Abschrift

13 O 51/23

Landgericht Duisburg

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

Klägerin,

Prozessbevollmächtigte: Rechtsanwälte WBS.LEGAL, Eupener Straße 67, 50933 Köln,

gegen

die Meta Platforms Ireland Limited, vertreten durch den Geschäftsführer (Director) Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland,

Beklagte,

Prozessbevollmächtigte: Rechtsanwälte Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB, Bockenheimer Anlage 44, 60322 Frankfurt,

hat die 13. Zivilkammer des Landgerichts Duisburg
auf die mündliche Verhandlung vom 23.05.2024
durch die Richterin am Landgericht als Einzelrichterin

für Recht erkannt:

Die Beklagte wird verurteilt, an die Klägerin 250,00 EUR nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 04.08.2023 zu zahlen.

Im Übrigen wird die Klage abgewiesen.

Die Klägerin trägt die Kosten des Rechtsstreits.

Das Urteil ist vorläufig vollstreckbar. Der jeweilige Vollstreckungsschuldner kann die Vollstreckung durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht der jeweilige Vollstreckungsgläubiger vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrags leistet.

T a t b e s t a n d :

Die Klägerin macht Schadensersatz-, Unterlassungs- und Auskunftsansprüche wegen der Verletzung der Datenschutz-Grundverordnung (im Folgenden: DSGVO) seitens der Beklagten im Zusammenhang mit dem sogenannten „Scraping-Vorfall“ bei Facebook geltend.

Die Beklagte betreibt in der Europäischen Union das soziale Online-Netzwerk Facebook und bietet u. a. über www.facebook.com Dienste an, die für private Nutzer kostenlos sind. Die Klägerin war spätestens seit dem Jahr 2015 als Nutzerin bei der Online-Plattform registriert und schloss in diesem Zusammenhang mit der Beklagten einen Nutzungsvertrag ab. Nach der Registrierung waren und sind bis heute bestimmte Informationen über den jeweiligen Nutzer – konkret relevant Vorname, Nachname, Benutzer-ID, Nutzername, Geschlecht – im Internet für jedermann, ohne sich dafür selbst ein eigenes Profil als Nutzer bei der Beklagten anlegen zu müssen, sicht- und suchbar (sogenannte "immer öffentliche" Nutzerinformationen). Sichtbar waren und sind im Einzelfall zusätzlich im Hinblick auf die von den Nutzern zu treffende sogenannte Zielgruppenauswahl sonstige Nutzerinformationen (u. a. Telefonnummern, Wohnort, Stadt, Beziehungsstatus, Geburtstag und Email-Adresse), nämlich dann, wenn die Zielgruppenauswahl auf "öffentlich" festgelegt war bzw. ist.

Seit spätestens Januar 2018 bis zum 06.09.2019 kam es zu einem sog. Daten-Scraping im Hinblick auf die bei der Beklagten gespeicherten Nutzerdaten. Hierbei sammelten Dritte bei der Beklagten hinterlegte Informationen von Nutzern der Beklagten. Die gesammelten Daten wurden im April 2021 im Darknet veröffentlicht.

Das Abgreifen der Daten geschah unter Nutzung von Suchfunktionen, die die Beklagte registrierten Nutzern damals zur Verfügung stellte:

Jeder Nutzer, der bei der Beklagten eine Mobilfunktelefonnummer hinterlegt hatte, konnte mithilfe der Zielgruppenauswahl bestimmen, für wen diese Telefonnummer sichtbar war. War die Einstellung nicht auf „öffentlich“ gestellt, war die Telefonnummer auf dem Profil grundsätzlich nicht für andere sichtbar. Daneben stellte die Beklagte die Möglichkeit der Einstellung der Suchbarkeit über die Telefonnummer zur Verfügung. Mit diesem Hilfsmittel sollten die Nutzer über ihre Telefonnummer gefunden werden können. So konnten neue Nutzer etwa andere Nutzer über die Eingabe der Telefonnummer suchen. Voraussetzung war, dass der zu findende Nutzer seine Suchbarkeit über die Telefonnummer auf „alle“ gestellt hatte. Eine Suche über die Telefonnummer war in diesem Fall auch dann möglich, wenn die Zielgruppenauswahl auf „nicht öffentlich“ gestellt war.

Darüber hinaus stellte die Beklagte ein sog. Kontakt-Importer-Tool (im Folgenden: Kontaktimportfunktion) zur Verfügung. Über dieses Werkzeug konnten Nutzer ihre Kontakte auf die Plattform und auch von ihren Mobilgeräten in den sogenannten Messenger von Facebook hochladen. Geschah dies, so war es möglich, diejenigen dieser Kontakte, die auf der Facebook-Plattform ebenfalls registriert waren, zu finden und mit ihnen in Verbindung zu treten. Um eine Suchbarkeit über die Suchfunktion auf der Plattform und über die Kontaktimportfunktionen auszuschließen oder einzuschränken, war es erforderlich, die jeweilige Standardeinstellung "alle" / "everyone" auf "Freunde" oder auch "Freunde von Freunden" sowie seit Mai 2019 auch auf "nur ich" umzustellen.

Die Scraper machten sich zunächst die Suchfunktion auf der Plattform zu Nutze, indem sie sich (unter Vorgabe fremder oder nicht existierender Identitäten) bei der Beklagten als Nutzer registrierten. Sodann – dies ist zwischen den Parteien streitig – gaben sie entweder ihnen bekannte Telefonnummern ein oder generierten unter Verwendung der gängigen Rufnummernformate fiktive Telefonnummern und suchten über die Suchfunktionen nach passenden Nutzern. Wurde eine Telefonnummer einem Nutzer zugeordnet, wurden dessen öffentliche Nutzerinformationen zugeordnet und abgerufen. Zu einem späteren Zeitpunkt nutzten die Scraper sodann die Kontaktimportfunktionen, um unter Einhaltung seitens der Beklagten eingeführter

Übertragungsbeschränkungen – ihnen bekannte oder künstlich generierte – Telefonnummern als ihre vermeintlichen Kontakte hochzuladen, die passenden konkret-individuell angezeigten Nutzer allein aufgrund dieser Telefonnummern zu identifizieren und ihnen ihre öffentlichen Nutzerinformationen zuzuordnen.

