bgl. Abs.

Landgericht Halle

Geschäfts-Nr.:

4 O 254/23

Verkündet am:28.02.2024

Gez. , JHS´in

als Urkundsbeamtin/beamter der Geschäftsstelle

Im Namen des Volkes!

Urteil

In dem Rechtsstreit

,

Klägerin,

Prozessbevollmächtigte:
Wilde Beuger Solmecke Rechtsanwälte Partnerschaft mbB,
vertreten durch die Rechtsanwälte Chahal und Gartner,
Eupener Straße 67, 50933 Köln,

gegen

Meta Platforms Ireland Ltd.,
vertreten durch den Director,
Merrion Road,
Dublin 4,
D04 X2K5,
Irland,

Beklagte,

Prozessbevollmächtigte:
Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB,

vertreten durch die Rechtsanwälte Dr. Mekat, Bilgenroth und Meyer,
Bockenheimer Anlage 44, 60322 Frankfurt/Main,

hat die 4. Zivilkammer des Landgerichts Halle auf die mündliche Verhandlung vom 9. Februar 2023 durch den Richter als Einzelrichter

für **R e c h t** erkannt:

1.) Die Beklagte wird verurteilt, an die Klägerin 400,00 Euro nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 1. November 2023 zu zahlen.

2.) Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerin alle zukünftigen Schäden zu ersetzen, die dieser durch die seitens der Beklagten erfolgte Verknüpfung ihrer personenbezogenen Daten beim Abschöpfen von Daten durch Dritte im Jahre 2019 noch entstehen werden.

3.) Im Übrigen wird die Klage abgewiesen.

4.) Die Kosten des Rechtsstreits tragen die Klägerin zu 3/5 und die Beklagte zu 2/5.

5.) Das Urteil ist vorläufig vollstreckbar. Die Beklagte kann die Vollstreckung gegen Sicherheitsleistung in Höhe von 120 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Klägerin vor der Vollstreckung Sicherheit in Höhe von 120 % des jeweils zu vollstreckenden Betrags leistet. Die Klägerin kann die Vollstreckung gegen Sicherheitsleistung in Höhe von 120 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 120 % des jeweils zu vollstreckenden Betrags leistet.

Und beschlossen:

Der Gegenstandswert für die Gerichtsgebühren des Rechtsstreits wird auf die Stufe bis 4.000 Euro festgesetzt.

****

Tatbestand

Die Klägerin nimmt die Beklagte wegen vermeintlicher Verstöße gegen die DSGVO in Anspruch.

Die Beklagte betreibt das soziale Netzwerk "Facebook", welches es Nutzern nach Registrierung ermöglicht, mit anderen Nutzern in Kontakt zu treten, Nachrichten zu versenden und persönliche Informationen zu teilen. Damit Nutzer sich leichter mit anderen Nutzern vernetzen und ihrerseits über eine Suchmaske aufgefunden werden können, müssen folgende Datenpunkte zwingend öffentlich angegeben werden: Vor- und Nachname, Geburtstag, Geschlecht. Die Angabe einer Telefonnummer ist optional.

Nach der erstmaligen Registrierung erhalten Nutzer ein persönliches Profil, auf dem sie weitere Angaben zu ihrer Person tätigen und im von der Beklagten vorgegebenen Rahmen darüber befinden können, welche anderen Nutzer ihre Daten einsehen bzw. abrufen können. So stellt die Beklagte Anwendungen zur Verfügung, die Nutzern eine Konfiguration ihrer sog. Privatsphäre-Einstellungen und damit auch ihrer Auffindbarkeit über die Suchmaske oder andere Suchanwendungen ermöglicht. Innerhalb der Privatsphäre-Einstellungen zur Suchbarkeit wird zwischen verschiedenen Möglichkeiten differenziert, welche von der privatesten Einstellung, der Abrufbarkeit der Daten nur für den Nutzer selbst ("Nur ich"), bis hin zur Abrufbarkeit für sämtliche Personen reicht, die als Nutzer registriert sind ("Alle").

Die Klägerin meldete sich im März 2008 auf der von der Beklagten betriebenen Plattform an und gab dieser gegenüber bei Anmeldung auch ihre Mobilfunknummer preis. Die standardmäßige Konfiguration zur Suchbarkeit ihres Profils unter Eingabe der Telefonnummer war auf "Alle" festgelegt, ermöglichte es also sämtlichen Nutzern das klägerische Profil jedenfalls mit den dort zwingend öffentlich einsehbaren Datenpunkten nebst der Nutzerkennung aufzufinden.

Im Jahre 2019 kam es auf der Plattform der Beklagten zu einem breit angelegten, automatisierten Abschöpfen von Millionen von Nutzerdaten durch unbekannte Dritte, von denen auch die Klägerin mit seinen Datenpunkten Vor- und Nachname, Nutzername und Geschlecht betroffen war (sog. Scraping-Vorfall). Scraping ist eine der Beklagten jedenfalls bereits seit April 2018 bekannt gewesene, informationstechnische Methode, mithilfe derer typischerweise öffentlich einsehbare Daten von Internetseiten durch automatisierte Software massenhaft abgerufen werden. Die Methode bedient sich dabei

in der Regel Anwendungen, die für eine ordnungsgemäße Nutzung der Internetseite entworfen worden sind.

