Landgericht Chemnitz

Zivilabteilung

Aktenzeichen: **1 O 944/23**

IM NAMEN DES VOLKES

ENDURTEIL

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **Wilde Beuger Solmecke Rechtsanwälte Partnerschaft mbB**, Eupener Straße 67, 50933 Köln, Gz.:

gegen

Meta Platforms Ireland Limited (zuvor: Facebook Ireland Ltd.), 4 Grand Canal Square, Dublin 2, Irland
vertreten durch den Direktor Gareth Lambe

- Beklagte -

Prozessbevollmächtigte:
Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB, Bockenheimer Anlage 44, 60322 Frankfurt am Main, Gz.:

wegen Persönlichkeitsrechtsverletzung, Verstöße gegen die Datenschutz-Grundverordnung (nachfolgend: DSGVO)

hat die 1. Zivilkammer des Landgerichts Chemnitz durch

Richter als Einzelrichter

auf Grund der mündlichen Verhandlung vom 10.01.2024 am 19.02.2024

für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger einen Betrag in Höhe von 300,00 EUR nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 23.08.2023 zu zahlen.

2. Im Übrigen wird die Klage abgewiesen.

3. Die Kosten des Rechtsstreits trägt der Kläger.

4. Das Urteil ist vorläufig vollstreckbar. Die Parteien können die Zwangsvollstreckung (durch die jeweils andere Partei) gegen Sicherheitsleistung i. H. v. 110% des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die jeweils andere Partei vor der Zwangsvollstreckung Sicherheit i. H. v. 110% des jeweils zu vollstreckenden Betrags leistet.

Beschluss:

Der Streitwert wird auf 5.500,00 EUR festgesetzt.

Tatbestand

Der Kläger macht Ansprüche wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung im Zusammenhang mit einem Datenschutzvorfall bei der Beklagten im Zeitraum zwischen Januar 2018 bis September 2019 geltend.

Der Kläger ist Nutzer des von der Beklagten betriebenen sozialen Netzwerkes Facebook. 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 Facebook-Plattform soll Menschen dazu dienen, mit Familie und Freunden in Kontakt zu bleiben, neue Menschen kennenzulernen, Gemeinschaften und Gruppen beizutreten und ganz allgemeine Vorgänge in der Welt zu beobachten. Dazu ermöglicht die Plattform deren Nutzern, persönliche Profile für und über sich zu erstellen und diese mit anderen Nutzern der Plattform zu teilen. Für die Profilerstellung ist die Angabe einer Telefonnummer oder einer E-Mail-Adresse zwingend notwendig. Die Nutzer können auf den persönlichen Profilen Angaben zu verschiedenen Daten ihrer Person machen. Dabei ist die Angabe der Daten Name, Geschlecht und eine von der Beklagten generierten Nutzer-ID zwingende Voraussetzung für

die Registrierung bei Facebook. Diese Profildaten können alle im Internetverkehr aktiven User („alle“) einsehen.

Hinsichtlich weiterer fakultativer Daten (zum Beispiel Wohnort, Geburtsdatum, Beziehungsstatus, E-Mail-Adresse und Telefonnummer (vgl. zu diesen beiden Daten oben)), hält die Beklagte im Rahmen der sog. „Privatsphäre-Einstellungen“ unterschiedliche Einstellungsmöglichkeiten bereit. So kann der Nutzer darüber entscheiden, wie öffentlich die zusätzlich angegebenen Informationen sein sollen, indem nur „Freunde“ oder „Freunde von Freunden“ auf der Facebook-Plattform oder „alle“ die jeweiligen (fakultativen) Informationen einsehen können. Soweit ein Nutzer sich dazu entscheidet, überobligatorisch seine Telefonnummer anzugeben, wird diese im Vergleich zu den zwingenden Einstellungen gesondert behandelt, indem diese standardmäßig nicht von „allen“ eingesehen werden kann.

Die Privatsphäre-Einstellungen auf der Facebook-Plattform unterscheiden sich zwischen der sog. „Zielgruppenauswahl“ und den sog. „Suchbarkeits-Einstellungen“. Während die „Zielgruppenauswahl“ Einstellungsmöglichkeiten umfasst, die festlegen, wer einzelne Informationen im Profil eines Facebook-Nutzers sehen kann, definieren die „Suchbarkeits-Einstellungen“, wer das Profil eines Nutzers u.a. anhand seiner hinterlegten Telefonnummer auffinden kann. Die Standard-Vorsteinstellung (sog. „default“) für die „Suchbarkeits-Einstellung“ bezüglich einer hinterlegten Telefonnummer war im streitgegenständlichen Zeitraum „alle“. Das bedeutet, dass standardmäßig jeder Facebook-User ein Facebook-Profil anhand einer ggf. dort hinterlegten Telefonnummer ausfindig machen konnte. Daneben besteht noch die Auswahlmöglichkeit „Nur Ich“, „Freunde“ oder „Freunde von Freunden“. Das Auffinden eines Nutzerprofils auf der Facebook-Plattform mittels einer Telefonnummer fand u.a. mit dem von der Beklagten angebotenen Contact Import Tool (CIT) statt. Dabei kann in dem Tool in ein Suchfeld eine Telefonnummer eingegeben werden, die – bei Erreichen der „Suchbarkeits-Einstellung“-Kriterien des gesuchten Profils – das entsprechende Nutzerprofil auf Facebook ausgibt.

Der Kläger meldete sich im Jahr 2010 auf der Facebook-Plattform an und durchlief dabei den Registrierungsprozess. Dabei gab er neben den zwingend für die Registrierung erforderlichen und stets öffentlich einsehbaren Daten Name, Geschlecht und Nutzer-ID u.a. auch seine Telefonnummer an. Die „Suchbarkeits-Einstellung“ bezüglich dieser Telefonnummer war zumindest seit dem 07.01.2014 auf „Alle“ eingestellt (Anlage B 20). Auf dem Facebook-Profil des Klägers war im streitgegenständlichen Zeitraum die hier fragliche Telefonnummer nicht öffentlich einsehbar.

Bei der Registrierung wurde der Kläger auf die Datenschutz- und Cookierichtlinie der Beklagten hingewiesen. Den Nutzern werden zudem im „Hilfebereich“, der unmittelbar auf der Facebook-Homepage verlinkt ist, Informationen über die Privatsphäre-Einstellungen zur Verfügung gestellt. Auf diese Einstellungen kann unter der Überschrift „Privatsphäre, Datenschutz und Sicherheit“ zugegriffen werden. Diesbezüglich wird auf die Abbildungen in der Klageschrift sowie die Anlagen B 1 bis B 11 Bezug genommen.

Im Zeitraum von Januar 2018 bis September 2019 kam es auf der Facebook-Plattform zu sog. „Scraping“, also dem massenhaften, automatisierten Sammeln persönlicher öffentlicher Daten von Facebook-Nutzern. Dieses Sammeln von Daten mittels automatisierter Tools und Methoden war und ist nach den Nutzungsbedingungen der Beklagten untersagt.

Im Zuge des „Scrapings“ lasen und persistierten Dritte zumindest die Nutzer-ID, Name sowie das Geschlecht der Klagepartei aus den öffentlich zugänglichen Daten auf den Facebook-Profilen aus und verknüpften diese mit einer Telefonnummer. Dazu luden die „Scraper“ mithilfe des „CIT“ Kontakte hoch, welche mögliche Telefonnummern von Nutzern enthielten, um festzustellen, ob diese Telefonnummern mit einem Facebook-Konto verbunden sind. Soweit sie feststellen konnten, dass eine Telefonnummer mit einem Facebook-Konto verknüpft war, kopierten sie die – per „Zielgruppenauswahl“ – öffentlich einsehbaren Informationen aus dem betreffenden Nutzerprofil und fügten die Telefonnummer den abgerufenen, öffentlich einsehbaren Daten hinzu. Diese Verknüpfung zwischen öffentlich einsehbaren Daten und der fraglichen Telefonnummer geschah gerade auch dann, wenn die im Profil hinterlegte Nummer in der „Zielgruppenauswahl“ nicht öffentlich einsehbar gemacht worden war. Das genaue Vorgehen der Scraper steht im Streit.