Nachdem sich die Beklagte dieses Scrapings gewahr geworden war, deaktivierte sie die Kontaktimportfunktion und ersetzte diese durch die sogenannte "People-You-May-Know"-Funktion ("Personen, die du kennen könntest"-Funktion, auch PYMK-Funktion genannt). Bei dieser kann zwar gleichfalls ein Nutzer der Beklagten seine Kontakte mitsamt Telefonnummer hochladen. Das System der Beklagten zeigt ihm dann aber nicht mehr allein aufgrund der Telefonnummer nur den einen passenden konkret-individuell Nutzer - "one-to-one" - an, sondern nur noch eine Liste von mehreren Personen, die aufgrund anderer zusätzlicher Zuordnungskriterien der hochgeladenen Kontakte, z. B. des Namens, zuzuordnen sein könnten.

Betroffen von dem Scraping-Vorfall war als Nutzerin der Beklagten auch die Klägerin. Ihre Mobilfunktelefonnummer war zwar in der sogenannten Zielgruppenauswahl auf „nicht öffentlich" und damit nicht sichtbar eingestellt. In der sogenannten Suchbarkeitseinstellung hingegen stand die Suchbarkeitseinstellung jedenfalls seit dem 15.11.2015 und noch bis Januar 2024 auf "alle", so dass die Mobilfunktelefonnummer der Klägerin trotz fehlender Sichtbarkeit suchbar war. In den im April 2021 veröffentlichten Daten waren die Telefonnummer der Klägerin, ihre Facebook-Nutzer-ID, ihr Vor- und Nachname, Geschlecht, das Land und ihr derzeitiger sowie ihr vorheriger Wohnsitz enthalten.

Mit anwaltlichem Schreiben vom 07.01.2023 forderte die Klägerin die Beklagte zur Zahlung von Schadensersatz und zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte sowie zur Auskunft darüber auf, welche konkreten Daten abgegriffen und veröffentlicht worden seien.

Die Klägerin behauptet, sie habe durch das Daten-Scraping einen Kontrollverlust über ihre Daten erlitten, ihr sei deshalb unwohl gewesen und sie habe sich Sorgen deshalb gemacht. Sie habe überdies befürchtet, dass ihre personenbezogenen Daten durch Dritte missbraucht werden könnten. Auch habe sie zahlreiche unbekannte Kontaktversuche über SMS und E-Mail erhalten, welche offensichtliche

Betrugsversuche und potentielle Virenlinks enthielten. Sie reagiere deshalb mittlerweile mit größter Vorsicht auf jegliche E-Mails und Nachrichten.

Die Klägerin beantragt,

1. die Beklagte zu verurteilen, an sie 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. festzustellen, dass die Beklagte verpflichtet ist, ihr alle künftigen Schäden zu ersetzen, die ihr 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 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 Klägerin, namentlich Telefonnummer, Facebook-ID, 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 Klägerin auf Grundlage der 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, ihr Auskunft über die Klägerin 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.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet, sie halte keine Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten enthalten würden. Daher habe der Klägerin lediglich mitgeteilt werden können, welche Datenkategorien betroffen sein könnten.

Die Beklagte behauptet weiter, sie setze unterschiedliche Maßnahmen zur Verringerung des Scraping-Risikos ein. Unter anderem identifiziere sie Aktivitätsmuster und auffällige Verhaltensweisen, die typischerweise mit automatisierten Computeraktivitäten in Zusammenhang stünden, verwende Übertragungsbeschränkungen und gehe juristisch gegen Scraper vor, soweit sie von entsprechenden Vorfällen erfahre. Sie passe ihre Systeme ferner laufend an die Entwicklungen der Scraping-Taktiken an.

Die Klageschrift ist der Beklagten am 03.08.2023 zugestellt worden. Das Gericht hat in der mündlichen Verhandlung vom 23.05..2023 die Klägerin persönlich angehört. Wegen der weiteren Einzelheiten des Sach- und Streitstands wird auf die zwischen den Parteien und ihren Prozessbevollmächtigten gewechselten Schriftsätze nebst Anlagen sowie auf das Protokoll der mündlichen Verhandlung vom 23.05.2023 Bezug genommen.

E n t s c h e i d u n g s g r ü n d e :

I.

Die Klage hat hinsichtlich des Antrags zu Ziffer 1. in Höhe von 250,00 EUR nebst Zinsen Erfolg. Im Übrigen ist die Klage unzulässig oder unbegründet.

1. Antrag zu Ziffer 1.

Die mit dem Antrag zu Ziffer 1. verfolgte Leistungsklage gerichtet auf den Ersatz immateriellen Schadens ist zulässig und in Höhe von 250,00 EUR begründet.

a.

Die Klage ist insoweit zulässig.

Das Landgericht Duisburg ist gemäß Art. 79 Abs. 2 S. 1, S. 2 DSGVO international zuständig, da die Beklagte in Deutschland eine Niederlassung und die Klägerin hier ihren gewöhnlichen Aufenthalt hat.

Der Antrag zu Ziffer 1. ist auch hinreichend bestimmt gemäß § 253 Abs. 2 Nr. 2 ZPO. Hiernach muss die Klageschrift neben einem bestimmten Antrag eine bestimmte Angabe des Gegenstandes und des Grundes des erhobenen Anspruchs enthalten. Damit werden der Streitgegenstand abgegrenzt und die Grenze der Rechtshängigkeit und der Rechtskraft festgelegt sowie Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts bestimmt. Eine ordnungsgemäße Klageerhebung erfordert eine Individualisierung des Streitgegenstandes. Der Kläger muss die gebotene Bestimmung des Streitgegenstandes vornehmen und kann sie nicht zur Disposition des Gerichts stellen (BGH, Urt. v. 17.01.2023 – VI ZR 203/22, juris Rn. 14). Die Klägerin stützt ihr Entschädigungsbegehren auf unterschiedliche Verstöße gegen die DSGVO vor und nach dem Scraping-Vorfall. Hierbei handelt es sich jedenfalls um eine nach § 260 ZPO zulässige Klagehäufung, sofern man nicht bereits von einem einheitlichen Streitgegenstand (hierzu OLG Hamm, Urt. v. 15.08.2023 – I-7 U 19/23, juris Rn. 51) ausgeht. Es besteht vorliegend auch keinerlei Zweifel daran, dass sämtliche auf Grund des Scraping-Vorfalls gerügten Datenschutzverstöße und Persönlichkeitsverletzungen der Klägerin und der dadurch bis zum Schluss der mündlichen Verhandlung entstandene immaterielle Schaden umfassend und abschließend – also auch nicht etwa als verdeckte Teilklage – rechtshängig geworden sind und einer Entscheidung zugeführt werden sollen. Da es bei einer Klage auf immateriellen Schadensersatz einer Bezifferung ohnehin nicht bedarf, begegnet auch die einheitliche Angabe eines Gesamtbetrages keinen Bedenken (OLG Hamm, Urt. v. 15.08.2023 – I-7 U 19/23, juris Rn. 53).

b.
Der Antrag ist auch in Höhe von 250,00 EUR begründet.