Im hiesigen Fall erfolgte der Datenabruf unter Verwendung des sog. Contact-Import-Tool (im Folgenden: CIT). Hierbei handelte es sich um eine Anwendung der Beklagten, die es an sich Nutzern ermöglichen sollte, im digitalen Adressbuch des Nutzergeräts vorhandene Kontakte mit den bereits vernetzten virtuellen Kontakten auf Facebook abzugleichen und gegebenenfalls weitere, noch nicht vernetzte Kontakte aufzufinden. Nach Eingabe einer Mobilfunktelefonnummer prüfte die Beklagte automatisiert, ob zu dieser ein Facebook-Profil bestand und stellte im Falle dessen die Verknüpfung zum jeweiligen Profil her, indem es der suchenden Person das Profil mit den öffentlich verfügbaren Daten als zur Telefonnummer gehörig anzeigte. Der Abruf der Daten erfolgte im Wege einer randomisierten Eingabe einer Vielzahl an möglichen Zahlenkombinationen zu Telefonnummern, wobei die Beklagte bei Übereinstimmung einer Telefonnummer entsprechend der obigen Verfahrensweise das dazugehörige Profil angab. Durch dieses Vorgehen gelang es unbekannten Dritten die zwingend öffentlich einsehbaren Daten der Klägerin als um deren Nummer erweitertes Datenbündel für andere Zwecke zu speichern.

Im April 2021 veröffentlichten Unbekannte das Datenbündel der Klägerin im Internet in einer vor dem Zugriff durch Dritte ungesicherten Datenbank. Erst nach Medienberichten (Business Insider, 3. April 2021, abrufbar unter https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leakedonline-2021-4?r=US&IR=T) über den Vorfall veröffentlichte die Beklagte am 6. April 2021 Einträge auf ihrer Website, wo sie zu dem Scraping-Vorfall Stellung bezog. Dabei gab sie zu erkennen, dass sie bereits Ende 2019 vom Scraping-Vorfall Kenntnis erlangt hatte. Eine Information der irischen Datenschutzaufsichtsbehörde DPC oder der Klägerin selbst erfolgte im Nachgang zur Kenntniserlangung nicht.

Mit anwaltlichem Schreiben 7. April 2023 forderte die Klägerin die Beklagte zur Auskunft über die Verarbeitung der klägerischen Daten im Zusammenhang mit dem Scraping-Vorfall auf. Wegen des konkreten Inhalts des Auskunftsersuchens wird auf die Anlage K1 Bezug genommen. Mit Schreiben vom 8. Mai 2023 erteilte die Beklagte der Klägerin hierauf konkrete Informationen, derentwegen auf die Anlage B16 Bezug genommen wird.

Die Klägerin beantragt,

1. die Beklagte zu verurteilen, 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 Euro nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

2. festzustellen, 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 zu verurteilen, 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. personenbezogene Daten der Klagepartei, namentlich Telefonnummer, Facebook-ID, Familienname, Vorname, Geschlecht, Bundesland, Land, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontaktdaten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahamen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf "privat" noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.

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

Die Beklagte beantragt,

die Klage abzuweisen.

Die Klage ist der Beklagten am 31. Oktober 2023 zugestellt worden

Entscheidungsgründe

A. Die Klage ist mit Ausnahme des Antrags zu 3.a zulässig, hat in der Sache indes nicht vollumfänglich Erfolg.

I. Der Klageantrag zu 1) ist lediglich teilweise begründet, da der dem Grunde nach bestehende Anspruch auf Ersatz immaterieller Schäden den klägerseits geforderten Mindestbetrag in der Höhe nicht erreicht.

1. Der Klägerin steht gegen die Beklagte ein Anspruch gem. Art. 82 Abs. 1 DSGVO zu, da diese schuldhaft die Anforderungen an die rechtmäßige Datenverarbeitung im Sinne von Art. 6 Abs. 1 S.1 DSGVO nicht eingehalten hat. Insbesondere war die Verarbeitung der klägerischen Daten entgegen der Auffassung der Beklagten nicht gem. § 6 Abs. 1 S.1 lit. b) DSGVO rechtmäßig. Die Datenverarbeitung setzt in Erfüllung eines Vertrags notwendigerweise zu ihrer Rechtmäßigkeit voraus, dass technisch ausreichende und nach dem Gesetz geschuldete Sicherheitsmaßnahmen vorgehalten werden, um wie das Zugänglichmachen personenbezogener Daten zu gegenüber Unbefugten verhindern. Diesen Anforderungen hat die Beklagte jedoch nicht genügt, da sie bei der Datenverarbeitung gegen Art. 24, 25 Abs. 1, 32 Abs. 1 Hs. 1, Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f) DSGVO verstoßen hat.

a) Eine Verarbeitung personenbezogener Daten der Klägerin gem. § 4 Nr. 1, 2 DSGVO ist dadurch erfolgt, dass die Beklagte im Rahmen des Scraping-Sachverhalts die im CIT eingegebene Telefonnummer mit den bei ihr bereits gespeicherten Daten zum Namen, Nutzernamen sowie Geschlecht abgeglichen und schlüssig verknüpft hat. Denn nach der