Anfang April 2021 veröffentlichten Unbekannte nach Angaben eines Artikels des „Business Insider“ vom 03.04.2021 die Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern in einer ungesicherten Datenbank im Internet. Darunter befanden sich auch Daten des Klägers, zumindest Name, Vorname, Geschlecht und Nutzer-ID. Die Beklagte veröffentlichte als Reaktion darauf am 06.04.2021 den Artikel „Die Fakten zu Medienberichten über Facebook-Daten“ (Anlage B 12). Sie informierte die Datenschutzbehörde Irish Data Protection Commission nicht über den Vorfall. Stattdessen ergriff die Beklagte als Reaktion auf die Medienberichterstattung Maßnahmen, um Nutzern Informationen über das „Scraping“ sowie die Möglichkeiten zur Änderung ihrer Privatsphäre-Einstellungen zur Verfügung zu stellen.

Die irische Datenschutzbehörde verhängte gegen die Beklagte wegen des streitgegenständli-

chen Datenschutzvorfalls mit ihrer Entscheidung vom 25.11.2022 ein noch nicht rechtskräftiges Bußgeld in Höhe von 265 Millionen Euro.

Mit E-Mail der Prozessbevollmächtigten des Klägers vom 21.04.2023 forderte dieser die Beklagte zur Schadensersatzzahlung in Höhe von 1.000,00 EUR, zur Zahlung außergerichtlicher Rechtsverfolgungskosten, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft darüber auf, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht worden waren (Anlage K 1). Hierauf hat die Beklagte mit Anwaltsschreiben vom 15.01.2024 (Anlage B 20) erwidert und teilte mit, welche Datenkategorien nach den ihr zum Zeitpunkt der Auskunftserteilung verfügbaren Erkenntnissen in den durch Scraping abgerufenen Daten erscheinen und mit den auf dem Facebook-Profil der Klagepartei verfügbaren Informationen übereinstimmen.

Der Kläger trägt vor, der Zugriff Dritter auf die Daten des Klägers sei nur deshalb erfolgt, weil die Beklagte die sie betreffenden Grundsätze und Pflichten aus der DSGVO bewusst nicht eingehalten habe.

Der gesamte Datenschutzvorfall bestehe aufgrund einer Sicherheitslücke der Facebook-Plattform. So seien die unbekannten Dritten nur wegen des nicht hinreichend gesicherten Contact Import Tools zur Korrelation zwischen Facebook-Profilen und deren Telefonnummern befähigt gewesen.
Weiter fehle zudem ein ausdrücklicher Hinweis der Beklagten, dass standardmäßig die Telefonnummer eines Nutzers von jedermann mit dessen Profil verknüpft werden kann. Außerdem seien die Einstellungen zur Sicherheit bezüglich der Telefonnummer auf Facebook bewusst so undurchsichtig und kompliziert gestaltet, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne.

Eine Information über etwaige Risiken oder über die Verwendung der Telefonnummer erfolge nicht, obwohl ein Nutzer geradezu zur Verwendung des „CIT“ gedrängt werde. Dies widerspräche allerdings den Grundsätzen eines nutzerfreundlichen Datenschutzes und damit dem Prinzip der Datenminimierung und des „privacy by default“-Grundsatzes.

Der Kläger trägt vor, dass die von ihm im „Scraping-Vorfall“ erlangten Daten insbesondere für gezielte Betrugsangriffe (u.a. „Phishing“) genutzt würden. Zudem könne zum jetzigen Zeitpunkt noch nicht abgesehen werden, welche Dritten Zugriff auf seine Daten erhalten hätten

und für welche konkreten kriminellen Zwecke die Daten missbraucht würden. Er habe daher durch den Datenschutzvorfall ungewollt in erheblichem Ausmaß die Kontrolle über seine abgegriffenen Daten verloren und werde seitdem vermehrt von Unbekannten in bösartiger Absicht via E-Mail und SMS kontaktiert. Durch die Veröffentlichung seiner Daten lebe der Kläger in einem Zustand von Unwohlsein. Er habe große Sorgen über einen möglichen Missbrauch seiner Daten.

Der Kläger beantragt:

1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 EUR nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.
2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.
3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,
    a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,
    b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei auf Einstellung „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.
4. Die Beklagte wird verurteilt der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich

welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.

5. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 887,02 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt:

Die Klage wird abgewiesen.

Die Beklagte trägt vor, dass die Daten weder durch Hacking, noch durch mangelnde Sicherheitssysteme der Beklagten in die Hände der Dritten gefallen seien. Vielmehr liege lediglich ein automatisiertes massenhaftes Sammeln ohnehin öffentlicher, und damit nicht vertraulicher Daten vor. Die so abgegriffenen Daten seien im Einklang mit den jeweiligen Privatsphäre-Einstellungen der Nutzer für jedermann öffentlich auf deren Profil einsehbar gewesen. Daten wie z.B. „Bundesland“ und „weitere korrelierende Daten“ seien nicht durch das „Scraping“ erlangt, da diese schon nicht den Profilfeldern auf der Plattform entsprächen.

Der Kläger sei sowohl über die Einstellungsmöglichkeiten als auch über mögliche Konsequenzen seiner Einstellungen hinreichend durch die Beklagte informiert worden. Die Standard-Voreinstellungen der Beklagten seien notwendig, um den Hauptzweck der Facebook-Plattform, die Vernetzung von Menschen, zu ermöglichen.

Die Beklagte habe hinreichende technische und organisatorische Maßnahmen ergriffen, um das Risiko von „Scraping“ zu unterbinden. Es sei grundsätzlich unmöglich, das „Scraping“ öffentlich einsehbarer Daten völlig zu verhindern, ohne den Kommunikationszweck der Plattform zu unterlaufen.

Letztlich sei der vorgetragene Kontrollverlust des Klägers über seine abgegriffenen Daten kein erstattungsfähiger Schaden. Selbst wenn der Kläger einem solchen Kontrollverlust unterliege, sei dies nicht der Beklagten zuzurechnen, da vorliegend nur ohnehin öffentlich einsehbare Daten abgegriffen worden seien. Außerdem fehle es an hinreichendem Vortrag zur Kausalität der behaupteten Datenschutzverletzungen und der daraus resultierenden Folgen.

Die Beklagte ist der Ansicht, dass die klägerischen Anträge zu 1), zu 2) und zu 3) unzulässig seien. Dem klägerischen Antrag zu 2) fehle bereits das notwendige Feststellungsinteresse.

Weiter sei der mit dem Antrag zu 4) geltend gemachte Auskunftsanspruch bereits außergerichtlich, nämlich mit Schreiben vom 15.01.2024 erfüllt worden.

Schließlich umfasse Art. 82 DSGVO keinen der von dem Kläger geltend gemachten Verstöße gegen die DSGVO. Anwaltskosten seien mangels Verzuges unbegründet.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die gewechselten Schriftsätze der Parteien nebst Anlagen Bezug genommen. Der Einzelrichter hat den Kläger persönlich informatorisch angehört. Wegen des Ergebnisses der Parteianhörung wird auf das Protokoll zur mündlichen Verhandlung vom 10.01.2024 Bezug genommen.