Der Klägerin steht ein Anspruch auf ein angemessenes Schmerzensgeld aus Art. 82 Abs. 2, Abs. 1 DSGVO zu.

Ein Anspruch aus Art. 82 Abs. 2, Abs. 1 DSGVO setzt zunächst voraus, dass diese Regelung zeitlich, sachlich und räumlich anwendbar ist. Im Übrigen hat Art. 82 Abs. 2 DSGVO, der die Haftungsregelung, deren Grundsatz in Abs. 1 dieses Artikels festgelegt ist, präzisiert, drei Voraussetzungen für die Entstehung des Schadensersatzanspruchs, nämlich eine Verarbeitung personenbezogener Daten unter Verstoß gegen die Bestimmungen der DSGVO, einen der betroffenen Person entstandenen Schaden und einen Kausalzusammenhang zwischen der rechtswidrigen Verarbeitung und diesem Schaden (EuGH Urt. v. 4.5.2023 - C-300/21, GRUR-RS 2023, 8972 Rn. 36).

aa.
Der Anwendungsbereich der DSGVO ist vorliegend teilweise eröffnet:

Die DSGVO gilt seit dem 25.05.2018 (Art. 99 Abs. 2 DSGVO) unmittelbar in jedem Mitgliedstaat der Europäischen Union (BGH Urt. v. 27.7.2020 - VI ZR 405/18, BGHZ 226, 28 Rn. 11), Art. 288 Abs. 2 AEUV.

Es ist - der Behauptung der Klägerin folgend - davon auszugehen, dass das Scraping konkret bezüglich der Daten der Klägerin nach dem 24.05.2018 erfolgte, da die Beklagte ihrer aus § 138 Abs. 2 ZPO abgeleiteten sekundären Darlegungslast bezüglich des genauen Zeitpunkts dieses Scraping-Vorgangs nicht genügt hat. Eine sekundäre Darlegungslast trifft den Prozessgegner der primär darlegungsbelasteten Partei, wenn diese keine nähere Kenntnis der maßgeblichen Umstände und auch keine Möglichkeit zur weiteren Sachaufklärung hat, während der Bestreitende alle wesentlichen Tatsachen kennt und es ihm unschwer möglich und zumutbar ist, nähere Angaben zu machen. Genügt der Anspruchsgegner seiner sekundären Darlegungslast nicht, gilt die Behauptung des Anspruchstellers nach § 138 Abs. 3 ZPO als zugestanden (vgl. zur ständigen Rechtsprechung etwa BGH Urt. v. 25.5.2020 - VI ZR 252/19, NJW 2020, 1962 Rn. 37 m. w. N.).

Der Beklagten, deren Sphäre das erfolgte Daten-Scraping hier zuzuordnen ist und die nach Art. 5 Abs. 2, Art. 15 DSGVO umfassend rechenschafts- und auskunftspflichtig hinsichtlich Verarbeitungszwecken und –art, aber auch hinsichtlich der Offenlegung der Daten gegenüber Dritten ist und gemäß Art. 5 Abs. 2 DSGVO die Beweislast für die rechtmäßige Datenerhebung und –verarbeitung trägt, obliegt hinsichtlich des konkreten Zeitpunkts des Daten-Scrapings in Bezug auf die Daten

der Klägerin eine sekundäre Darlegungslast (OLG Hamm, Urt. v. 15.08.2023 – I-7 U 19/23, juris Rn. 64 ff.). Dem ist die Beklagte, die den Zeitraum des Daten-Scrapings lediglich mit zwischen Januar 2018 und September 2019 angegeben hat, nicht hinreichend nachgekommen. Es ist daher davon auszugehen, dass das Daten-Scraping vorliegend nach dem 25.05.2018 erfolgte.

Nicht in den Anwendungsbereich der DSGVO fällt jedoch die Rüge der Klägerin, die Beklagte habe sie bei Erhebung ihrer Daten nicht hinreichend über die Verarbeitung personenbezogener Daten informiert und aufgeklärt und hierdurch gegen Art. 5 Abs. 1 i.V.m. Art. 13, 14 DSGVO verstoßen. Denn maßgeblich für die Erfüllung der Pflichten aus Art. 13, 14 DSGVO ist der Zeitpunkt der Erhebung der Daten, die vorliegend – die Registrierung der Klägerin und die Hinterlegung ihrer Telefonnummer erfolgten bereits vor 2018 – vor dem Zeitpunkt des Inkrafttretens der DSGVO erfolgte. Der insoweit geltend gemachte Verstoß fällt daher nicht in den zeitlichen Anwendungsbereich der DSGVO.

Auch der sachliche Anwendungsbereich der DSGVO ist eröffnet. Der Betrieb eines sozialen Netzwerkes durch Sammlung / Speicherung jedenfalls des Namens und Geschlechts von Mitgliedern und die automatisierte Vernetzung der Mitglieder sowie deren Beschickung mit individualisierter Werbung fällt in den sachlichen Anwendungsbereich der DSGVO im Sinne des Art. 2 Abs. 1 DSGVO; die Tätigkeit unterfällt keinem Ausnahmetatbestand im Sinne von Art. 2 Abs. 2 bis Abs. 4 DSGVO oder der Öffnungsklausel nach Art. 85 Abs. 2 DSGVO (OLG Hamm, Urt. v. 15.08.2023 – I-7 U 19/23, juris Rn. 78).

Bei den hier in Rede stehenden Daten (Telefonnummer Facebook-Nutzer-ID, Vor- und Nachname, Geschlecht, Land, Wohnort) handelt es sich auch um personenbezogene Daten im Sinne des Art. 2 Abs. 1 i.V.m Art. 4 Nr. 1 DSGVO. Diese Daten hat die Beklagte auch automatisiert verarbeitet im Sinne von Art. 2 Abs. 1 i.V.m. Art. 4 Nr. 2 DSGVO.