Funktionsweise des CIT genügte die Eingabe einer mit einem Konto verknüpften Telefonnummer, um die Beklagte zu veranlassen, das dazugehörige Konto im öffentlich einsehbaren Umfang mitzuteilen und damit zugleich konkludent die Existenz und die Zugehörigkeit der Mobilfunknummer zum mitgeteilten Profil zu bestätigen.

b) Das Gericht geht davon aus, dass die Daten nicht in einer dem Grundsatz der Integrität und Vertraulichkeit genügenden Weise verarbeitet worden sind.

aa) Gem. Art. 32 Abs. 1 Hs. 1 DSGVO hat der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zugleich finden nach Art. 32 Abs. 2 DSGVO insbesondere die Risiken Berücksichtigung, die mit der Verarbeitung verbunden sind. Namentlich betrifft dies unter anderem die unbefugte Offenlegung von beziehungsweise den unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden.

bb) In Anwendung des vorstehenden Maßstabs hat die gem. Art. 5 Abs. 2 DSGVO darlegungsbelastete (vgl. EuGH, Urteil vom 14. Dezember 2023 – C-340/21 –, Rn. 52, juris) Beklagte nicht hinreichend dargetan, dass sie ihrer Verpflichtung zur Gewährleistung eines angemessenen Schutzniveaus bei der Datenverarbeitung in zureichendem Umfang nachgekommen ist.

(1) Zur Beurteilung des erforderlichen Schutzniveaus ist zunächst hinsichtlich der Gefährdungslage zu berücksichtigen, dass zum damaligen Zeitpunkt sowohl die hier relevante Scraping-Methode zum missbräuchlichen Abschöpfen von Daten bereits bekannt war, wie auch gängige technische Gegenmaßnahmen z.B. durch Sicherheitscaptchas, die der verarbeitenden Software eine Differenzierung zwischen menschlicher und computergesteuerter Abfrage erlauben, zur Verfügung standen.

Weiterhin sind die Risiken des Eintritts von materiellen und immateriellen Schäden, die sich aus der Möglichkeit der Zuordnung von Telefonnummern zum Plattform-Profil und den öffentlich einsehbaren Daten gerade bei massenhaftem Auslesen und ggf. auch automatisierter missbräuchlicher Folgenutzung ergeben, nicht von geringer Erheblichkeit. Nimmt man nämlich in den Blick, dass einerseits mit der fortschreitenden

Digitalisierung für die Identifikation des Vertragspartners im Massengeschäftsverkehr mittlerweile häufig auf die sog. 2-Faktor-Authentifizierung unter Zuhilfenahme der Mobilfunknummer zurückgegriffen wird (z.B. SMS-TAN-Verfahren im Online-Zahlungsverkehr) und andererseits die Möglichkeit besteht, ohne wesentliche Schwierigkeiten die Telefonnummer durch den Mobilfunkanbieter auf eine neue SIM-Karte überschreiben zu lassen (sog. SIM-Swapping), so lässt sich erkennen, dass das Risiko der missbräuchlichen Ausnutzung beträchtlich ist. Dass bei isolierter Betrachtung bestimmte Profildaten der Klägerin öffentlich waren, ist dagegen insoweit unerheblich (a.A. LG Halle, Urteil vom 7. Dezember 2022, – 6 O 195/22). Denn gerade die durch die Beklagte vorgenommene Verknüpfung der zwar für alle Nutzer suchbaren, jedoch nicht öffentlich einsehbaren Telefonnummer zu einem erweiterten Datenbündel, begründet Risiken von eigenständigen Gewicht (LG Halle, Urteil vom 28. April 2023 – 4 O 250/22). Den damit einhergehenden Verpflichtungen zum Schutz der informationellen Selbstbestimmung hat die Beklagte als Betreiberin eines sozialen Netzwerks, das zur gesellschaftlich-kommunikativen Teilhabe eine dominante Position einnimmt, und der daraus folgenden Annährung an eine Grundrechtsbindung in besonderem Maße Rechnung zu tragen (vgl. BGH, Beschluss vom 23. Juni 2020 – KVR 69/19 –, Rn. 105, juris).

Bei Ansatz des Schutzniveaus hat das Gericht allerdings auch in die Beurteilung eingestellt, dass Art. 32 Abs. 1 DSGVO keine absolute Obergrenze eines Schutzes verpflichtend normiert, sondern im jeweiligen Verarbeitungskontext lediglich angemessen sein muss. Dies ist hier zum einen insoweit von Bedeutung, als dass die Bereitstellung bestimmter Nutzeranwendungen wie des CIT der angebotenen Dienstleistung zur Vernetzung mit anderen Personen zugutekommt und damit eine Abschaltung der Anwendung in der Abwägung mit den oben genannten Risiken einseitig zulasten der Nutzbarkeit der von der Beklagten angebotenen Dienstleistungen ginge. Da es sich beim CIT jedoch um eine optionale Anwendung handelt, die die Kontaktsuche vereinfachen soll, aber nicht zwingend voraussetzt, fällt der Gesichtspunkt der vereinfachten Nutzbarkeit im Übrigen jedoch nur in geringem Maße ins Gewicht. Zum anderen kommt der Angemessenheit des Schutzniveaus dahingehend eine Bedeutung zu, als eine missbräuchliche Verwendung von informationstechnischen Anwendungen mit vollendeter Sicherheit nie ausgeschlossen werden kann. Die Gefährdung der Daten des Einzelnen nimmt bei wirtschaftlicher Betrachtung daher vor allem dort streiterhebliche Form an, wo nicht nur aufgrund einer einzelnen Abfrage Daten verknüpft werden, sondern

die Verknüpfung in einer Masse stattfindet, die auch für böswillige Dritte einen Nutzen generiert (vgl. LG Halle, Urteil vom 28. April 2023 – 4 O 250/22; vgl. auch Erwägungsgrund 75 a.E. der DSGVO).