Entscheidungsgründe

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

A.

Die Klage ist bereits hinsichtlich der Anträge zu 2. und 3. unzulässig, im Übrigen zulässig.

I.

1.

Der klägerische Antrag zu 1) ist zulässig. Er ist im Sinne des § 253 Abs. 2 Nr. 2 ZPO hinreichend bestimmt.

Entgegen der Ansicht der Beklagten liegt kein Fall einer unzulässigen alternativen Klagehäufung vor (so auch: OLG Dresden, Urteil vom 05.12.2023 – 4 U 709/23; OLG Hamm, Urteil vom 15.08.2023 – 7 U 19/23; OLG Köln, Urteil vom 07.12.2023 – 15 U 33/23 und OLG Stuttgart, Urteil vom 22.11.2023 – 4 U 20/23).

2.

Der mit dem klägerischen Antrag zu 2) geltend gemachte Feststellungsantrag ist unzulässig, da dem Kläger das nach § 256 Abs. 1 ZPO erforderliche Feststellungsinteresse fehlt (so auch OLG Dresden, aaO; OLG Hamm, aaO und OLG Köln, aaO).

Ein Feststellungsinteresse besteht zwar bereits schon dann, wenn die Schadensentwicklung noch nicht gänzlich abgeschlossen und der Kläger aus diesem Grund nicht im Stande ist, seinen Anspruch deshalb ganz oder teilweise zu beziffern (OLG Hamm, Urteil vom 21.05.2019 – 9 U 56/18). Das Feststellungsinteresse ist daher nur dann zu verneinen, wenn aus der Sicht des Geschädigten keinerlei Besorgnis besteht, zumindest mit dem Eintritt eines Schadens zu rechnen (BGH, Beschluss vom 09.01.2007 -VI ZR 133/06).

Nach Ansicht des Gerichts besteht für den Kläger auf Basis dessen eigenen Vortrages kein Grund zur Besorgnis wegen des streitgegenständlichen „Scraping-Vorfalls“ mit einem künftigen Schadenseintritt zu rechnen, da sämtliche seiner Befürchtungen zur künftigen Schadensentwicklung rein theoretischer Natur sind. Ihm ist bis heute kein materieller (s.u.) Schaden entstanden und er hat auch keine Anhaltspunkte dafür vorgetragen, die solche (zudem zwingend kausal auf den Vorfall zurückzuführenden) Schäden in Zukunft als möglich erscheinen lassen, zumal die Veröffentlichung seiner personenbezogenen Daten im Darknet bereits mehrere Jahre vorhält.

3.
Weiter ist auch der klägerische Antrag zu 3) unzulässig, da er nicht hinreichend bestimmt gefasst und damit unzulässig ist (so auch OLG Dresden, aaO; OLG Hamm, aaO; OLG Köln aaO und OLG Stuttgart, aaO).

Nach § 253 Abs. 2 Nr. 2 ZPO darf ein Unterlassungsantrag – und nach § 313 Abs. 1 Nr. 4 ZPO eine darauf beruhende Verurteilung – nicht derart undeutlich gefasst sein, dass der Streitgegenstand und der Umfang der Prüfungs- und Entscheidungsbefugnis des Gerichts (§ 308 Abs. 1 ZPO) nicht erkennbar abgegrenzt sind, da die Entscheidung darüber, was der Beklagten verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt.

Diesen Anforderungen wird der klägerische Antrag zu 3) nicht gerecht.

II.

Das angerufene Landgericht Chemnitz ist international, sachlich und örtlich zuständig.

1.
Das Landgericht Chemnitz ist zunächst gem. Art. 6 Abs. 1, Art. 18 Abs. 1 Alt. 2 EuGVVO international zuständig (vgl. OLG Dresden, aaO).

2.

Das Landgericht Chemnitz ist gemäß §§ 23 Nr. 1, 71 Abs. 1 GVG sachlich zuständig.

3.

Die örtliche Zuständigkeit des Landgerichts Chemnitz folgt aus Art. 18 Abs. 1 2. Alt. EuGVVO.

B.

Die Klage ist lediglich hinsichtlich des Antrags zu 1) begründet.

I.

Dem Kläger steht gegen die Beklagte ein Schadensersatzanspruch in Höhe von 300,00 EUR gem. Art. 82 Abs. 1 DSGVO zu.

Nach dieser Vorschrift hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein kausaler materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen (EuGH, Urteil vom 04.05.2023 – C-300/21).

1.

Der Anwendungsbereich der DSGVO ist sowohl persönlich, räumlich und sachlich, zeitlich jedoch nur hinsichtlich der Datenschutzverstöße nach Inkrafttreten der DSGVO am 25.05.2018 (Art. 99 Abs. 2 DSGVO) eröffnet.

a.

Der Kläger ist als natürliche Person nach Art. 4 Nr. 1 DSGVO in persönlicher Hinsicht anspruchsberechtigt. Die Beklagte ist als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO taugliche Anspruchsgegnerin (OLG Köln, aaO).

b.

Der räumliche Anwendungsbereich der DSGVO ist gem. Art. 2, 3 DSGVO eröffnet.

Gemäß Art. 3 Abs. 1 DSGVO erfasst der räumliche Anwendungsbereich die Niederlassung eines Verantwortlichen oder eines Auftragbearbeiters in der europäischen Union, unabhängig davon, ob die Verarbeitung auch in der Union stattfindet.

Die Beklagte hat ihren Sitz in Irland, einem Mitglied der europäischen Union.

c.
Weiter ist der sachliche Anwendungsbereich des Art. 82 Abs. 1 DSGVO für alle von dem Kläger behaupteten Verletzungen der DSGVO durch die Beklagte eröffnet.

Der Ansicht der Beklagten, dass im Rahmen des Anwendungsbereiches von Art. 82 Abs. 1 DSGVO eng auf den Begriff der „Datenverarbeitung“ abzustellen ist, ist nicht zu folgen. Der Wortlaut des Art. 82 Abs. 1 DSGVO „Verstoß gegen die Verordnung“ ist grundsätzlich weit gefasst und dementsprechend auch so zu verstehen (Paal/Pauly/*Frenzel*, DS-GVO 3. Aufl., Art. 82 Rn. 8). Vom Schutzbereich des Art. 82 Abs. 1 sind folglich alle formellen und materiellen Verstöße umfasst, ohne dass es auf die Datenverarbeitung als solche ankommt (BeckOK DatenschutzR/*Quaas*, Stand: 01.08.2022, DS-GVO Art. 82 Rn. 14; vgl. auch LAG Hamm, ZD 2021, 710; ArbG Düsseldorf, ZD 2020, 649; Möllenkamp, NZA-RR 2020, 416 Franck, ZD 2021, 680). Eine andere Ansicht würde dem insoweit eindeutigen Wortlaut des Art. 82 Abs. 1 DSGVO und dessen Schutzzweck, dem umfangreichen Schutz der Betroffenen, entgegenstehen.

d.
Verstöße im Rahmen des Anmeldeprozesses, der bei dem Kläger im Jahr 2010 erfolgt ist, sind von Art. 82 DSGVO nicht erfasst (vgl. OLG Dresden, aaO). Dies betrifft den Vorwurf der unzureichenden Information bei erstmaliger Erhebung seiner Daten im Rahmen dieses Registrierungsprozesses (Art. 13 DSGVO) und den Verstoß gegen die Pflicht zu einer Datenschutzfolgenabschätzung (Art. 35 DSGVO) vor Festlegung der Kriterien für die Suchbarkeitsfunktion und die Einführung des CIT.

