlichen bereits bei der Entwicklung von Produkten, Diensten und Anwendungen sicherzustellen, dass die Anforderungen der DSGVO erfüllt werden ("Privacy by Design"). Abs. 2 konkretisiert diese allgemeine Verpflichtung und verlangt, vorhandene Einstellungsmöglichkeiten standardmäßig auf die "datenschutzfreundlichsten" Voreinstellungen ("Privacy by default") zu setzen (Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 3).

"Datenschutz durch Voreinstellungen" soll insbesondere diejenigen Nutzer schützen, welche die datenschutztechnischen Implikationen der Verarbeitungsvorgänge

entweder nicht zu erfassen in der Lage sind oder sich darüber keine Gedanken machen und sich deshalb auch nicht dazu veranlasst sehen, aus eigenem Antrieb datenschutzfreundliche Einstellungen vorzunehmen, obwohl der Telemediendienst ihnen diese Möglichkeit prinzipiell eröffnet (Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 25 Rn. 13).

Die Nutzer sollen keine Änderungen an den Einstellungen vornehmen müssen, um eine möglichst "datensparsame" Verarbeitung zu erreichen. Vielmehr soll umgekehrt jede Abweichung von den datenminimierenden Voreinstellungen erst durch ein aktives "Eingreifen" der Nutzer möglich werden. Die Regelung soll die Verfügungshoheit der Nutzer über ihre Daten sicherstellen und sie vor einer unbewussten Datenerhebung schützen. Abs. 2 verlangt aber nicht, dass der Verantwortliche stets die jeweils denkbar datenschutzfreundlichste Voreinstellung trifft. Der Verantwortliche entscheidet vielmehr durch die Festlegung eines bestimmten Verarbeitungszweckes auch über den Umfang der dafür erforderlichen Daten. Dem Wortlaut nach ist daher auch eine besonders datenintensive Voreinstellung mit Abs. 2 vereinbar, wenn der Zweck der Verarbeitung dies erfordert. Vor dem Hintergrund der Schutzrichtung des Abs. 2, den Nutzer vor einer Überrumpelung oder dem Ausnutzen seiner Unerfahrenheit zu schützen, muss der Verantwortliche aber stets sicherstellen, dass die geplante Datennutzung auch für einen nicht-technikaffinen Nutzer hinreichend transparent ist. (Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 18 f.).

Die Beklagte hat zur Überzeugung der Kammer (§ 286 ZPO) gegen Art. 25 Abs. 1 DSGVO verstoßen. Nach den umfangreichen Ermittlungen der DPC haben im Zeitpunkt des Scraping-Vorfalls das von der Beklagten implementierte Rate Limiting (Begrenzung der Anfragen pro Sekunde und pro IP-Adresse) und die Bot Detection (Erkennen, ob der Zugriff durch Mensch oder Maschine erfolgt) nicht den Anforderungen des Art. 25 Abs. 1 DSGVO im Hinblick auf den große Menge an persönlichen Daten, auf die das CIT den Zugriff ermöglichte, entsprochen. Hierdurch entstand eine erhöhte Gefahr eines Missbrauchs des CIT durch Scraping. Der Beklagten hätte eine Vielzahl von Möglichkeiten nach den plausiblen Ausführungen der DPC zur Verfügung gestanden, um diesen Missbrauch zu verhindern. Hierfür sprechen auch die eigenen Angaben der Beklagten, aus denen folgt, dass sie im September 2019 Änderungen am CIT vornehmen konnte, durch die das Scraping verhindert wurde (vgl. Anlage B 10, Anlagenband zum Schriftsatz vom 08.11.2022). Aus der Entscheidung der DPC ergibt sich, dass die Beklagte bereits im März 2018

das Abschöpfen von Daten bemerkte, und zunächst andere Maßnahmen ergriff, um das Scraping zu verhindern.