(b) Soweit die Beklagte vorträgt, sie habe im relevanten Zeitraum Sicherheitscaptchas, Bot-Erkennungen und Übertragungsbeschränkungen eingesetzt, hat sie nicht hinreichend dargelegt, inwiefern die Maßnahmen auch Anwendung fanden, um nicht erkannte, automatisierte sowie umfangreiche Datenabfragen zu verhindern. Dies wäre jedoch gemessen am Ausmaß der durch das Scraping drohenden Gefahren geboten gewesen (so auch die Irische Datenschutzaufsichtsbehörde DPC, Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018 and Article 60 of the General Data Protection Regulation, S. 44 ff.). Es kann in diesem Sinne zugunsten der Beklagten unterstellt werden, dass sie die beschriebenen Sicherheitsmaßnahmen zumindest dann einsetzte, wenn zuvor Abfrageaktivitäten festgestellt worden sind, die wahrscheinlich auf unauthentischem Verhalten beruhten. Wie die Beklagte allerdings selbst vorträgt, beruht Scraping gerade auf einer missbräuchlichen Nutzungsweise von normalen Funktionen, im Rahmen derer das verarbeitende System im Einzelfall den Missbrauch nicht von einer ordnungsgemäßen Nutzung zu unterscheiden vermag. Gerade daher war die Beklagte hier gehalten, verhältnismäßig leichte Einschränkungen im Nutzererlebnis zu implementieren, die wegen des nicht fernliegenden Ausfalls der Missbrauchserkennung ein umfangreiches Abschöpfen von Daten effektiv verhinderten.

Die einzige präventiv-effektive Gegenmaßnahme im Einzelfall, die dem Vortrag der Beklagten hierzu für den relevanten Zeitraum konkret zu entnehmen ist, ist die Durchführung von Captcha-Abfragen vor der Verarbeitung. Selbst wenn man aber beispielsweise eine Captcha-Abfrage für jeden Fall der Suche einer Telefonnummer für unangemessen hielte, ist nicht einzusehen, warum die Beklagte nicht zumindest in regelmäßigen Abständen billigerweise eine solche hätte vorsehen müssen, um jedenfalls den massenhaften Datenabruf zu verhindern und so für böswillige Dritte unattraktiv zu gestalten. Captcha-Abfragen in einem bestimmten, regelmäßigen Umfang oder zumindest gleich geeignete Maßnahmen für den relevanten Zeitraum sind dem Vortrag der Beklagten aber nicht zu entnehmen.

Soweit die Beklagte darüber hinaus zu ihrer Reaktion auf den "Scraping-Vorfall" und die infolgedessen entwickelten Gegenmaßnahmen vorgetragen hat, kommt es hier darauf

nicht an, da maßgeblicher Beurteilungszeitpunkt das Schutzniveau im Zeitpunkt der rechtswidrigen Verarbeitung ist.

Schließlich führt der Vortrag der Beklagten, "im Nachgang" zu Scraping-Vorfällen im Jahre 2018 im CIT weitere Schutzmechanismen in Form des sog. Social-Connection-Checks oder der sog. PMYK-Funktion zu keinem anderen Ergebnis. Mangels zeitlicher Konkretisierung ist der Vortrag nicht geeignet, eine Prüfung dahingehend zuzulassen, ob die genannten Maßnahmen auch im hier relevanten Zeitraum zwischen 2019 und 2021 ein angemessenes Schutzniveau gewährleistet haben. Es kann daher dahinstehen, ob die Beklagte mit den Maßnahmen in der Sache ihrer Verpflichtung aus Art. 32 DSGVO zu Genüge nachgekommen ist.

2. Die Höhe des ersatzfähigen, durch die Verstöße verursachten immateriellen Schadens beläuft sich hier auf 400 Euro.

a) Der Klägerin ist ein immaterieller Schaden entstanden, der gem. Art. 82 Abs. 1 DSGVO ersatzfähig ist.