Demgegenüber ist zugunsten des Klägers zu unterstellen, dass der streitgegenständliche „Scraping-Vorfall“ sich nach Inkrafttreten der DSGVO ereignet hat, auch wenn die Beklagte ihn lediglich auf den Zeitraum Januar 2018 bis September 2019 eingrenzt. Die Beklagte ist ihrer sekundären Darlegungslast nicht dahingehend nachgekommen, dass sich der streitgegenständliche „Scraping-Vorfall“ vor Inkrafttreten der DSGVO ereignet hat (vgl. OLG Dresden, aaO).

2.
Die Beklagte hat im Zusammenhang mit dem streitgegenständlichen „Scraping-Vorfall“ als Verantwortliche (vgl. dazu: EuGH, Urteil vom 21.12.2023, C-667/21, Rdnr. 93 f., juris) im Sinne

des Art. 4 Nr. 7 DSGVO gegen Artt. 25 Abs. 1, 2; 5 Abs. 1 lit. a, b; Art. 6 Abs. 1 Unterabs. 1 und 13 DSGVO verstoßen.

a.
Die Beklagte hat durch die Ausgestaltung ihrer standardmäßigen Voreinstellungen gegen ihr obliegende Verpflichtungen aus Art. 25 Abs. 1, 2 DSGVO und Artt. 5 Abs. 1 lit. a, b, Art. 6 Abs. 1 Unterabs. 1 verstoßen (so auch OLG Dresden, aaO).

Nach Art. 25 Abs. 2 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, um den Anforderungen der DSGVO gerecht zu werden.

Durch standardmäßige Voreinstellungen („privacy by default“) soll sichergestellt werden, dass nur diejenigen personenbezogenen Daten von dem Verarbeiter erhoben werden, die für den jeweiligen Verarbeitungszweck notwendig sind (Sydow/Marsch/*Mantz,* DS-GVO/BDSG 3. Aufl., DS GVO Art. 25 Rn. 3,7).

Durch Art. 25 Abs. 2 DSGVO soll kein genereller Zwang zur standardmäßigen Einrichtung einer datenschutzfreundlichsten Voreinstellung statuiert werden. Vielmehr sollen datenschutzfeindliche Voreinstellungen unterbunden werden. Welche Erhebung datenschutz(un)freundlich ist, bestimmt sich dabei maßgeblich nach dem Zweck der Erhebung und Verarbeitung der betroffenen personenbezogenen Daten. Demnach sind nur Voreinstellungen für solche Verarbeitungen zulässig, die für den Verarbeitungszweck erforderlich sind (Paal/Pauly/*Martini,* DS-GVO 3. Aufl., Art. 25 Rn. 45). Nach Art. 25 Abs. 2 S. 2 DSGVO gilt der Grundsatz „privacy by default“ für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Gegen diese Anforderungen hat die Beklagte verstoßen, indem die standardmäßigen Voreinstellungen für die „Suchbarkeits-Einstellung“ der vom Kläger hinterlegten Telefonnummer auf „Alle“ eingestellt waren. Diese Voreinstellung war nicht für den Verarbeitungszweck der Beklagten erforderlich.

aa.
Die default-Einstellung hinsichtlich der „Suchbarkeits-Einstellung“ der klägerischen Telefonnummer verstößt gegen Art. 25 Abs. 3 S. 2 DSGVO.

Die Norm adressiert insbesondere soziale Netzwerke. Der Verantwortliche – hier die Beklagte

– soll durch geeignete technische und organisatorische Maßnahmen sicherstellen, dass personenbezogene Daten eines Nutzers – hier des Klägers – nicht ohne dessen Eingreifen einer unbestimmten Anzahl von Personen zugänglich gemacht wird (Ehmann/Selmayr/*Baumgartner,* DS-GVO 2. Aufl., Art. 25 Rn. 20). Dem Nutzer muss die Möglichkeit verbleiben, die Hoheit über seine Daten und deren Veröffentlichung bzw. Verarbeitung aktiv zu gestalten. Konkret bezogen auf soziale Netzwerke folgt daraus, dass ein Nutzer selbst in die Lage versetzt werden muss, darüber zu entscheiden, ob und mit wem er diese inner- und außerhalb des Netzwerkes teilt (LG Paderborn, Urteil vom 19.12.2022 – 3 O 99/22).

Aus Art. 25 Abs. 2 S. 3 DSGVO folgt, dass Inhalte und Daten eines Nutzers nicht standardmäßig mit anderen geteilt werden bzw. für diese verfügbar sind. Als Voreinstellung ist somit der kleinstmögliche Adressatenkreis zu wählen (Gola/Heckmann/*Nolte*/*Werkmeister,* DS-GVO 3. Aufl., Art. 25, Rn. 31).

Dem widerspricht die fragliche Gestaltung der Beklagten diametral. Durch die Voreinstellung der „Suchbarkeits-Einstellung“ hinsichtlich der Telefonnummer des Klägers auf „Alle“ war es einer unbegrenzten Anzahl von natürlichen Personen möglich, das Facebook-Profil des Klägers mittels des von der Beklagten vorgehaltenen CIT aufzufinden, wodurch weitere persönliche Daten, die zwingend öffentlich sind, einsehbar werden.

bb.
Die von der Beklagten standardmäßig getroffene „Suchbarkeits-Einstellung“ hinsichtlich der der von dem Kläger hinterlegten Telefonnummer war auch nicht zur Erreichung ihres Verarbeitungszweckes erforderlich. Erforderlichkeit im Sinne des Artt. 25 Abs. 2 S. 1, 6 Abs. 1 Unterabschnitt 1 lit. b DSGVO besteht dann, wenn sich der Verarbeitungszweck ohne die standardmäßig erhobenen Daten nicht erreichen lässt (vgl. ErwGr 39, S. 8).

Nach dem eigenen Vortrag der Beklagten dient die von ihr betriebene Facebook-Plattform dazu, Menschen miteinander zu verbinden und Kommunikation zwischen ihnen zu ermöglichen. Zwar ist der Verarbeiter in der Wahl seines Verarbeitungszweckes frei (Paal/Pauly/*Martini,* DS-GVO 3. Aufl., Art. 25 Rn. 45c). Für die Erreichung dieses kommunikativen und verbindenden Verarbeitungszweckes war es nach Ansicht des Einzelrichters jedoch nicht erforderlich, dass die „Suchbarkeits-Einstellung“ der bei Facebook hinterlegten Telefonnummer „Alle“ war. Zwar mag es dem Verarbeitungszweck der Beklagten nützlich sein, wenn die Nutzer der Facebook-Plattform auch über ihre hinterlegte Telefonnummer aufgefunden werden können. Für den Einzelrichter erscheint es aber fernliegend, dass sich der kommunikative und verbin-

dende Zweck der Facebook-Plattform ohne die Auffindbarkeit eines Facebook-Users über seine Telefonnummer nicht erreichen lässt. Das Wissen um eine Mobilfunknummer einer anderen Person spricht bereits deutlich dafür, dass sich diejenigen Personen bereits kennen. Selbst wenn dies nicht namentlich der Fall sein sollte, ließe sich eine Kontaktaufnahme unter Zuhilfenahme ebendieser Telefonnummer bewerkstelligen, ohne dass dafür auf die Facebook-Plattform und deren CIT zugegriffen werden müsste. Eine Suche über Facebook erübrigt sich in diesem Fall. Die Möglichkeit der Suche eines anderen Facebook-Nutzers mittels dessen Telefonnummer stellt somit lediglich einen zusätzlichen Nutzer-Service dar, der zur Erreichung der selbst deklarierten Zwecke der Beklagten nicht erforderlich ist und darüber hinaus auch Datenmissbrauch mittels Scraping ermöglicht.