Die Beklagte hat zur Überzeugung der Kammer auch gegen Art. 25 Abs. 2 DSGVO verstoßen. Dadurch, dass die Beklagte die Suchbarkeits-Einstellungen so gestaltete, dass mit Hilfe des CIT von jedem Nutzer die Telefonnummer und E-Mail-Adresse gefunden werden konnten, dessen Suchbarkeitseinstellung „Alle" war, hat sie diese persönlichen Daten für eine unbestimmte Anzahl von Personen zugänglich gemacht, ohne dass die Nutzer dies verhindern konnten. Die persönlichen Daten wurden dem Zugriff von in unlauterer Absicht handelnden Scrapern ausgesetzt, die die Funktion des CIT in dem umgekehrten Sinne der vorgesehenen Funktion (statt einem Suchen von befreundeten Kontakten durch den Nutzer ein Auffinden des Nutzers auf der Plattform durch Fremde) ausnutzten. Die Beklagte unterließ insoweit angemessene technische und organisatorische Maßnahmen um standardmäßig sicherzustellen, dass persönliche Daten der Nutzer lediglich dem konkreten Bearbeitungszweck des CIT als auch den von den Nutzern mit der Anmeldung bei Facebook beabsichtigten Zwecken – Freunde zu finden und mit diesen zu kommunizieren - entsprechend verarbeitet wurden.

Der Schutzbereich des Art. 82 DSGVO ist erfasst. Gemäß Art. 82 Abs. 2 S. 1 DSGVO haftet jeder an einer Verarbeitung beteiligte Verantwortliche für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.

Verstöße im Sinne von Art. 25 Abs. 1 und 2 DSGVO gegen organisatorische Maßnahmen, welche zu einer rechtswidrigen Datenverarbeitung geführt haben, sind vom Schutzbereich des Art. 82 DSGVO erfasst (vgl. Nolte/Werkmeister in: Gola/Heckmann, DSGVO – BDSG, 3. Aufl., Art. 25, Rn 31; aA LG Paderborn aaO).

Eine Datenverarbeitung durch die Beklagte im Sinne von Art. 82 Abs. 2 S. 1 DSGVO ist gegeben.

Das Bereitstellen des CIT durch die Beklagte, mit welchem Unbekannte Handynummern, die Facebook-Adressen und weitere auf den Profilen vorhandene Daten von Facebook-Nutzern gescrapt haben, stellt eine der DSGVO nicht entsprechende Datenverarbeitung dar. Eine Datenverarbeitung im Sinne von Art. 4 Nr. 2 DSGVO ist gegeben. Für ein sonstiges Bereitstellen von Daten im Sinne von Art. 4

Nr. 2 DSGVO genügt es, wenn der Verantwortliche den Zugriff auf Daten ermöglicht, während die entscheidende Aktivität von einem Dritten ausgeht (vgl. Schild in: BeckOK, Datenschutzrecht, aaO, Art. 4 Rn 50). Nach dem Sinn und Zweck der Vorschrift entfällt ein zweckgerichtetes Bereitstellen nicht dadurch, dass der Dritte unbefugt auf die bereitgestellten Daten zugreift, wenn dem Unbefugten der Zugriff durch eine unzureichende Sicherung des die Daten Bereitstellenden gerade erst ermöglicht wurde (vgl. Dammann in: Smitis, BDSG, 7. Aufl., § 3 Rn 150). Dies ist vorliegend wie dargelegt der Fall.

1.2. Verstoß gegen Art. 33, 34 DSGVO

Die Beklagte hat ihre Meldepflicht aus Art. 33, 34 DSGVO verletzt.

Gemäß Art. 33 Abs. 1 DSGVO meldet der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der gem. Art. 55 DSGVO zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Der Mindestinhalt der Meldung ist in Art 33 Abs. 3 DSGVO festgelegt.

Dem ist die Beklagte vorliegend nicht nachgekommen. Ausweislich der Entscheidung der DPC hat diese von dem "Scraping"-Vorfall erst im April 2021 aus den Medien erfahren.

Eine Verletzung personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO ist gegeben. Darunter fällt eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Dies war wie dargelegt vorliegend der Fall.

Ein Verstoß gegen die Meldepflicht ist geeignet, für den Verantwortlichen eine Haftung und eine Schadensersatzpflicht gem. Art. 82 DSGVO gegenüber dem Betroffenen zu begründen (vgl. LG Paderborn aaO; Kühling/Buchner/Jandt, 3. Aufl. 2020, DSGVO

Art. 33 Rn. 27; Spindler/Schuster/Laue DSGVO Art. 33 Rn. 24). Denn die Vorschrift dient sowohl dem Schutz des Betroffenen, als auch der Ermöglichung von Maßnahmen zur Eindämmung und Ahndung der Rechtsverletzung durch die Aufsichtsbehörde. Insofern genügt bereits ein solch formeller Verstoß gegen die DSGVO zur Begründung eines Schadensersatzanspruchs dem Grunde nach (vgl. LG Paderborn aaO; BeckOK DatenschutzR/Quaas, 41. Edition Stand: 01.08.2022, DS-GVO Art. 82 Rn. 14).