aa) Entgegen der Auffassung der Klägerin begründet nicht schon jeder Verstoß gegen die DSGVO einen Schadensersatzanspruch. Vielmehr folgt bereits aus dem Wortlaut des Art. 82 Abs. 1 DSGVO und den Erwägungsgründen 75, 85 und 146 der DSGVO, dass der Schaden ein eigenständiges Tatbestandsmerkmal darstellt, der der Feststellung durch das erkennende Gericht bedarf (EuGH, Urteil vom 04.05.2023, C-300/21, Rn. 33 ff., juris). Andererseits bedingt insbesondere die gebotene weiten Auslegung des Schadensbegriffs in Art. 82 Abs. 1 DSGVO entsprechend der Ziele der DSGVO (Erwägungsgrund 146 S.3 der DSGVO), dass die Ersatzfähigkeit – anders als die Beklagte meint – nicht auf solche immateriellen Schäden beschränkt ist, die eine wie auch immer geartete Erheblichkeitsschwelle überschreiten (EuGH, Urteil vom 04.05.2023, C-300/21, Rn. 44 ff., juris). Das Gericht versteht die neuere Rechtsprechung des EuGH dahingehend, dass der Verordnungsgeber insbesondere den bloßen Verlust der Kontrolle des Betroffenen über seine eigenen Daten infolge eines Verstoßes gegen die DSGVO als ersatzfähigen Schaden erfassen wollte und zwar dies selbst dann, wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte oder andere schadensvertiefende Umstände hinzugetreten sind (EuGH, Urteil vom 14. Dezember 2023 – C-456/22 –, Rn. 22, juris; Urteil vom 14. Dezember 2023 – C-340/21 –, Rn. 82, juris). Dieser Auffassung schließt sich das Gericht an (so bereits LG Halle, Urteil vom 28. April 2023 – 4 O 250/22). Unter Berücksichtigung

der Wertung der Erwägungsgründe 75 und insbesondere 85 S.1 genügt es jedenfalls für die Annahme eines immateriellen Schadens, wenn aus einem Kontrollverlust über die eigenen personenbezogenen Daten hinreichend konkretisierte Risiken für die Rechte und Freiheiten des Betroffenen z.B. in Form eines Identitätsdiebstahls erwachsen (vgl. LG Halle, Urteil vom 28. April 2023 – 4 O 250/22). Ob darüber hinaus psychische Beeinträchtigungen, negative Gefühle oder Befürchtungen der Klägerin zum Kontrollverlust hinzugetreten sind, kann für die Annahme eines immateriellen Schadens hingegen nicht von ausschlaggebender Bedeutung sein (a.A. etwa OLG München, Beschluss vom 23. Januar 2024 – 27 U 3696/23 e; OLG Köln, Urteil vom 7. Dezember 2023 – I-15 U 33/23 –, Rn. 41, juris; OLG Stuttgart, Urteil vom 22. November 2023 – 4 U 20/23 –, Rn. 294, juris). Die Forderung nach "Spürbarkeit" oder "Objektivierbarkeit" der Beeinträchtigung würde letztlich eine – nach nationalem Verständnis des immateriellen Schadens durchaus nachvollziehbare, europarechtlich indes nicht vorgesehene (vgl. EuGH, Urteil vom 14. Dezember 2023 – C-456/22 –, Rn. 17, juris) – Erheblichkeitsschwelle durch die Hintertür einführen.

bb) Dies zugrunde gelegt, liegt ein immaterieller Schaden bei der Klägerin vor. Zwischen den Parteien ist nämlich unstreitig, dass das Datenbündel in der durch die Beklagte verknüpften Form im Jahr 2021 in einer ungesicherten Datenbank im Internet veröffentlicht wurde und dementsprechend dem ungehinderten Zugriff einer unüberblickbaren Anzahl an Dritten ausgesetzt war. Damit hat die Klägerin zur Überzeugung des Gerichts in einer ihre Freiheiten gefährdenden Art und Weise die Hoheit über ihr personenbezogenes Datenbündel verloren und folglich auch einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DSGVO erlitten.

cc) Soweit die Beklagte unter Verweis auf die obergerichtliche Rechtsprechung schließlich einwendet, dem Klagevortrag fehle es angesichts der zahlreichen inhaltsgleichen Schriftsätze in Parallelverfahren an der nötigen Individualisierung zum Verlust der Kontrolle, wird verkannt, dass der Scraping-Vorfall und die nachfolgende Veröffentlichung der Datenbank eine Vielzahl an identischen Sachverhalten verursacht hat, die einer weiteren Konkretisierung nur schwerlich zugänglich sind (vgl. hierzu auch *Hillert*, in: jurisPR-ITR 21/2023 Anm. 2). Es kann der Beklagten aber nicht zum Vorteil gereichen, dass sie nicht nur im konkreten, sondern wahrscheinlich in einer unüberschaubaren Vielzahl an identisch gelagerten Einzelfällen pflichtwidrig gehandelt hat, wenn wir hier feststellbar ist, dass konkret der Klägerin die Kontrolle über ihr Datenbündel entzogen worden ist.

b) Die Verletzung von Vorschriften über die Datenverarbeitung war ursächlich für den festgestellten Schaden. Dabei schadet es der Zurechenbarkeit von Schäden nicht per se, wenn auch Dritte – wie vorliegend – bei der Schadensentstehung mitwirken. Vielmehr genügt es, wenn die hier von der Beklagten gesetzten Verursachungsbeiträge mitursächlich waren (vgl. OLG Hamm, Urteil vom 20. Januar 2023 – I-11 U 88/22 –, Rn. 125, juris; vgl. auch EuGH, Urteil vom 5. Juni 2014 – C-557/12 –, juris) und auch in einem Adäquanzzusammenhang stehen. Bei dem Ursachenzusammenhang zwischen Haftungsgrund und dem Eintritt des geltend gemachten Schadens handelt es sich um eine Frage der haftungsausfüllenden Kausalität, weshalb das Beweismaß des § 287 Abs. 1 ZPO Anwendung findet (BGH, Urteil vom 15. Juni 2023 – III ZR 44/22 –, Rn. 14, juris; a.A. OLG Hamm, Urteil vom 15. August 2023 – I-7 U 19/23 –, Rn. 196, juris).