Die Nichterforderlichkeit der fraglichen Voreinstellung ist auch daran erkennbar, dass die „Suchbarkeits-Einstellung“ der Telefonnummer restriktiv geändert werden kann, ohne dass dies ersichtlich dem kommunikativen Aspekt der Plattform der Beklagten entgegensteht (vgl. KG Berlin, Urteil vom 20.12.2019 - 5 U 9/18, Rn. 39).

cc.

Eine andere Bewertung wird auch nicht dadurch gerechtfertigt, dass der Kläger die Suchbarkeitseinstellungen nachträglich ändern oder einen „Privatsphäre-Check“ durchführen konnte. Art. 25 Abs. 2 DSGO stellt auf datenschutzfreundliche Voreinstellungen und nicht auf nachträgliche Änderungsmöglichkeiten ab. Entgegen der Ansicht der Beklagten sind vielmehr Voreinstellungen zu treffen, die dem Nutzer mittels eines „Opt-In-Verfahrens“ ermöglichen, seine personenbezogenen Daten über den voreingestellten Adressatenkreis hinaus zugänglich zu machen (Sydow/Marsch/*Mantz,* DS-GVO/BDSG 3. Aufl., DSGVO Art. 25 Rn. 69).

dd.

Da der Kläger am 25.05.2018, also zum Geltungsbeginn der DSGVO, bereits registriert war, es aber zuvor entgegen Art. 25 Abs. 2 DSGVO („privacy by default“) die nicht datenschutzfreundliche Grund-/Voreinstellung der Suchbarkeitseinstellung auf „alle“ gab, musste die Beklagte sicherstellen, dass nicht geänderte unfreundliche Voreinstellungen zum 25.05.2018 unter Abkehr vom „Opt-Out“-System geändert wurden (OLG Hamm, aaO). Eine solche Änderung hat sie unstreitig nicht vorgenommen. Entgegen der auch in diesem Verfahren vertretenen Auffassung der Beklagten ist eine Rechtfertigung dieses Verhaltens über Art. 6 Abs. 1 lit f) DSGVO nicht möglich (s.o.).

ee.

Die rechtliche Bewertung des Einzelrichters wird indiziell auch durch die Entscheidung der irischen Datenschutzbehörde DPC gestützt. Diese hat am 28.11.2022 gegen die Beklage u.a. wegen eines Verstoßes gegen Art. 25 Abs. 2 DSGVO ein (noch nicht rechtskräftiges) Bußgeld in Höhe von 265 Mio. Euro verhängt.

b.
Die Beklagte hat die ihr nach Art. 13 DSGVO auferlegten Informations- und Aufklärungspflichten verletzt. Sie hat den Kläger zum Zeitpunkt der Erhebung seiner Mobilfunknummer nicht im ausreichende Maße über die Zwecke der Erhebung bzw. Verarbeitung seiner Telefonnummer aufgeklärt (ebenso: OLG Dresden, aaO; OLG Hamm aaO).

aa.
Nach Art. 13 DSGVO treffen den Verantwortlichen eines Datenverarbeitungsprozesses zum Zeitpunkt der Erhebung von personenbezogenen Daten umfangreiche Informationspflichten.
Eine Verletzung dieser Pflicht besteht bereits dann, wenn der Verantwortliche der betroffenen Person nicht bereits bei Datenerhebung die nach Art. 13 Abs. 1 und 2 DSGVO erforderlichen Informationen vollständig und inhaltlich korrekt mitteilt.
Nach Erwägungsgrund 60 der DSGVO erfordern die Grundsätze einer fairen und transparenten Verarbeitung, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird.

Der Kläger gab im Rahmen seiner Registrierung auf der Facebook-Plattform seine Mobilfunknummer an. Bei der Mobilfunknummer des Klägers handelt es sich um ein personenbezogenes Datum gemäß Art. 4 Nr. 1 DSGVO. Bei der Hinterlegung der Telefonnummer in seinem Facebook-Profil wurde der Kläger durch die Beklagte darüber informiert, dass diese für verschiedene Zwecke benutzt wird (Anlagen B 5, 6, 7, 9 und 18).

Der Kläger wurde jedoch durch die Beklagte nicht hinreichend über den Zweck der Verwendung seiner Mobilfunknummer für das seitens der Beklagten bereitgestellte Contact-Import-Tool aufgeklärt, obwohl eine solche Information vorliegend notwendig war (ebenso OLG Hamm, aaO).

(1)
Seitens des Einzelrichters ist nicht ersichtlich, dass die Beklagte den Kläger bei der Angabe seiner Mobilfunknummer hinreichend im Sinne des Art. 13 Abs. 1 lit. a DSGVO über die Verwendung seiner Nummer im Zusammenhang mit dem Contact-Import-Tool (CIT) aufgeklärt

hat.

Das CIT ermöglicht, dass jedermann mithilfe einer Mobilfunknummer abgleichen kann, ob ein Profil auf der Facebook-Plattform existiert, welches diese Mobilfunknummer hinterlegt hat und entsprechend seiner „Suchbarkeits-Einstellungen“ von dem jeweiligen Abgleichenden gefunden werden kann.

(2)
Eine solche Aufklärung lässt sich zunächst nicht aus der Datenschutzrichtlinie der Beklagten (Anlage B 11) entnehmen.

Unter der Überschrift „Wie verwenden wir diese Informationen“ gibt die Beklagte an, dass von einem Facebook-Nutzer bereitgestellten Information auf der Plattform zur Bereitstellung, Verbesserung und Entwicklung der Dienste, zur Kommunikation mit dem die Daten bereitstellenden Nutzer, für Werbezwecke und zur Förderung der Sicherheit verwendet werden. Weder ein konkreter noch ein abstrakter Hinweis auf die Benutzung der angegebenen Mobilfunknummer für das CIT sind enthalten. Solche Hinweise finden sich auch nicht unter der Überschrift „Wie werden diese Informationen geteilt“ derselben Datenrichtlinie.

(3)
Weiter kann eine im Sinne des Art. 13 Abs. 1 lit. c DSGVO hinreichende Information der Beklagten gegenüber dem Kläger hinsichtlich der Verwendung der Telefonnummer für das CIT auch nicht in den vorgelegten Anlagen B 1 bis 11 gesehen werden.

Die vorgelegten Auszüge enthalten allgemein gefasste Informationen über die Verwendungsmöglichkeiten der bei Facebook hinterlegten Mobilnummer. Nach Ansicht des Einzelrichters wird diese Information jedoch nicht der der Beklagten obliegenden Informationspflichten nach Art. 13 Abs.1 lit. c DSGVO gerecht.

In diesem Rahmen muss der Verantwortliche, hier die Beklagte, der betroffenen Person, hier dem Kläger, mitteilen, zu welchem Zweck sie ihre personenbezogenen Daten, hier die klägerische Mobilfunknummer, verarbeiten will. Die Mitteilung über die Zwecke der Verarbeitung der erhobenen personenbezogenen Daten ist für die Transparenz der Verarbeitung von hoher Bedeutung (Paal/Pauly/Paal/*Hennemann* DSGVO 3. Aufl., Art. 13 Rn 16). Die Angaben dazu müssen nicht nur vollständig, sondern auch so detailliert sein, dass sich der Kläger ausmalen kann, mit welcher Datenverarbeitung er zu rechnen hat (Kühling/Buchner/*Bäcker*, DSGVO 3.

Aufl., Art. 13 Rn 25; Ehmann/Selmayr/*Knyrim* DSGVO 2. Aufl., Art. 13 Rn 37).