Auch ein Verstoß gegen Art 34 Abs. 1 DSGVO liegt vor. Nach dieser Vorschrift benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten, wenn diese voraussichtlich ein hohes Risiko für seine persönlichen Rechte und Freiheiten zur Folge hat.

Der Verstoß gegen diese Vorschrift ist ebenfalls geeignet, einen Schadensersatzanspruch zu begründen (vgl. OLG Frankfurt a.M. GRUR 2022, 1252; LG Paderborn aaO; Gola/Heckmann/Reif, 3. Aufl. 2022, DSGVO Art. 34 Rn. 32; Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Auflage 2019, § 11 Rn. 4).

Die Benachrichtigung muss grundsätzlich gegenüber der betroffenen Person im Sinne von Art. 4 Nr. 1 DSGVO erfolgen. Insofern bedarf es der Bestimmung der durch den Vorfall konkret betroffenen Personen. Der in Art. 34 Abs. 1 Hs. 2 DSGVO gewählte Singular "Person" verdeutlicht, dass in den Fällen des Art. 34 regelmäßig eine individuelle Information bezüglich des Datenschutzvorfalls erfolgen muss (Gola/Heckmann/Reif DSGVO Art. 34 Rn. 4). Eine solche individualisierte Information des Klägers ohne schuldhaftes Verzögern nach Offenbarung der Verletzung des Schutzes personenbezogener Daten hat die Beklagte nicht vorgenommen.

Die hier vorliegende Verletzung des Schutzes personenbezogener Daten hatte ein hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen zur Folge. Ein solches Risiko besteht dann, wenn zu erwarten ist, dass bei ungehindertem Geschehensablauf mit hoher Wahrscheinlichkeit ein Schaden für die Rechte und Freiheiten des Betroffenen eintritt. In einem solchen Fall ist es nicht maßgeblich, ob die Datenschutzverletzung auch zu einem besonders hohen Schadensumfang führt (vgl. BeckOK DatenschutzR/Brink, DSGVO Art. 34 Rn. 25.). Aufgrund des Verstoßes gegen Art. 25 DSGVO bestand eine hohe Wahrscheinlichkeit eines Schadens für die

Rechte und Freiheiten der Nutzer, die sich in der Veröffentlichung der Daten im Darknet nachfolgend auch realisiert hat.

Eine Ausnahme von der Benachrichtigungspflicht liegt nicht vor.

Nach Art 34 Abs. 3 a) DSGVO ist eine Benachrichtigung nicht erforderlich, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt hat, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung.

Dies ist hier nicht geschehen. Die gescrapten Daten der Nutzer sind bis heute im Darknet veröffentlicht und für jedermann zugänglich.

Ferner ist eine Benachrichtigung nicht gem. Art. 34 Abs. 3 c) DSGVO entbehrlich. Dafür müsste die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden sein. In diesem Fall hätte stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Eine zeitnahe Benachrichtigung der betroffenen Nutzer – die Beklagte hatte spätestens im September 2019 Kenntnis von dem Scraping-Vorfall (vgl. Anlage B 10, Anlagenband zum Schriftsatz vom 08.11.2022) - hätte für die Beklagte, die auch eine Vielzahl von Nutzern auf digitalem Weg einfach erreichen kann, nicht bestanden.

1.3. Betroffenheit des Klägers von den Datenschutzverstößen

Der Kläger war von dem Scraping-Vorfall betroffen. Dies steht zur Überzeugung der Kammer (§ 286 ZPO) aufgrund der persönlichen Anhörung des Klägers fest. Der Kläger hat plausibel geschildert, dass er von dem streitgegenständlichen Scraping-Vorfall betroffen ist. Er hat dargelegt, dass er und seine Frau, nicht aber sein Sohn von dem Datenschutzleck, das durch die Medien gegangen sei, betroffen seien, obwohl sie alle drei die Facebook-Plattform nutzten. Daraus folgt zur Überzeugung der Kammer, dass der Kläger vor Klageerhebung genau geprüft hat oder hat prüfen lassen, wer von seiner Familie von dem streitgegenständlichen Vorgang, der sich für