In Anwendung des § 287 Abs. 1 ZPO ist das Gericht davon überzeugt, dass zureichende Anhaltspunkte für einen adäquaten Kausalzusammenhang zwischen Schaden mit den vorgenannten Verstößen vorliegen. Zum einen befand sich im klägerischen Datenbündel wie auch bei einer riesigen Anzahl an anderen Datenbündeln im veröffentlichten Datensatz dessen Facebook-ID, weshalb das Gericht davon überzeugt ist, dass das veröffentlichte Datenbündel deckungsgleich mit dem im Rahmen des streitgegenständlichen Scraping-Sachverhalts erlangten Datenbündel ist. Zum anderen ist das Gericht davon überzeugt, dass der Scraping-Sachverhalt auch auf dem Verstoß der Beklagten gegen die DSGVO beruht. Der mögliche Missbrauch von Nutzeranwendungen zum massenhaften Auslesen von Daten mit der Scraping-Methode war schon damals bekannt, weshalb ohne Weiteres vorhersehbar war, dass unzureichende Schutzmaßnahmen eine latente Gefahr für die unberechtigte Datenabschöpfung bildeten. Darüber hinaus kann auch mit hinreichender Wahrscheinlichkeit davon ausgegangen werden, dass das Datenbündel des Beklagten nicht durch Scraping hätte abgerufen werden können, wenn die Beklagte die ihr aus Art. 32 DSGVO erwachsenen Verpflichtung eingehalten hätte. Denn angemessene Schutzvorkehrungen hätten mit hinreichender Wahrscheinlichkeit den Abruf der betroffenen Daten beim Scraping-Vorfall verhindert. Aus dem Umstand folgende Zweifel, dass dem Missbrauch informationstechnischer Nutzungsfunktionen nicht mit Sicherheit Einhalt geboten werden kann, verblassen hier insoweit, als die oben beschriebenen Maßnahmen jedenfalls einen prozessökonomischen, massenhaften Abruf der Daten von der Plattform der Beklagten mit hinreichender Sicherheit verhindert hätten. Es steht schon zu bezweifeln, dass die unbekannten Dritten bei Bestehen effektiver

Abrufbeschränkungen im CIT überhaupt Daten von der Plattform der Beklagten in der streitgegenständlichen Form ausgelesen hätten, da die Funktionen der Anwendung auf dem damaligen Stand das Scraping im großen Stil erst ermöglicht haben. Jedenfalls wäre aber in diesem Fall in Anbetracht des hier erfolgten millionenfachen Datenabrufs die Wahrscheinlichkeit eines zufälligen Abrufs der klägerischen Daten bei bestehenden effektiven Beschränkungen auf ein Minimum reduziert gewesen, da wegen des erheblichen Mehraufwands ein Abschöpfen lediglich in deutlich verringertem Maß erfolgen hätte können.

c) Das Gericht hält in Bemessung nach § 287 Abs. 1 ZPO einen Ersatz für die immateriellen Einbußen in Höhe von 400 Euro für angemessen.

aa) Ausgangspunkt für die Bemessung der Höhe ist – wie auch im Rahmen des § 253 Abs. 2 BGB – die Ausgleichs- und Genugtuungsfunktion des immateriellen Schadensersatzes, deren Schwerpunkt auf dem Ausgleich der erlittenen Einbußen liegt (vgl. BGH, Beschluss vom 16. September 2016 – VGS 1/16 –, Rn. 48, juris). So soll nach Erwägungsgrundes 146 S.6 der DSGVO die betroffene Person einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten. In welchem Umfang der Schadensersatz Vollständigkeit und Wirksamkeit erreicht, hängt von den Umständen des Einzelfalles ab. Dabei können beispielsweise unter Berücksichtigung der Wertungen aus Art. 9, 10 und Art. 82 Abs. 3 DSGVO die Schutzbedürftigkeit und der Umfang der betroffenen Daten, die Art und Erheblichkeit der Datenschutzverstöße, das Ausmaß der subjektiven Gefühlsbeeinträchtigung ebenso Beachtung finden, wie Maßnahmen des Schädigers zur Minderung oder Intensivierung des der betroffenen Person entstandenen Schadens. Schließlich ist auch eine etwaige Mitverursachung der Schäden durch den Betroffenen selbst nicht außer Betracht zu lassen (LG Halle, Urteil vom 28. April 2023 – 4 O 250/22).

bb) Hieran gemessen ist der Ansatz in der genannten Höhe gerechtfertigt.

Dabei hat das Gericht zunächst zugrunde gelegt, dass die betroffenen Daten teilweise bereits öffentlich waren, in ihrer Gesamtheit keiner besonders schutzbedürftigen Datenkategorie unterfallen und folglich der Kontrollverlust relativ betrachtet nicht von besonders starkem Gewicht ist. Zugleich war aber auch zu beachten, dass aufgrund der aufgezeigten Missbrauchspotenziale der Kontrollverlust über den verknüpften Datensatz und das nach allgemeiner Lebenserfahrung naturgemäß damit einhergehende Unwohlsein über die zweckwidrige Verwendung auch nicht unerheblich sind.