Diesen Anforderungen wird die Beklagte vorliegend nicht gerecht. Sie verweist lediglich auf weitere Einstellungsmöglichkeiten, in denen reguliert werden kann, wer nach dem Nutzer suchen kann (vgl. Anlage B 7).

Einerseits stellt die Beklagte hier nur allgemein auf Kontaktinformationen ab, ohne konkret auf die Verwendung der hinterlegten Mobilnummer einzugehen. Weiter wird daraus nicht ansatzweise die Verwendung der vom User hinterlegten Mobilnummer für das CIT ersichtlich. Dem Nutzer, der gerade im Zuge ist, seine personenbezogenen Daten preiszugeben, wird nicht hinreichend deutlich gemacht, dass jedermann, der zufällig oder nicht über diese Handynummer verfügt, durch das von der Beklagten bereitgestellte CIT sein Facebook-Profil ausfindig machen kann.

Die Möglichkeit, dass durch die Preisgabe der Telefonnummer über das CIT der Beklagten auch durch einen völlig Fremden ein Facebook-Profil ermittelt werden kann, wird dadurch nach Ansicht des Einzelrichters unvollständig und intransparent dargestellt.
Im Übrigen ersetzt der bloße Verweis auf Einstellungsmöglichkeiten nicht die detaillierte Darlegung des Verwendungszweckes der hinterlegten Mobilnummer (s.o.).

(4)
Ein detaillierter Hinweis der Beklagten der Verwendung der vom Nutzer hinterlegten Mobilfunknummer kann auch nicht in den von der Beklagten verfassten Informationen aus dem „Hilfebereich“, vorgelegt als Anlage B 1 gesehen werden.

bb.
Ein Verstoß der Beklagten scheidet nicht deswegen aus, weil der Kläger gemäß Art. 6 Abs. 1 S. 1 lit. a) DSGVO in die Erhebung seiner Mobilfunknummer eingewilligt hat.

Eine solche Einwilligung entfaltet keine Wirkung, wenn die betroffene Person nicht hinreichend darüber informiert wurde, welche Daten zu welchem Zweck erhoben wurden (Ehmann/Selmayr/*Heberlein* DS-GVO, 2. Aufl. Art. 6 Rn. 8). Eine solche vollständige Information fand vorliegend gerade nicht statt (s.o.).

c.
Im Hinblick auf die unter a) und b) festgestellten Verstöße der Beklagten kann offenbleiben, ob

sie zudem gegen ihre Verpflichtung verstoßen hat, ausreichende geeignete technische und organisatorische Maßnahmen zu treffen, um die personenbezogenen Daten gegen unbefugte Zugriffe Dritter zu schützen, Art. 24, 32 DSGVO (OLG Dresden, Urteil vom 05.12.2023 - 4 U 709/23).

d.

Die Frage, ob der Beklagten vorliegend ein Verstoß gegen Melde- und Benachrichtigungspflichten nach den Artt. 33, 34 DSGVO anzulasten ist, kann ebenso dahinstehen. Dem Klagevortrag lässt sich nach Ansicht des Gerichts nichts entnehmen, wie und dass eine rechtzeitige Erfüllung dieser Pflichten durch die Beklagten den Eintritt der behaupteten Schäden des Klägers verhindert hätte bzw. hätte verhindert werden können (ebenso OLG Dresden aaO; OLG Hamm aaO).

f.

Der Beklagten fällt kein Verstoß gegen Art. 15 DSGVO zur Last, da dem Kläger eine Auskunft über seine von der Beklagten verarbeiteten personenbezogenen Daten mit Schreiben vom 15.01.2024 erteilt wurde.

Eine vollständige Erteilung der Auskunft nach Art. 15 DSGVO liegt dann vor, wenn die Angaben in dem Auskunftsschreiben nach dem Willen des Schuldners die Auskunft im gesamten geschuldeten Umfang darstellen sollen. Liegt die – gegebenenfalls konkludente – Erklärung des Schuldners über die Vollständigkeit seiner Auskunft vor, kann auch der Verdacht der Unvollständig- oder Unrichtigkeit der erteilten Auskunft keinen weitergehenden Anspruch begründen (vgl. BGH, Urteil vom 03.09.2020 - III ZR 136/18).

Entscheidend ist damit, dass die erteilte Auskunft vom 15.01.2024 erkennbar den (berechtigten) Auskunftsanspruch des Klägers inhaltlich vollständig beantworten soll (so auch OLG Dresden, Urteil vom 05.12.2023 – 4 U 709/23). Dies ist mit dem fraglichen Antwortschreiben geschehen. Ein darüber hinaus gehender Auskunftsanspruch steht dem Kläger nicht zu (ebenda).

3.

Dem Kläger ist nach Auffassung des Einzelrichters ein immaterieller Schaden in Höhe von 300,00 EUR gemäß Art. 82 Abs. 1 DSGVO entstanden und hat diesen auch hinreichend nachgewiesen (vgl. EuGH, Urteil vom 14.12.2023, C-456/22, Rdnr. 21, juris).

a.

Der Kläger erlitt nach Ansicht des Einzelrichters einen immateriellen Schaden in Form der Angst aufgrund der Veröffentlichung seiner während des „Scraping-Vorfalls“ abgegriffenen Daten im Darknet. Dies steht zur Überzeugung des Einzelrichters aufgrund der informatorischen Anhörung des Klägers in der mündlichen Verhandlung vom 10.01.2024 fest.

aa.
Der Begriff des Schadens soll nach dem Erwägungsgrund 146 S. 3 DSGVO „im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht.“.

Soweit das OLG Dresden in seinem Urteil vom 05.12.2023 – 4 U 709/23 ausführt, dass vorliegend bloße negative Gefühle wie Angst keinen Schadensersatzanspruch rechtfertigen können, kann dem nach dem zeitlich nach der Entscheidung des OLG Dresden ergangenen Urteil des EuGHs vom 14.12.2023 – C-340/21 nicht mehr gefolgt werden. Allein der Umstand, dass eine betroffene Person infolge eines Verstoßes gegen die DSGVO befürchtet, dass ihre personenbezogenen Daten durch missbräuchlich verwendet werden könnten, kann einen immateriellen Schaden i.S.d. Art. 82 Abs. 1 DSGVO darstellen (EuGH, Urteil vom 14.12.2023 – C-340/21). Das Gericht muss in diesem Falle prüfen, ob diese Befürchtung unter den gegebenen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann (ebenda). Erforderlich ist hierfür, dass der Betroffene Umstände darlegt, in denen sich seine erlebten Empfindungen widerspiegeln, und dass nach der Lebenserfahrung der Datenschutzverstoß mit seinen Folgen Einfluss auf das subjektive Empfinden hat (OLG Hamm, aaO).

An die Darlegung dieses Schadens dürfen dabei keine überhöhten Anforderungen gestellt werden (vgl. Dickmann r + s 2018, 345 (353)). Jedenfalls müssen die von der Klagepartei vorgetragenen Ängste und Sorgen einen – irgendwie gearteten – Einfluss auf die Lebensführung des Betroffenen habe, sodass ein konkreter Rückschluss von äußeren Umständen auf die innere Gefühlswelt des Klägers möglich ist (so auch: OLG Dresden, Urteil vom 05.12.2023 – 4 U 709/23).

bb.
Der Kläger hat infolge der Veröffentlichung seiner im Rahmen des „Scraping-Vorfalls“ abgegriffenen Daten im Darknet einen nach Art. 82 Abs. 1 DSGVO sanktionsfähigen Zustand der Angst und Besorgnis erlitten.