die Nutzer nur durch Feststellung, dass ihre Daten im Darknet veröffentlicht wurden, betroffen ist. Auf Vorhalt der von ihm mit Schriftsatz vom 30.11.2022 (Bd. II Bl. 112 d.A.) mitgeteilten Daten aus dem Darknet hat der Kläger bestätigt, dass – mit Ausnahme des Datums – es sich auf seinem Facebook-Account hinterlegte Daten handelt und die Einstellung zu seinem Arbeitgeber „öffentlich" war. Auch hierdurch hat er zur Überzeugung der Kammer konkludent bestätigt, dass diese Daten wie vorgetragen im Darknet veröffentlicht sind. Im Übrigen geht die Kammer davon aus, dass auch die Beklagte die technischen und organisatorischen Möglichkeiten hat, im Darknet zu überprüfen, ob und welche Daten des Klägers im Darknet auf der von dem Kläger in der Klageschrift angegebenen Website raidforums.com veröffentlicht sind. Ein Bestreiten mit Nichtwissen, dass die von dem Kläger mitgeteilten Daten im Darknet veröffentlicht wurden, ist damit gemäß § 138 Abs. 4 ZPO nicht zulässig.

1.4. Kausaler Schaden

Der Kläger hat einen ersatzfähigen Schaden im Sinne von Art. 82 DSGVO durch die Datenverstöße der Beklagten erlitten.

Der Schaden liegt in einem Kontrollverlust persönlicher Daten, der den Kläger belastet. Der Kläger hat nachdrücklich geschildert, dass er im von ihm erinnerten – seine Erinnerungsschwierigkeiten an den genauen Zeitraum lassen sich plausibel damit erklären, dass der Vorgang mehrere Jahre zurückliegt - zeitlichen Zusammenhang mit dem Scraping-Vorfall bereits unerwünschte Kontaktaufnahmen durch Telefonanrufe angeblicher Police-Departements und SMS-Nachrichten über nicht getätigte Paketzustellungen erhalten hat. Auch wenn diese seltsamen, beängstigenden Anrufe und SMS-Nachrichten nicht mit der Veröffentlichung der Daten des Klägers zusammenhängen sollten, so führt nach dem Eindruck der Kammer allein der durch die Veröffentlichung im Darknet mögliche Zusammenhang mit solchen unerwünschten Kontaktaufnahmen bei dem Kläger zu großem Unbehagen, was für die Kammer nachvollziehbar ist.

Mit der unterlassenen Benachrichtigung hat die Beklagte den in der Veröffentlichung der gescrapten Daten liegenden Schaden eines Kontrollverlustes bewusst aufrechterhalten. Durch die unterlassene Benachrichtigung des Klägers wurde diesem die Möglichkeit genommen, geeignete Maßnahmen zu ergreifen, um das Risiko des Missbrauchs seiner Daten zu minimieren. Auch die zuständige Datenschutzbehörde

konnte mangels rechtzeitiger Meldung keine Schritte zur Risikominimierung und Absicherung der Daten einleiten.

Der von dem Kläger aufgrund der Datenverstöße der Beklagten erlittene Kontrollverlust über persönliche Daten begründet einen immateriellen Schadenersatzanspruch gemäß Art. 82 DSGVO.

Ein immaterieller Schadenersatzanspruch gemäß Art. 82 DSGVO unterliegt keiner Erheblichkeitsschwelle. Ausgehend von Erwägungsgrund 146 Satz 3 ist eine weite Auslegung geboten ist, um den Zielen der Verordnung in vollem Umfang zu entsprechen. Hiermit wäre es unvereinbar, würde eine Schadensersatzpflicht nur bei erheblichen Rechtsverstöße eintreten, da dann eine Vielzahl von Fallgestaltungen denkbar wäre, in denen Betroffene trotz Verstößen gegen die Regelungen der DSGVO keine Kompensation erhielten (vgl. EuGH 17. Dezember 2015 - EUGH Aktenzeichen C40714 C-407/14 - Rn. 44). Zudem sollen die betroffenen Personen nach Erwägungsgrund 146 Satz 3 einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten. Dass ein Schaden erlitten ist, ergibt sich nicht erst bei Überschreiten einer gewissen Erheblichkeitsschwelle - der Schwere der Pflichtverstöße und damit einhergehenden Beeinträchtigungen kann vielmehr effektiv auf Ebene der Höhe des Schadensersatzes begegnet werden (vgl. LAG Niedersachsen, Urteil vom 22.10.2021 – 16 Sa 761/20, Rn 196, BeckRS 2021, 32008; Quaas, aaO, Art. 82 Rn 31 f; Nola/Piltz, aaO, Art. 82 Rn 14).