Darüber hinaus ist auch die rechtswidrige Verarbeitung unter mehrfachem Verstoß gegen die DSGVO ebenso in die Bewertung eingeflossen, wie in zeitlicher Hinsicht, dass seit Abruf der Daten durch das Scraping ca. zwei Jahre vergangen sind, ehe die Öffentlichkeit hiervon durch die Beklagte erfuhr. Unstreitig hat die Beklagte überdies weder die Klägerin selbst gem. Art. 34 DSGVO, noch die gem. Art. 55 DSGVO zuständige irische Datenschutzaufsichtsbehörde DPC gem. Art. 33 DSGVO im gebotenen Zeitraum informiert, um dafür Sorge zu tragen, dass mögliche Gegenmaßnahmen wie z.B. die Änderung der Mobilfunknummer zeitnah ergriffen werden können.

Ohne Bedeutung ist dagegen im vorliegenden Fall, dass die Klägerin sich frei verantwortlich auf der Plattform registriert, ihre Telefonnummer dort angegeben und die Suchbarkeitseinstellungen nicht auf die privateste Einstellung nach Registrierung verändert hat. Eine Berücksichtigung würde den der DSGVO zugrundeliegenden Gedanken konterkarieren, dass Nutzer von einer rechtmäßigen und integren Datenverarbeitung ausgehen dürfen. Dies gilt erst recht dann, wenn sich Nutzer unter anderem dann zu einer Registrierung entscheiden, weil das soziale Netzwerk Facebook im Zeitpunkt der Anmeldung bereits eine gesellschaftlich dominante Position zur Teilhabe an zwischenmenschlicher Kommunikation eingenommen hat. Zuletzt steht einer Berufung auf die unveränderten Voreinstellungen auch entgegen, dass die verordnungswidrige Standardkonfiguration entgegen Art. 25 Abs. 2 DSGVO (vgl. LG Halle, Urteil vom 28. April 2023 – 4 O 250/22) zur Suchbarkeit von der Beklagten gerade präferiert war, um die von ihr verfolgten Zwecke der Vernetzung von Nutzern zu erreichen. Ihr ist es dann aber verwehrt, sich darauf zu berufen, dass es an der Klägerin gewesen wäre, ihre rechtswidrigen Einstellungsmodalitäten zu korrigieren (vgl. LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 101, juris).

3. Der Zinsanspruch zum Antrag zu 1.a. ergibt sich aus §§ 286, 288 BGB.

II. Der Antrag zu 2. ist zulässig und begründet. Die Klägerin hat ein Interesse an der begehrten Feststellung, da in Ansehung der bereits beschriebenen latenten Gefahren, die mit einer Veröffentlichung eines Datenbündels unter Einschluss einer Mobilfunknummer einhergehen, nicht ausgeschlossen ist, dass unbefugte Dritte durch betrügerisches Verhalten z.B. im Online-Banking oder -Handel zulasten der Klägerin diesem weiteren materiellen Schaden zufügen. Macht die Klägerin – wie vorliegend in Form des Rechts auf Schutz der sie betreffenden personenbezogenen Daten – die Beeinträchtigung absolut geschützter Rechtsgüter und nicht nur Vermögensschäden

geltend, so genügt es, dass der Eintritt derartiger Schäden nicht ausgeschlossen werden kann, die Möglichkeit von Spätschäden also gegeben ist (vgl. BGH, Beschluss vom 09. Januar 2007 – VI ZR 133/06 –; BGH, Urteil vom 20. März 2001 – VI ZR 325/99 –, Rn. 11, juris). Der Feststellungsantrag ist auch begründet, da ein haftungsrechtlich relevanter Eingriff gegeben ist, der zu möglichen künftigen Schäden führen kann. Die sachlichen und rechtlichen Voraussetzungen eines Schadensersatzanspruchs liegen nämlich im geltend gemachten Umfang vor.

III. Der Antrag zu 3.a. ist unzulässig, da ein Rechtsschutzbedürfnis nicht ersichtlich ist. Einem "Scrapen" der Telefonnummer unter Verwendung des CIT, das der gegenständlichen Rechtsgutsverletzung zugrunde liegt, konnte die Klägerin schon seit Kenntniserlangung vom Scraping-Sachverhalt ohne gerichtliche Hilfe jedenfalls vorbeugen, indem sie die Suchbarkeitseinstellungen auf der Webseite der Beklagten eigenhändig privateste Einstellung anpassen, jedenfalls aber ihre optional angegebene Telefonnummer von der Plattform löschen konnte und dies nach wie vor kann.

IV. Der Antrag zu 3.b. ist zulässig (vgl. LG Halle, Urteil vom 28. April 2023 – 4 O 250/22), aber unbegründet. Es ist schon mit Blick auf die unterschiedlichen Rechtfertigungsgründe in Art. 6 Abs. 1 S.1 lit. b) – f) DSGVO nicht einzusehen, warum allein eine unwirksam erteilte Einwilligung zwingend die Rechtswidrigkeit der Verarbeitung und damit auch eine den Unterlassungsanspruch stützende Rechtsverletzung begründet. Zwischen den Parteien ist zudem unstreitig, dass eine Einwilligung seitens der Beklagten nicht eingeholt wurde. Es erschließt sich folglich nicht, woraus mangels in der Vergangenheit erfolgter Verarbeitung der Telefonnummer auf Grundlage einer Einwilligung das klägerische Recht resultieren soll, dies künftig der Beklagten zu untersagen.