Der Kläger gab im Rahmen seiner informatorischen Befragung an, dass er sich Sorgen dar-

um gemacht habe, was mit seinen Daten nach deren Veröffentlichung passiere. Insbesondere könne er nicht abschätzen, wer seine Mobilfunknummer habe und was damit in krimineller Absicht geschehen könne. Die Ungewissheit bezüglich seiner Telefonnummer belaste ihn umso mehr vor dem Hintergrund, dass er seine Handynummer seit 13 Jahre habe und mit deren Herausgabe sparsam umgegangen sei. Wegen des Vorfalls werde seine Telefonnummer nun wechseln und habe sich auch deswegen von Facebook abgemeldet.

Nach Ansicht des Einzelrichters sind die Schilderungen des Klägers glaubhaft. Er legt ohne Belastungseifer gegenüber der Beklagten inhaltlich nachvollziehbar seine eigenen Erfahrungen und inneren Gedanken und Gefühle dar. Er beschränkt sich insbesondere nicht darauf, lediglich den Vortrag aus der Klageschrift zu wiederholen. Sein Vortrag gestaltete sich bildhaft, ohne inhaltliche Widersprüche und war von Detailreichtum geprägt.

cc.

Der Kläger beschreibt für das Gericht nachvollziehbar und plausibel, dass, warum und in welchem Umfang er unter Sorgen und Ängsten hinsichtlich der Veröffentlichung seiner im Wege des „Scraping-Vorfalls“ bei der Beklagten abgegriffenen Daten leidet. Das Gericht erachtet diese Ängste auch als hinreichend begründet im Sinne des Urteils des EuGHs vom 14.12.2023 – C-340/21. Der Umstand, dass eine Person, deren Daten in einem Datensatz im Darknet veröffentlicht wird, dessen Missbrauchszweck sich geradezu aufdrängt, deswegen Angst vor betrügerischen Aktivitäten hat, ist für das Gericht ohne Weiteres nachvollziehbar. Die von dem OLG Dresden geforderte Einschränkung der Lebensführung aufgrund dieser Angst ist einerseits in der begründeten Skepsis des Klägers vor missbräuchlichen Absichten eingehender Benachrichtigungen auf seinem Telefon und der ungewissen Verwendung seiner Telefonnummer durch Dritte zu sehen. Das Mobiltelefon inklusiver der damit verwendeten Nummer wird zunehmend als Werkzeug zur Behandlung und Verarbeitung hochsensibler persönlicher, finanzieller und medizinischer Daten verwendet, sodass seiner Sicherheit und Integrität eine große Bedeutung zu kommen. Weiter stellt sich im Fall des Klägers die Beeinträchtigung seiner Lebensführung auch vor dem Hintergrund des Wechsels seiner langjährig genutzten Telefonnummer und der Abmeldung von Facebook dar.

dd.

Darüber hinaus sieht Art. 82 DSGVO eine etwaige Bagatellgrenze nicht vor (EuGH, Urteil vom 04.05.2023 – C-300/21; EUGH, Urteil vom 14.12.2023, C-456/22, Rdnr. 16 f., juris).

ee.

Die vom Kläger beschriebenen Anstrengungen im Wege der Nachverfolgung des Datenschutzvorfalles rechtfertigen nach Ansicht der Kammer keine schadensersatzrechtliche Sanktionierung der Beklagten (so auch: OLG Hamm, aaO).

ff.

Auch der vom Kläger behauptete Kontrollverlust rechtfertigt keinen Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO (so auch OLG Dresden, aaO; OLG Hamm, aaO; OLG Köln aaO und OLG Stuttgart, aaO). Insbesondere ist es dem Kläger nicht gelungen hinreichend substantiiert zu dem Kausalzusammenhang zwischen dem von ihm beschriebenen Benachrichtigungen, die das Ausmaß des Kontrollverlustes darstellen sollen, und dem streitgegenständlichen „Scraping-Vorfall“ vorzutragen (vgl. OLG Dresden, aaO). Es ist gerichtsbekannt, dass auch Personen, die nicht auf der Facebook-Plattform angemeldet waren, die von dem Kläger beschriebenen Benachrichtigungen erhalten. Weshalb diese dann trotz dessen auf den streitigen Vorfall zurückzuführen sein sollen, ergibt sich aus dem klägerischen Vortrag nicht.

c.

Die vom Kläger erlittene Angst aufgrund der Veröffentlichung seiner im Rahmen des „Scraping“ abgegriffenen persönlichen Daten ist kausal auf die oben festgestellten Verletzungen der DSGVO durch die Beklagten zurückzuführen.

Die Verstöße gegen die DSGVO durch die Beklagte können nicht hinweg gedacht werden, ohne dass der Schaden des Klägers entfiele. Erst durch diese Verstöße war es den unbekannten Scrapern möglich, personenbezogene Daten des Klägers abzugreifen und letztlich zu veröffentlichen.

d.

Der vom Kläger erlittene immaterielle Schaden war vorliegend auf 300,00 EUR zu bemessen.

Diese Summe erachtet des Gerichts im Rahmen des von ihm ausgeübten Ermessens nach § 287 Abs. 1 ZPO (vgl. BAG NJW 2022, 2779) als ausreichend aber auch angemessen, um einen vollständigen Schadensausgleich vorzunehmen (vgl. EuGH, Urteil vom 21.12.2023, C-667/21, Rdnr. 102, juris).

Bei der Bemessungshöhe des immateriellen Schadensersatzes nach Art. 82 Abs. 1 DSGVO können dabei die Grundlagen des Art. 83 Abs. 2 DSGVO herangezogen werden. Demnach sind u.a. Art und Dauer des Verstoßes und die Kategorien personenbezogener Daten, die von

dem Verstoß betroffen sind, zu berücksichtigen.

Unter Berücksichtigung der Artikel 83 und 84 DSGVO muss weiter beachtet werden, dass dem Schadenersatzanspruch keine abschreckende Wirkung gegenüber dem Verantwortlichen zukommen soll. Dem Schadensersatzanspruch soll dabei insbesondere kein Straf- bzw. Sanktionscharakter zukommen (EuGH, Urteil vom 21.12.2023, C-667/21, Rdnr. 85 f., juris). Auch auf den Grad des Verschuldens der Beklagten kommt es demnach bei der Bemessung der Höhe des als Entschädigung für einen immateriellen Schaden auf der Grundlage dieser Bestimmung gewährten Schadenersatzes nicht an.

Letztlich sind auch die konkreten Umstände des maßgeblichen Einzelfalls zu berücksichtigen.

Von dem Kläger sind zumindest Vorname, Geschlecht und Facebook-ID abgegriffen worden. Zudem ist im Rahmen der durch den „Scraping-Vorfall“ abgegriffenen Daten des Klägers auch dessen Mobilfunknummer zu berücksichtigen. Unabhängig davon, wie die Telefonnummer von den Scrapern generiert oder diesen zur Kenntnis gelangt ist, fand erst durch die Verbindung des Facebook-Profils mit ebendieser Nummer mittels des CIT eine individualisierte Zuordnung zu den Daten des Klägers statt, die vorher schlicht qualitativ nicht vorhanden war.