Ob etwas Anderes im Falle bloßer Bagatellschäden zu gelten hat (vgl. Quaas aaO; Nola/Piltz aaO), kann vorliegend dahingestellt bleiben. Das Abschöpfen und Veröffentlichen privater Daten im Darknet und die dadurch ermöglichten Kontaktaufnahmen auch durch mutmaßliche Kriminelle stellt schon objektiv keine Bagatelle für die Betroffenen dar.

1.5. Keine Exkulpation gemäß Art. 82 Abs. 3 DSGVO

Der Beklagten gelingt zur Abwendung des Anspruchs auch nicht die Exkulpation gemäß Art. 82 Abs. 3 DSGVO. Demnach gelingt eine Befreiung nur, wenn der Verantwortliche oder der Auftragsverarbeiter nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Damit wird die Verantwortlichkeit der Beklagten widerleglich vermutet.

Die Beklagte hat die Vermutung ihrer Verantwortlichkeit nicht widerlegt. Die Verhängung der Geldbuße durch die DPC gemäß Art. 83 DSGVO streitet für die Verantwortlichkeit der Beklagten.

1.6. Verschulden

Ein Verschulden ist für die Haftung des Verantwortlichen gemäß Art. 82 DSGVO nicht erforderlich (vgl. BAG, Beschluss vom 26.08.2021 – 8 AZR 253/20, juris).

1.7. Höhe

Die Kammer hält gemäß § 287 ZPO ein Schmerzensgeld für den von dem Kläger durch die Datenschutzverstöße der Beklagten erlittenen Kontrollverlust in Höhe von 500,00 EUR für angemessen, aber auch ausreichend. Wie dargelegt belastet den Kläger die Veröffentlichung seiner Daten im Darknet und den dadurch ermöglichten Zugriff insbesondere auch durch mutmaßliche Kriminelle. Veröffentlicht sind auch Daten, die es ermöglichen könnten, seinen Aufenthaltsort zu bestimmen. Dass er die Gefahr ernst nimmt und ihr aktiv entgegenwirken möchte, hat er dadurch gezeigt, dass er die Suchbarkeitsfunktion seiner Telefonnummer nach Bekanntwerden seiner Betroffenheit von dem Scraping-Vorfall geändert hat. Schmerzensgelderhöhend ist auch in Ansatz zu bringen, dass die Beklagte durch die unterlassene zeitnahe Information über den Scraping-Vorfall bewusst verhindert hat, dass der Kläger zu einem früheren Zeitpunkt geeignete Schritte einleiten konnte, um die Gefahr des Kontrollverlustes zu minimieren. Andererseits muss aber bei der Bemessung des Schmerzensgeldes auch berücksichtigt werden, dass sich das Risiko, die von dem Kontrollverlust ausgehende Gefahr werde sich in einem konkreten Schaden niederschlagen, bisher über einen Zeitraum von mehr als drei Jahren nicht verwirklicht hat. Denn unstreitig hat der Kläger seit dem Vorfall keinen materiellen Schaden aufgrund des Scraping-Vorfalls erlitten. Vorgerichtlich hielt auch der Kläger ein Schmerzensgeld von nur 500,00 Euro für angemessen.

Der Zinsanspruch ergibt sich aus §§ 291, 286 Abs. 1 BGB.

II. Der Feststellungsantrag ist im zulässigen Umfang wie tenoriert auch begründet.

Aus der Verletzung des Rechts auf informationelle Selbstbestimmung des Klägers als absolutem Rechtsgut im Sinne von § 823 BGB und der Möglichkeit eines Schadenseintritts, der sich vorliegend auch schon verwirklicht hat, folgt die

Begründetheit der Feststellungsklage (vgl. BGH, Urt. v. 17. Oktober 2017 – VI ZR 423/16, Rn 49, juris).

Anders als beantragt behauptet die Beklagte einschränkend, dass sich der Scraping-Vofall im Zeitraum Januar 2018 bis September 2019 ereignet haben soll, so dass nur insoweit dem Feststellungsantrag entsprochen werden konnte.

III. Der Unterlassungsantrag zu Ziffer 3. a) ist begründet, der Unterlassungsantrag zu Ziffer 3. b) ist unbegründet.

1. Der Kläger hat gegen die Beklagte auch einen Anspruch Unterlassung analog §§ 1004 Abs. 1 S. 2, 823 Abs. 1 und 2 BGB in Verbindung mit Art. 6 DSGVO hinsichtlich seines Antrags zu Ziffer 3. a).