Die DSGVO ist auch räumlich gemäß Art. 4 Nr. 7 DSGVO anwendbar, da die Beklagte, die Verantwortliche der Verarbeitung im Sinne von Art. 4 Nr. 7 DSGVO ist, ihren Sitz in Irland hat und dort eine Niederlassung für die Tätigkeit ihrer Datenverarbeitung betreibt (OLG Hamm, Urt. v. 15.08.2023 – I-7 U 19/23, juris Rn. 82).

bb.
Auch die weiteren Voraussetzungen des Art. 82 Abs. 2, Abs. 1 DSGVO sind vorliegend erfüllt. Die Beklagte hat personenbezogene Daten der Klägerin unter Verstoß gegen die Vorschriften der DSGVO verarbeitet (dazu unter (1)) und der Klägerin ist hierdurch ein immaterieller Schaden entstanden (dazu unter (2)).

(1)
Die Beklagte, die als Verantwortliche im Sinne der DSGVO für die Einhaltung der Vorschriften der DSGVO darlegungs- und beweisbelastet ist (EuGH, Urt. v. 14.12.2023 – C-340/21, Rn. 48 ff.), hat Verstöße gegen die Art. 5 Abs. 1 lit. a), Art. 6 Abs. 1 DSGVO (dazu unter (a), gegen Art. 5 Abs. 1 lit. b), Art. 25 Abs. 1 und Abs. 2 DSGVO (unter (b)) und gegen Art. 5 Abs. 1 lit. f), Art. 32 DSGVO (unter (c)) nicht ausgeräumt.

(a)
Die Beklagte hat personenbezogene Daten der Klägerin ab dem 25.05.2018 fortgesetzt verarbeitet im Sinne des Art. 5 Abs. 1 lit. a) Var. 1, Art. 6 Abs. 1, Art. 7 i.V.m. Art. 4 Nr. 2 DSGVO verarbeitet. Die Datenverarbeitung war nur rechtmäßig, wenn ab diesem Zeitpunkt ein Rechtfertigungsgrund nach Art. 6 Abs. 1 Unterabs. 1 DSGVO vorlag. Daran fehlte es.

Die Klägerin hat nicht wirksam gemäß Art. 6 Abs. 1 lit. a) in die Suchbarkeit ihrer Telefonnummer eingewilligt. Denn vor und auch über den 25.05.2018 hinaus waren die Suchbarkeitseinstellungen bei einer Registrierung auf Facebook oder der Hinterlegung einer Telefonnummer auf der Plattform auf „alle“ voreingestellt. Der jeweilige Nutzer musste dies zunächst deaktivieren, wollte er nicht über seine Telefonnummer gesucht werden können. Eine solche Voreinstellung genügt indes nicht den Anforderungen der DSGVO an eine wirksame Einwilligung. Insoweit ist vielmehr ein aktives Verhalten des Einwilligenden zwingend erforderlich (EUGH, Urt. v. 11.11.2020 – C-61/19, juris Rn. 52). Ob die Klägerin – die sich bereits vor 2018 registriert und ihre Telefonnummer hinterlegt hatte – eine zu diesem Zeitpunkt mit den geltenden rechtlichen Bestimmungen konforme Einwilligung in die Datenverarbeitung abgegeben hat, kann hier dahinstehen. Denn ab der Geltung der DSGVO war für die weitere Verarbeitung der Daten das Vorliegen einer den Anforderungen der DSGVO entsprechenden Einwilligung erforderlich (OLG Hamm,

Urt. v. 15.08.2023 – I-7 U 19/23, juris Rn. 114). Hieran fehlt es. Die Beklagte beruft sich daher zu Recht nicht auf den Rechtfertigungsgrund des Art. 6 Abs. 1 lit. a).

Entgegen der Auffassung der Beklagten war die Datenverarbeitung mit Blick auf die Suchbarkeit des Nutzerprofils über die Mobilnummer per Such- und Kontaktimportfunktion und insbesondere die diesbezügliche Voreinstellung der Suchbarkeit für "alle" nicht zur Vertragszweckerfüllung erforderlich und damit nicht gemäß Art. 6 Abs. 1 lit. b) DSGVO gerechtfertigt. Damit eine Verarbeitung personenbezogener Daten als für die Erfüllung eines Vertrags erforderlich im Sinne des Art. 6 Abs. 1 Unterabs. 1 lit. b DSGVO angesehen werden kann, muss sie objektiv unerlässlich sein, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist. Der Verantwortliche muss somit nachweisen können, inwiefern der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte (EuGH Urt. v. 4.7.2023 - C-252/21, GRUR-RS 2023, 15772 Rn. 98). Das hat die Beklagte hier nicht dargelegt. Die Datenverarbeitung mit Blick auf die Suchbarkeit des Nutzerprofils über die Mobilfunknummer per Such- und Kontaktimportfunktion sowie die diesbezügliche Voreinstellung der Suchbarkeit auf „alle“ war nicht für die Erfüllung des Vertragszwecks objektiv unerlässlich. Das zeigt sich schon daran, dass die Nutzer insoweit unterschiedliche Einstellungsmöglichkeiten hatten, die Nutzung und Vernetzung über die Online-Plattform also erkennbar auch ohne die Angabe der Telefonnummer des jeweiligen Nutzers sowie die Aktivierung der Suchfunktion möglich war (OLG Hamm, Urt. v. 15.08.2023 – I-7 U 19/23, juris Rn. 94 ff.).

Auch sonstige Rechtfertigungsgründe gemäß Art. 6 Abs. 1 DSGVO sind vorliegend nicht ersichtlich und werden von der Beklagten auch nicht behauptet.

(b)

Die Beklagte hat auch einen Verstoß gegen Art. 5 Abs. 1 lit. b), Art. 25 Abs. 2 DSGVO nicht ausgeräumt. Da die Klägerin 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. Wie dargelegt lässt sich insoweit ein Rechtfertigungsgrund nicht feststellen. Die Beklagte kann sich auch

insoweit daher nicht darauf berufen, dass die Voreinstellung für die Erreichung des Hauptzwecks des Vertrags erforderlich war.

(c)
Die Beklagte hat auch nicht dargelegt, dass die Datenverarbeitung im Einklang mit Art. 5 Abs. 1 lit. f), Art. 32 DSGVO stand.

Die Beklagte hat nicht hinreichend substantiiert dargelegt, dass sie den Vorgaben des Art. 32 zur Sicherheit der Verarbeitung genügt hätte.

Die Argumentation der Beklagten verfängt zunächst insoweit nicht, als sie sich auf den Rechtsstandpunkt einer als solchen schon fehlenden, aber jedenfalls rechtmäßigen Datenverarbeitung durch sie stellt - mit der Begründung, die Daten gar nicht unbefugt Dritten, den Scrapern, offen gelegt zu haben, weil unter Verstoß gegen die Meta-Nutzungsbedingungen nur die Art des Abrufs der Daten durch die Scraper, nicht aber der Zugang zu den abgerufenen, ohnehin öffentlichen Daten unberechtigt gewesen sei.