Anspruchsmindernd war – entgegen der Ansicht der Beklagten – nicht zu bewerten, dass es sich bei einem Teil der abgegriffenen Daten um sogenannte „stets öffentliche“ Daten auf dem klägerischen Facebook-Profil handelte. Erst durch die Verknüpfung der Telefonnummer mit dem Facebook-Profil mittels des CIT kamen die stets öffentlichen Daten den Scrapern zur Kenntnis. Es ist nach Auffassung des Einzelrichters abwegig, dass die Scraper ohne automatisiertes Auffinden von Facebook-Profilen an die öffentlichen Informationen des Klägers gelangt wären. Die Möglichkeit des massenhaften, ja millionenfachen Ausfindigmachens von Profilen, dem somit verbundenen Abgreifen der dort befindlichen Daten und dem letztlich damit verbundenen Kontrollverlust des Klägers über diese Daten ermöglichte die Beklagte erst durch ihre Verstöße gegen die DSGVO (s.o.). Dies kann nicht zu Lasten des Klägers gehen.

Eine besonders hohe persönliche Betroffenheit des Klägers vermag der Einzelrichter dennoch nicht festzustellen. Dabei war auch zu berücksichtigen, dass dem Kläger bisher kein vermögensrechtlicher Nachteil entstanden ist.

cc.

Dabei kann dahinstehen, ob ein Mitverschulden anspruchsmindernd zu berücksichtigen wäre (dagegen: Kühling/Buchner/*Bergt,* DS-GVO 3. Aufl., Art. 82 Rn. 59), denn dem Kläger fällt ein solches Verschulden nach Ansicht des Einzelrichters nicht zur Last.

Insoweit muss zwischen einem rechtmäßigen Datenabgleich zwischen Nutzern der Facebook-Plattform und dem unbefugten Scraping durch Dritte unterschieden werden. Allein daraus, dass ein Nutzer durch seine unveränderten standardmäßigen Datenschutzeinstellungen die Möglichkeit eines Abgreifens seiner Daten durch das CIT mittels „Scraping“ eröffnet, erklärt er damit nicht zugleich, dass diese Daten für rechtswidrige Zwecke abgegriffen werden dürfen. Dies würde das angemessene Maß von Eigenverantwortung des Nutzers unverhältnismäßig auf ihn überlagern. Dies gilt zwingend umso mehr vor dem Hintergrund, dass der Beklagten vorliegend ein Verstoß gegen den Grundsatz „privacy by default“ zur Last fällt (s.o.).

e.
Der Beklagten gelingt es nicht, sich nach Art. 82 Abs. 3 DSGVO im Hinblick auf den streitgegenständlichen Datenschutzvorfall und den damit einhergehenden Verstößen gegen die DS-GVO zu entlasten.

Eine Entlastung des Verantwortlichen nach Art. 82 Abs. 3 DSVO gelingt nur, wenn dieser nachweist, dass er in keiner Hinsicht den schadensbegründenden Umstand verschuldet hat, was grundsätzlich vermutet wird (BeckOK DatenschutzR/*Quaas,* DS-GVO Stand 01.08.2022, Art. 82 Rn. 17).

Die Beklagte kann diese Vermutung vorliegend nicht widerlegen, da sie nicht nachweisen konnte, dass sie kein Verschulden trifft.

4.
Der Zinsanspruch folgt aus §§ 288, 291 BGB, § 187 Abs. 1 BGB analog. Die Zustellung der Klageschrift erfolgte am 22.08.2023 (Bl. 52 d.A.).

IV.

Der klägerische Antrag zu 4) ist ebenso unbegründet, wie der klägerische Antrag zu 5).

1.
Einen grundsätzlich bestehenden Anspruch nach Art. 15 DSGVO des Klägers gegen die Be-

klagte hat diese mit Schreiben vom 15.01.2024 (Anlage B 20) nach Ansicht des Einzelrichters nach § 362 BGB erfüllt.

Mit ebendiesem Schreiben hat die Beklagte gegenüber dem Kläger kenntlich gemacht, dass sie davon ausgeht, dass diese Antwort abschließend ist (s.o.). Einen weiteren, über die erteilte Antwort hinausgehenden, Auskunftsanspruch steht dem Kläger nicht zu.

2.
Weiter steht dem Kläger der mit dem Antrag zu 5) geltend gemachte Anspruch auf Ersatz vorgerichtlicher Rechtsanwaltskosten nicht zu.

a.
Zu den ersatzpflichtigen Aufwendungen des Geschädigten zählen grundsätzlich auch die durch das Schadensereignis erforderlich gewordenen Rechtsverfolgungskosten.

Dabei ist zu klären, ob die Gebühr aus Nr. 2300 RVG VV überhaupt ausgelöst worden ist. Ob eine vorprozessuale anwaltliche Zahlungsaufforderung eine Geschäftsgebühr nach Nr. 2300 RVG VV auslöst oder als der Vorbereitung der Klage dienende Tätigkeit nach § 19 Abs. 1 Satz 2 Nr. 1 RVG zum Rechtszug gehört und daher mit der Verfahrensgebühr nach Nr. 3100 RVG VV abgegolten ist, ist eine Frage der Art und des Umfangs des im Einzelfall erteilten Mandats. Erteilt der Mandant den unbedingten Auftrag, im gerichtlichen Verfahren tätig zu werden (vgl. Vorbemerkung zu § 3 I 1 RVG VV), lösen bereits Vorbereitungshandlungen die Gebühren für das gerichtliche Verfahren aus, und zwar auch dann, wenn der Anwalt zunächst nur außergerichtlich tätig wird. Für das Entstehen der Geschäftsgebühr nach Nr. 2300 RVG VV ist dann kein Raum mehr.

Nach alldem besteht ein Anspruch auf Erstattung der Rechtsanwaltskosten nicht.

b.
Aus der Anlage K 1 ergibt sich, dass die erste unmittelbare Kontaktaufnahme mit der Geltendmachung von Unterlassungs-, Schadenersatz- und Auskunftsansprüchen direkt durch die Prozessbevollmächtigten des Klägers erfolgte, weshalb sich die Beklagte zu diesem Zeitpunkt noch nicht im Verzug befunden hat, also nicht auf die §§ 286 ff. BGB abgestellt werden kann.

c.
Der Kläger hat bezüglich der vorgerichtlichen Anwaltskosten lediglich auf die Anlage K 1 Be-

zug genommen, mit der sein Prozessvertreter entsprechende Ansprüche geltend gemacht hat, jedoch inhaltlich keinen weitergehenden Vortrag zu den oben dargestellten Anspruchsvoraussetzungen gehalten.

Die Anlage K 1 vom 21.04.2023 enthält zwar noch keine unmittelbare Ankündigung, dass nach Ablauf der bis zum 21.05.2023 gesetzten Frist Klage erhoben wird, die Vollmacht, die der Kläger bereits am 07.01.2023 unterzeichnet hat, erstreckt sich aber ausdrücklich bereits auf eine Prozessführung, weshalb das Mandat unbedingt und umfassend erteilt war und nach den oben dargestellten Grundsätzen die Mail als zur Vorbereitung der Klage dienende Tätigkeit nach § 19 Abs. 1 Satz 2 Nr. 1 RVG zum Rechtszug gehört und daher mit der Verfahrensgebühr nach Nr. 3100 RVG VV abgegolten ist (OLG Stuttgart, aaO).

C.

Die Kostenentscheidung beruht auf § 92 Abs. 2 Nr. 1 ZPO, die Entscheidung über die vorläufige Vollstreckbarkeit auf §§ 708 Nr. 11, 711 ZPO.

Die Streitwertentscheidung beruht auf § 48 GKG i.V.m. §§ 3, 4, 5 ZPO.

Dabei wurde der Antrag zu 1) mit 1.000,00 EUR, der Antrag zu 2) mit 500,00 EUR, der Antrag zu 3) mit 3.500,00 EUR und der Antrag zu 4) mit 500,00 EUR bemessen (vgl. dazu OLG Dresden, Beschluss vom 31.07.2023 – 4 W 396/23).

Richter