Der geltend gemachte Unterlassungsanspruch ergibt sich nicht aus Art. 17 DSGVO.

In § 17 DSGVO sind Löschungsansprüche bzw. Ansprüche auf Unterlassen der weiteren Datennutzung geregelt (vgl. BGH Urteil vom 12.10.2021 – VI ZR 488/19, Rn 21, juris). Vorliegend wird indes nicht die Löschung der Daten bzw. das Unterlassen der Weiternutzung begehrt, sondern die Sicherstellung der Weiternutzung der persönlichen Daten auf der Facebook-Plattform durch das Unterlassen rechtswidriger Ermöglichung der Datenweitergabe- und verarbeitung durch die Beklagte.

Da das Unterlassungsbegehren des Klägers nicht von Art. 17 DSGVO erfasst wird, ergibt sich keine Sperrwirkung für die Anwendbarkeit der §§ 1004 Abs. 1 S. 2 analog, 823 Abs. 1 und 2 BGB als nationale Vorschriften (vgl. BGH, Urt. v. 03.05.2022- VI ZR 832/20, Rn 10).

Die Voraussetzungen des § 1004 Abs. 1 S. 2 BGB analog in Verbindung mit § 823 Abs. 1 und 2 BGB sind gegeben.

Analog § 1004 Abs. 1 S. 2 BGB kann bei der Verletzung absoluten Rechts im Sinne von § 823 Abs. 1 BGB der Rechtsinhaber auf das Unterlassen weiterer Störungen klagen.

Das durch die Datenschutzverstöße verletzte Recht des Klägers auf informationelle Selbstbestimmung, das eine Ausprägung des allgemeinen Persönlichkeitsrechts im Sinne von Art. 2 Abs. 1 GG ist, ist ein absolutes Recht im Sinne von § 823 Abs. 1 BGB.

Aufgrund der unter I. dargelegten rechtswidrigen Datenverstöße der Beklagten ist eine Wiederholungsgefahr zu vermuten (vgl. Herrler in: Grüneberg, BGB, 82. Aufl., § 1004 Rn 32 mwN). An die Widerlegung der Vermutung durch den Störer sind hohe Anforderungen zu stellen (Herrler aaO). Hieran gemessen hat die Beklagte die Vermutung nicht widerlegt. Der lange Zeitraum von Januar 2018 bis September 2019, in dem die Beklagte keine wirksamen Maßnahmen gegen das durch das CIT ermöglichte Scraping vorgenommen hat und das Unterlassen einer zeitnahen Benachrichtigung bekräftigen im Gegenteil die Annahme einer Wiederholung von Datenschutzverstößen durch die fortgesetzte Verwendung des CIT zum Nachteil der Nutzer.

2. Ein darüber hinaus gehender Unterlassungsanspruch hinsichtlich des Antrags unter Ziffer 3.b) ist hingegen nicht gegeben. Der durch Ziffer 3. a) tenorierte, weit gefasste Unterlassungsanspruch umfasst das mit Ziffer 3. b) begehrte Unterlassen.

IV. Dem Kläger steht der mit dem Klageantrag zu 4.) verfolgte Auskunftsanspruch gegen die Beklagte nicht zu.

Der Anspruch ist durch Erfüllung untergegangen, § 362 Abs. 1 BGB.

Erfüllt im Sinne des § 362 Abs.1 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 (vgl. BGH, Urteil vom 03.09.2020 - III ZR 136/18 = GRUR 2021,110). Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll.

So liegt es auch im Streitfall. Die Beklagte behauptet, des klägerische Auskunftsersuchen ordnungsgemäß beantwortet zu haben.

V. Der Anspruch auf vorgerichtlichen Rechtsanwaltskosten ergibt sich aus Art. 82 Abs. 1 DSGVO.

Der Höhe nach ist der Anspruch nur teilweise begründet.

Bei der Berechnung der zu erstattenden Anwaltskosten ist lediglich der Gegenstandswert in Ansatz zu bringen, der sich aus den vorgerichtlich geltend gemachten berechtigten Ansprüchen ergibt.

Unter Zugrundelegung eines Gegenstandswertes von 3.000,00 Euro errechnet sich eine Forderung in Höhe von 287,98 Euro.

Der Zinsanspruch folgt aus §§ 288, 291 BGB.

B. Die prozessualen Nebenentscheidungen beruhen auf §§ 92 Abs. 1, 709 S. 1 und 2 ZPO.

[redacted]