V. Der Antrag zu 4 ist zulässig, aber unbegründet, da die Beklagte mit Schreiben vom 8. Mai 2023 den Anspruch der Klägerin auf Auskunft aus § 15 DSGVO bereits vorprozessual i.S.d. § 362 Abs. 1 BGB erfüllt hat. Dabei ist ohne Belang, ob die Auskunft auch inhaltlich der Richtigkeit entspricht. Es kommt lediglich darauf an, dass die Auskunft nach dem Willen des Schuldners im geschuldeten Gesamtumfang erteilt wird (BGH, Urteil vom 3. September 2020 – III ZR 136/18 –, Rn. 43, juris). Dies war hier der Fall. Die Beklagte hat mitgeteilt, dass sie über eine Kopie der verlangten Rohdaten, welche die durch Scraping abgerufenen Daten enthielten, nicht verfüge. Auf Grundlage der bislang vorgenommenen Analysen sei es ihr jedoch gelungen, der Nutzer-ID der Klägerin die bestimmten Daten zuzuordnen, die nach ihrem Verständnis in den durch Scraping

abgerufenen Daten erschienen und mit den auf dem Facebook-Profil der Klägerin verfügbaren Informationen übereinstimmten. Weiter hat die Beklagte erläutert, wie das Daten-Scraping ihrer Einschätzung nach erfolgte. Schließlich hat die Beklagte auch erklärt, dass sie davon ausgehe, dass die Telefonnummer der Klägerin in den durch Scraping abgerufenen Daten enthalten gewesen sei. Mit dem umfangreichen Schreiben hat die Beklagte nicht zuletzt in Ansehung des letzten Absatzes des Schreibens zum Ausdruck gebracht, dass sie die von ihr geschuldeten Angaben mitgeteilt hat.

VI. Die Klägerin hat keinen Anspruch auf Ersatz ihrer vorgerichtlichen Anwaltskosten gem. § 82 Abs. 1 DSGVO. Dem klägerischen Vortrag lässt sich nicht entnehmen, dass sich die Beklagte bereits in Verzug befand, als die Klägerin den Rechtsanwalt beauftragt hatte. Ein kausaler Schaden ist folglich nicht schlüssig dargelegt.

B. Die Kostenentscheidung beruht auf § 92 Abs. 1 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus §§ 708 Nr. 11, 711, 709 S.1, 2 ZPO.

C. Der von Amts wegen durch das Gericht gem. § 63 Abs. 2 S.1 GKG festzusetzende Gegenstandswert liegt in Bemessung nach §§ 39, 40, 43, 48 Abs. 1 GKG i.V.m. § 3 ZPO innerhalb der festgesetzten Stufe.

Die Entscheidung über die Festsetzung des Streitwertes kann mit der Beschwerde angefochten werden. Sie ist nur zulässig, wenn sie innerhalb von sechs Monaten, nachdem die Entscheidung in der Hauptsache rechtskräftig geworden ist oder das Verfahren sich anderweitig erledigt hat, bei dem Landgericht Halle, 06108 Halle, Hansering 13 eingeht.
Wird der Streitwert später als einen Monat vor Ablauf dieser Frist festgesetzt, kann die Beschwerde innerhalb eines Monats nach Zustellung oder formloser Mitteilung der Festsetzung bei dem Gericht eingelegt werden. Die Beschwerde ist nur zulässig, wenn der Wert des Beschwerdegegenstandes 200,00 € übersteigt oder das Gericht die Beschwerde in diesem Beschluss zugelassen hat.
Beschwerdeberechtigt ist, wer durch diese Entscheidung in seinen Rechten beeinträchtigt ist. Die Beschwerde wird durch Einreichung einer Beschwerdeschrift oder zur Niederschrift der Geschäftsstelle des genannten Gerichts eingelegt. Sie kann auch zur Niederschrift der Geschäftsstelle eines jeden Amtsgerichts erklärt werden, wobei es für die Einhaltung der Frist auf den Eingang bei dem genannten Gericht ankommt. Sie ist von dem Beschwerdeführer oder seinem Bevollmächtigten zu unterzeichnen.
Die Einlegung kann auch in elektronischer Form erfolgen. Informationen zu den weiteren Voraussetzungen zur Signatur und Übermittlung sind auf dem Justizportal des Bundes und der Länder (www.justiz.de) im Themenbereich zur elektronischen Kommunikation zu finden. Eine Einlegung per einfacher E-Mail ist unzulässig.
Die Beschwerde muss die Bezeichnung des angefochtenen Beschlusses sowie die Erklärung enthalten, dass Beschwerde gegen diesen Beschluss eingelegt wird. Soll die Entscheidung nur zum Teil angefochten werden, so ist der Umfang der Anfechtung zu bezeichnen.

Beglaubigte Abschrift
Halle, 29.02.2024

_____ ,
, JHS´in,als Urkundsbeamtin der Geschäftsstelle des Landgerichts