Entgegen ihrer Rechtsansicht hat die Beklagte die geleakten Daten den Scrapern offengelegt; denn in der (seitens der Beklagten automatisierten) Ausführung des Abrufs über die Such- oder Kontaktimportfunktionen liegt unzweifelhaft eine Datenverarbeitung im Sinne des Art. 4 Nr. 2 DSGVO in Form der Offenlegung durch Übermittlung. Der Begriff "Verarbeitung", wie er in Art. 4 Nr. 2 DSGVO definiert wird, ist nach dem Willen des Unionsgesetzgebers mit der Formulierung "jede[r] Vorgang" weit zu fassen und stellt keine erschöpfende Aufzählung von Vorgängen im Zusammenhang mit personenbezogenen Daten oder Sätzen solcher Daten - wie etwa Erheben, Erfassen, Speicherung und Abfragen - dar (vgl. EuGH Urt. v. 22.6.2023 - C-579/21, BeckRS 2023, 14515 Rn. 46 ff. m. w. N. zu Abfragen von Mitarbeitern des datenverarbeitenden Unternehmens; EuGH Urt. v. 4.5.2023 - C-487/21, NJW 2023, 2253 Rn. 27 m. w. N.).

Ohne die automatisierte Datenverarbeitung der Beklagten hätten die Scraper die Nutzerinformationen nicht zusammenstellen und veröffentlichen können.

Offenlegung und Zugangsgewährung geschahen auch unbefugt. Das ergibt sich schon - unabhängig von deren genauer rechtlicher Einordnung - aus den

Nutzungsbedingungen der Beklagten, die ein Vorgehen wie das der Scraper, die als Nutzer registriert sein mussten, explizit untersagen (Anl. B19, Bl. 917 d.A.):

"Du darfst (ohne unsere vorherige Genehmigung) nicht mittels automatisierter Methoden auf Daten unserer Produkte zugreifen, solche Daten erfassen oder versuchen, auf Daten zuzugreifen, für die du keine Zugriffsberechtigung hast."

Das galt erst recht für Personen, die sich - wie die Scraper unter Vorgabe fremder oder nicht existierender Identitäten - bereits unrechtmäßig im Netzwerk der Beklagten angemeldet hatten.

Auch die weitere Argumentation der Beklagten verfängt nicht, soweit sie sich im Wesentlichen schlicht auf den Standpunkt stellt, ihre Pflichten zur Implementierung angemessener technischer und organisatorischer Maßnahmen gemäß Art. 32, Art. 24, Art. 5 Abs. 1 lit. f DSGVO im Zusammenhang mit der Kontaktimportfunktion nicht verletzt zu haben, weil sie ihre Anti-Scraping-Maßnahmen im relevanten Zeitraum regelmäßig überprüft und gegebenenfalls entsprechend den Marktgepflogenheiten zu den Sicherheitsstandards sukzessive aus der maßgeblichen ex-ante-Betrachtung in angemessener Weise angepasst habe, z. B. durch Übertragungsbegrenzungen, Boterkennung, Captchas ("Completely Automated Public Turing Test to tell Computers and Humans Apart" [auf Deutsch: Vollständig automatisierter öffentlicher Turing-Test, um Computer von Menschen zu unterscheiden]) und den "Social Connection Check" (Anzeige von Personen, nur wenn diese sich zu kennen schienen).

Tatsächlich waren die im Zeitpunkt des Scraping-Vorfalls bestehenden Maßnahmen unter Zugrundelegung des unstreitigen und streitigen Vortrags der Beklagten technisch und organisatorisch ungeeignet im Sinne des Art. 32 Abs. 1 Hs. 1 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, obwohl es in Bezug auf die Kontaktimportfunktionen bei Facebook und im Facebook-Messenger geeignete Maßnahmen gab.

Es ist weder von der Beklagten dargetan noch sonst ersichtlich, dass trotz ex-ante-Betrachtung wie geboten ab Geltung der DSGVO im Mai 2018 ausreichende Sicherheitsvorkehrungen gegen Scraping getroffen wurden. Konkret war es für die Beklagte, der ein Scraping bereits spätestens im März 2018 aufgefallen war, ohne

Weiteres möglich und im Hinblick auf die Datensicherheit ihrer Nutzer geboten sowie zumutbar - auch wenn es ihrem wirtschaftlichen Interesse möglicherweise widersprach -, die Kontaktimportfunktion auf Facebook, im Friend Center und im Facebook-Messenger unverzüglich einzuschränken und somit einen massiven weiteren Datenverlust an Unbefugte zu unterbinden. Es ist nicht ersichtlich, warum die vollständige Deaktivierung der Kontaktimportfunktionen noch rund sechzehn Monate dauerte oder warum nicht wenigstens andere weniger einschneidende, aber wirkungsvolle Maßnahmen getroffen wurden.Dass die zögerliche Vorgehensweise der Beklagten von der Hoffnung getragen gewesen sein mag, das Scrapen zu erschweren, reicht nicht aus, um das geforderte angemessene Schutzniveau zu erreichen. Dies gilt insbesondere vor dem Hintergrund, dass die Beklagte ihre Standardeinstellung "alle" für die Suchbarkeit über die Telefonnummer nicht - wie geboten - geändert hatte.

Soweit die Beklagte vorträgt, sie habe für die Kontaktimportfunktion der Plattform zu einem nicht näher konkretisierten Zeitpunkt einen "Social Connection Check" eingeführt, war dieser im Hinblick auf die allein vorgesehene Ähnlichkeitskontrolle und die danach fortbestehende Notwendigkeit, die streitgegenständliche Kontaktimportfunktion im Rahmen der Plattform - wie schon im April 2018 die Suchfunktion der Plattform - gleichwohl im Oktober 2018 zu eliminieren, evident ungeeignet (das gesamte Vorstehende unter (c): OLG Hamm, Urt. v. 15.08.2023 – I-7 U 19/23, juris Rn. 129 ff).

(d)
Es kann vorliegend dahinstehen, ob die Beklagte Verstöße gegen Art. 33, 34 DSGVO hinreichend ausgeräumt hat. Denn es ist nicht ersichtlich, dass der Verstoß gegen diese Pflichten zu einem eigenen Schaden oder zu einer Vertiefung des bereits durch die Veröffentlichung der gescrapten Daten entstandenen Schadens geführt hätte.

(e)
Gleiches gilt auch, soweit die Klägerin ihren Schadensersatzanspruch auch auf eine Verletzung der Auskunftspflicht gemäß Art. 15 DSGVO stützt. Es kann dahinstehen, ob der Beklagten überhaupt ein entsprechender Verstoß vorzuwerfen ist. Ein kausaler immaterieller Schaden ist hierdurch vorliegend schon deshalb nicht entstanden, weil die Klägerin im Rahmen ihrer persönlichen Anhörung in der Sitzung

vom 23.05.2024 angegeben hat, dass sie keinerlei Kenntnis darüber habe, ob gegenüber der Beklagten Auskunftsansprüche geltend gemacht worden seien. Auch das Schreiben der Beklagten vom 13.02.2024 – mit dem die Beklagte nach der klägerischen Darstellung nur unzureichend Auskunft erteilt haben soll – sei ihr, der Klägerin, nicht erinnerlich. Mit Rücksicht auf diese Angaben ist die Verursachung eines kausalen immateriellen Schadens durch die – unterstellt – unzureichende Auskunftserteilung ausgeschlossen.

(2)
Die Klägerin hat aufgrund der erfolgten Verstöße gegen Art. 5 Abs. 1 lit. a), Art. 6 Abs. 1 DSGVO , gegen Art. 5 Abs. 1 lit. b), Art. 25 Abs. 1 und Abs. 2 DSGVO sowie gegen Art. 5 Abs. 1 lit. f), Art. 32 DSGVO auch einen immateriellen Schaden im Sinne des Art. 82 Abs. 1 DSGVO erlitten.

Unter den Begriff des immateriellen Schadens fällt hierbei nach der Auslegung des EuGH schon der bloße – auch nur kurzzeitige – Kontrollverlust über die eigenen Daten (dazu EuGH, Urt. v. 11.04.2014 – C-741/21, juris Rn. 42) sowie die Befürchtung einer betroffenen Person, dass ihre personenbezogenen Daten durch Dritte missbräuchlich verwendet werden könnten (EuGH, Urt. v. 14.12.2023 – C-340/21, Rn. 75 ff.). Der der betroffenen Person entstandene Schaden muss auch keinen bestimmten Grad an Erheblichkeit aufweisen (EuGH, Urt. v. 04.05.2023 – C-300/21, Rn. 51).

Die Klägerin hat vorliegend einen Kontrollverlust über ihre Daten erlitten, welche von unbekannten Personen mittels Scrapings abgegriffen, zusammengeführt und im Internet veröffentlicht wurden, erlitten. Dem steht nicht entgegen, dass ihre personenbezogenen Daten Name, Land, Geschlecht, Wohnort bereits zuvor auf ihrem Facebook-Profil für jedermann öffentlich einsehbar waren. Denn jedenfalls auf ihre Telefonnummer traf dies nicht zu. Hinsichtlich dieser hat die Klägerin einen Kontrollverlust erlitten. Soweit die Telefonnummer von den Scrapern in das Kontaktimportertool eingegeben wurde, mithin nicht von der Beklagten „abgegriffen“ wurde, steht dies nicht entgegen. Denn die bloße Nummernfolge der Telefonnummer ist erst durch die Verknüpfung der Nummer mit den weiteren persönlichen Daten der Klägerin – insbesondere ihrem Namen – zu einem personenbezogenen Datum geworden. Gerade durch die Verknüpfung der Daten hat die Klägerin daher einen Kontrollverlust über ihre Daten erlitten.

Ferner ist das Gericht auf der Grundlage der im Rahmen der Sitzung vom 23.05.2024 erfolgten Parteianhörung gemäß § 141 ZPO mit der nach § 286 Abs. 1 ZPO erforderlichen Sicherheit davon überzeugt, dass die Klägerin tatsächlich die missbräuchliche Verwendung ihrer Daten durch Dritte infolge des Daten-Scrapings fürchtete. Gemäß § 286 Abs. 1 S. 1 ZPO hat das Gericht unter Berücksichtigung des gesamten Inhalts der Verhandlung und des Ergebnisses einer Beweisaufnahme nach freier Überzeugung zu entscheiden, ob eine tatsächliche Behauptung für wahr oder nicht wahr zu erachten sei. Dem Tatrichter ist es dabei auch grundsätzlich erlaubt, allein aufgrund des Vortrags der Parteien und ohne Beweiserhebung festzustellen, was wahr und was unwahr ist. Er kann dabei im Rahmen der freien Würdigung des Verhandlungsergebnisses den Behauptungen und Angaben einer Partei glauben, obwohl die Parteianhörung nach § 141 ZPO kein förmliches Beweismittel darstellt. Dies gilt unter Umständen auch dann, wenn eine Partei die Wahrheit ihrer Behauptung sonst nicht - auch nicht mittels Parteivernehmung, weil es an der erforderlichen Anfangswahrscheinlichkeit fehlt - beweisen kann und ihr im Einzelfall sogar den Vorzug vor Bekundungen eines Zeugen oder des als Partei vernommenen Gegners geben (BGH, Beschl. v. 27.09.2017 - XII ZR 48/17, juris Rn. 12).

Die Klägerin hat im Rahmen der persönlichen Anhörung glaubhaft geschildert, dass sie bei einer Internet-Recherche von dem Scraping-Vorfall erfahren und über die Internetseite eines Rechtsanwalts auch seine eigene Betroffenheit festgestellt. Die Klägerin hat weiter geschildert, dass sie deshalb befürchte, dass ihre Daten missbräuchlich verwendet werden könnten. Die Angaben der Klägerin sind glaubhaft, sie hat das Geschehen, insbesondere ihre Befürchtungen im Hinblick auf die Verwendung ihrer Daten, für das Gericht nachvollziehbar und widerspruchsfrei geschildert. Die Klägerin hat hierbei Erinnerungslücken – etwa dass sie nicht wisse, ob auch Auskunftsansprüche gegenüber der Beklagten geltend gemacht worden seien – von sich aus eingeräumt und auch für sie nachteilige Gesichtspunkte – wie dass sie keine Kenntnis darüber gehabt habe, ob die Beklagtenseite Auskünfte erteilt habe (dazu s. unten) – offen geschildert. Der Glaubhaftigkeit der Angaben der Klägerin steht hierbei auch nicht entgegen, dass sie ihre Telefonnummer im Anschluss an das Bekanntwerden des Datenlecks nicht gewechselt hat. Hierzu hat sie für das Gericht nachvollziehbar angegeben, dass dies für sie eine erhebliche

Unannehmlichkeit darstelle, da sie ihre Telefonnummer bereits seit langem habe und gut erinnern könne.

Das Gericht ist demgegenüber nicht mit der nach § 286 Abs. 1 ZPO erforderlichen Gewissheit davon überzeugt, dass die von der Klägerin geschilderten Spam-Nachrichten und unerwünschten Anrufe auf den hier in Rede stehenden Scraping-Vorfall zurückgeführt werden können. Eine Kausalität zwischen dem Vorfall und den von der Klägerin geschilderten Belästigungen erscheint zwar nicht fernliegend. Mit Blick darauf, dass heute die Angabe der eigenen Daten, insbesondere auch der eigenen Telefonnummer, auch bei sonstigen Tätigkeiten im Internet (z.B. Online-Shopping, sonstige soziale Netzwerke) häufiger vorkommt, kann nach Auffassung des Gerichts indes nicht ausgeschlossen werden, dass eine andere Ursache kausal für die Nachrichten und Anrufe ist. Dass die Klägerin ihre Daten sonst in keiner Weise im Internet verwendet hat, ist nicht vorgetragen.

In der Höhe ist der dem Grunde nach zu bejahende Schadensersatzanspruch der Klägerin aus Art. 82 Abs. 1, Abs. 2 DSGVO hier allerdings auf einen Betrag von 250,00 EUR beschränkt. Bei der Bemessung des Schadensersatzes sind die Kategorie der betroffenen personenbezogenen Daten, Art, Schwere und Dauer des Datenschutzverstoßes, die seelischen Auswirkungen bei dem Betroffenen, der Grad des Verschuldens, die ergriffenen Maßnahmen zur Minderung der Schadensfolgen sowie der Gesichtspunkt, ob etwa dauerhafte Beeinträchtigungen verbleiben, zu berücksichtigen (OLG Düsseldorf, Urt. v. 28.10.2021 – 16 U 275/20, juris Rn. 56).

Unter Anwendung dieser Maßstäbe war das der Klägerin zustehende angemessene Schmerzensgeld mit 250,00 EUR zu bemessen. Hierbei war auf der einen Seite zu berücksichtigen, dass die Beklagte in mehrfacher Hinsicht gegen die DSGVO verstoßen hat, und diese Verstöße auch länger andauerten. Auch erfuhr die Klägerin erst verhältnismäßig spät von der Betroffenheit ihrer Daten und wurde auch nicht durch die Beklagte selbst hierüber unterrichtet. Der Höhe nach begrenzend wirkt sich hier aber vor allem aus, dass es sich bei den betroffenen Daten der Klägerin mit Ausnahme der Telefonnummer um ohnehin über ihr bei der Beklagten vorhandenes Nutzerprofil öffentlich einsehbare Daten handelte, diese auch keine so hohe Sensibilität aufweisen (anders als beispielsweise Gesundheitsdaten) und es zudem auch bei dem bloßen Kontrollverlust über die Daten und die hiernach von der Klägerin erlittenen Befürchtungen geblieben ist. Zu einer darüber hinausgehenden

Schädigung der Klägerin ist es nicht gekommen. Des Weiteren zeigen auch die Ausführungen der Klägerin, dass ihre Befürchtungen im Hinblick auf die missbräuchliche Verwendung ihrer Daten nicht so groß waren, dass sie deshalb die mit einem Wechseln der Telefonnummer verbundenen Unannehmlichkeiten in Kauf genommen hätte.

Nach Abwägung dieser Gesichtspunkte erachtet das Gericht einen immateriellen Schadensersatz in Höhe von 250,00 EUR für erforderlich, aber auch ausreichend.

Der Zinsanspruch folgt insoweit aus §§ 288, 291 BGB.

2. Antrag zu Ziffer 2.
Der unter Ziffer 2. gestellte Antrag ist nach der Klarstellung der Klägerin in der Replik dahingehend auszulegen, dass er sich auf zukünftige materielle Schäden beschränkt. Der Antrag ist indes unzulässig, da dem Antrag das nach § 256 Abs. 1 ZPO erforderliche Feststellungsinteresse fehlt. Ein Feststellungsantrag ist bereits dann zulässig, wenn die Schadensentwicklung noch nicht gänzlich abgeschlossen ist und der Kläger aus diesem Grund nicht imstande ist, seinen Anspruch vollständig zu beziffern. Das Feststellungsinteresse ist daher nur dann zu verneinen, wenn aus Sicht des Geschädigten keinerlei Besorgnis besteht, zumindest mit dem Eintritt eines Schadens zu rechnen (BGH, Beschl. v. 09.01.2007 – VI ZR 133/06, NJW-RR 2007, 601). Das ist vorliegend der Fall. Die Klägerin hat im Rahmen der persönlichen Anhörung berichtet, dass sie durch die Veröffentlichung ihrer Daten bislang keine materiellen Schäden erlitten habe. Es kann zwar nicht ausgeschlossen werden, dass der Klägerin bereits ein materieller Schaden zugefügt wurde, ohne dass sie hiervon bereits Kenntnis erlangt hat. Die Wahrscheinlichkeit eines Schadens infolge des Scraping-Vorfalls ist jedoch umso unwahrscheinlicher, je länger der Vorfall zurückliegt. Es ist daher davon auszugehen, dass mit dem Eintritt eines materiellen Schadens nicht zu rechnen ist (s. auch OLG Dresden, Endurt. v. 05.12.2023 – 4 U 709/23, GRUR-RS 2023, 36707 Rn. 39; OLG Hamm, Urt. v. 15.08.2023 – I-7 U 19/23, juris Rn. 215 ff.).

3. Anträge zu Ziffer 3.
Die unter Ziffer 3. gestellten Anträge sind unzulässig.

a.

Der Antrag zu Ziffer 3 a) beinhaltet eine verdeckte Leistungsklage, da die Klägerin hier letztlich ein aktives Tun – nämlich die zukünftige Freischaltung der Kontaktimportfunktionen nur unter Einhaltung ausreichender Sicherungsvorkehrungen – verlangt. Die Klage enthält daher mit der geforderten Androhung nach § 890 Abs. 2 ZPO ein unzulässiges Antragsbegehren, da die Titulierung einer Handlungsverpflichtung grundsätzlich nur nach § 887 ZPO in Betracht kommt, nicht aber nach § 890 ZPO.

Der Antrag ist ferner nicht hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO. Hiernach darf ein Unterlassungsantrag 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. Aus diesem Grund sind Unterlassungsanträge, die lediglich den Wortlaut eines Gesetzes wiederholen, grundsätzlich als zu unbestimmt und damit als unzulässig anzusehen. Abweichendes kann gelten, wenn der gesetzliche Verbotstatbestand eindeutig und konkret gefasst ist, sein Anwendungsbereich durch eine gefestigte Auslegung geklärt ist oder der Kläger hinreichend deutlich macht, dass er kein Verbot im Umfang des Gesetzeswortlauts beansprucht, sondern sich mit seinem Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert (vgl. BGH, Urt. v. 26.01.2017 – I ZR 207/14 –, juris Rn. 18; OLG Dresden, Endurt. v. 05.12.2023 – 4 U 709/23, GRUR-RS 2023, 36707 Rn. 43; OLG Hamm, Urt. v. 15.08.2023 – I-7 U 19/23, juris Rn. 230). Unter Anwendung dieser Grundsätze ist der Antrag zu Ziffer 3 a) nicht hinreichend bestimmt. Der Antrag beschränkt sich letztlich auf die (teilweise) Wiedergabe des Gesetzes, ohne den Anspruch hinreichend zu individualisieren. Es bleibt völlig unklar, wie etwa geklärt werden soll, wodurch ein „angemessenes Schutzniveau“ gewährleistet werden soll, was nach dem Stand der Technik mögliche Sicherheitsmaßnahmen sind, mit denen die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern ist. Darüber hinaus ist nicht ersichtlich, welche Pflichten die Beklagte konkret zur Erfüllung ihrer Pflicht zu ergreifen hat.

b.

Der Antrag zu Ziffer 3 b) ist ebenfalls unzulässig. Insoweit fehlt es schon an einem Rechtsschutzbedürfnis der Klägerin. Denn der Antrag ist darauf gestützt, der

Beklagten die Weiterverarbeitung ihrer Telefonnummer auf der Grundlage einer für unwirksam erachteten Einwilligung zu untersagen. Diesem Begehren kann aber durch Widerruf dieser Einwilligung jederzeit Rechnung getragen werden. Angesichts des Umstandes, dass der Unterlassungsanspruch insoweit auch ausdrücklich mit der möglichen Verwendung der Telefonnummer über das Kontaktimporttool begründet wird, dieses Tool aber spätestens seit Oktober 2019 nicht mehr besteht, ist jedenfalls ein Rechtsschutzbedürfnis für einen in die Zukunft gerichteten Unterlassungsantrag nicht mehr zu erkennen (OLG Dresden, Urt. v. 05.12.2023 – 4 U 709/23, GRUR-RS 2023, 36707).

4. Antrag zu Ziffer 4.
Die mit dem Antrag zu Ziffer 4. verfolgte Leistungsklage auf Auskunftserteilung ist zulässig, aber unbegründet.

Nach Art. 15 Abs. 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und bestimmte weitere Informationen. Gemäß Art. 15 Abs. 3 Satz 1 DSGVO stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Die Auskunftserteilung mittels Fernzugriffs auf ein elektronisches Auskunftssystem des Datenverantwortlichen genügt hierbei den an die Auskunftserteilung zu stellenden formellen Anforderungen (OLG Dresden, Endurt. v. 05.12.2023 – 4 U 709/23, GRUR-RS 2023, 36707 Rn. 52). Ein Auskunftsanspruch ist erfüllt, 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 allein die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (vgl. BGH, Urt. v. 03.09.2020 – III ZR 136/18, GRUR 2021, 110 Rn. 43; OLG Dresden, Endurt. v. 05.12.2023 – 4 U 709/23, GRUR-RS 2023, 36707 Rn. 52; OLG Hamm, Urt. v. 15.08.2023 – I-7 U 19/23, juris Rn. 250).

Unter Anwendung dieser Maßstäbe ist Erfüllung eingetreten. Das anwaltliche Antwortschreiben vom 13.02.2023 enthält eine Auflistung der Datenpunkte und der Telefonnummer, eine Erläuterung des Datenabrufs über die immer öffenltichen Daten, das Facebook-Profil und die Kontaktimportfunktion, die zeitliche Angabe „im Zeitraum bis September 2019“, den Hinweis, dass der Beklagten keine Rohdaten zu den abgerufenen Daten vorliegen, und den Hinweis auf das Handeln mehrerer Scraper, nicht eines Scrapers mit Blick auf die Frage nach der konkreten Person. Es wird hinreichend deutlich, dass die Beklagte zur Identität der Scraper und zum genauen Zeitpunkt des die Klägerin betreffenden Scrapings machen kann.

II.
Die Nebenentscheidungen folgen aus §§ 92 Abs. 1, 708 Nr. 11, 711 ZPO.

Streitwert: bis 7.000,00 EUR

Rechtsbehelfsbelehrung:

Gegen die Streitwertfestsetzung ist die Beschwerde an das Landgericht Duisburg statthaft, wenn der Wert des Beschwerdegegenstandes 200,00 EUR übersteigt oder das Landgericht die Beschwerde zugelassen hat. Die Beschwerde ist spätestens innerhalb von sechs Monaten, nachdem die Entscheidung in der Hauptsache Rechtskraft erlangt oder das Verfahren sich anderweitig erledigt hat, bei dem Landgericht Duisburg, König-Heinrich-Platz 1, 47051 Duisburg, schriftlich in deutscher Sprache oder zur Niederschrift des Urkundsbeamten der Geschäftsstelle einzulegen. Die Beschwerde kann auch zur Niederschrift der Geschäftsstelle eines jeden Amtsgerichtes abgegeben werden. Ist der Streitwert später als einen Monat vor Ablauf dieser Frist festgesetzt worden, so kann die Beschwerde noch innerhalb eines Monats nach Zustellung oder formloser Mitteilung des Festsetzungsbeschlusses eingelegt werden.

Hinweis zum elektronischen Rechtsverkehr:
Die Einlegung ist auch durch Übertragung eines elektronischen Dokuments an die elektronische Poststelle des Gerichts möglich. Das elektronische Dokument muss für die Bearbeitung durch das Gericht geeignet und mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg gemäß § 130a ZPO nach näherer Maßgabe der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere

elektronische Behördenpostfach (BGBl. 2017 I, S. 3803) eingereicht werden. Auf die Pflicht zur elektronischen Einreichung durch professionelle Einreicher/innen ab dem 01.01.2022 durch das Gesetz zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013, das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017 und das Gesetz zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten und zur Änderung weiterer Vorschriften vom 05.10.2021 wird hingewiesen.
Weitere Informationen erhalten Sie auf der Internetseite www.justiz.de.