Beglaubigte Abschrift

Landgericht Hof

Az.: 33 O 99/22

IM NAMEN DES VOLKES

In dem Rechtsstreit

[redacted]
- Klägerin -

Prozessbevollmächtigte:
Rechtsanwälte **WBS.LEGAL Wilde Beuger Solmecke Rechtsanwälte Partnerschaft mbB**, WBS.LEGAL, Eupener Straße 67, 50933 Köln, [redacted]

gegen

Meta Platforms Ireland Ltd., vertreten durch d. 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, [redacted]

wegen Schadensersatz, Unterlassung, Auskunft durch Verletzung von Persönlichkeitsrechten

erlässt das Landgericht Hof - 3. Zivilkammer - durch die Richterin am Landgericht [redacted] als Einzelrichterin aufgrund der mündlichen Verhandlung vom 01.09.2023 folgendes

Endurteil

1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in Höhe von 500,00 EUR nebst Zinsen hieraus seit 10.05.2022 in Höhe von 5 Prozentpunkten über dem Basiszinssatz zu bezahlen.

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, noch entstehen

werden.

3. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 159,94 € zuzüglich Zinsen hieraus seit 10.05.2022 in Höhe von 5 Prozentpunkten über dem Basiszinssatz zu zahlen.

4. Im Übrigen wird die Klage abgewiesen.

5. Von den Kosten des Rechtsstreits trägt die Beklagte 14,3 % und die Klagepartei 85,7 %.

6. Das Urteil ist jeweils vorläufig vollstreckbar, wobei die Vollstreckung gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrags abgewendet werden kann, wenn nicht die Gegenseite vor der Vollstreckung Sicherheit in selbiger Höhe leistet.

Beschluss

Der Streitwert wird auf 7.000,00 € festgesetzt.

Tatbestand

Die Parteien streiten um Ansprüche auf Schadensersatz, Unterlassung und Auskunft sowie Erstattung der vorgerichtlichen Rechtsanwaltskosten wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung (DSGVO).

Die Beklagte ist die Betreiberin der Webseite www.facebook.com und der Dienste auf dieser Seite für Nutzer in der Europäischen Union (nachfolgend: Facebook). Die angebotenen Dienste ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Die Klagepartei ihrerseits ist Nutzer/in der Plattform „Facebook“ und nutzt die Dienste insbesondere, um mit Freunden zu kommunizieren, zum Teilen privater Fotos und für Diskussionen mit anderen Nutzern.

Im Jahr 2019 (nachfolgend: relevanter Zeitraum) wurden von unbekannten Dritten personenbezogene Daten von ca. 533 Millionen Facebook-Nutzern/Nutzerinnen (im folgenden zur leichteren Lesbarkeit nur: Nutzer) aus 106 betroffenen Ländern aus dem Datenbestand von Facebook abgeschöpft („gescrapt“) und im Jahr 2021 im Darknet öffentlich verbreitet. Die „abgegriffenen“ Daten wurden dabei auf Seiten veröffentlicht, die illegale Aktivitäten begünstigen sollen, beispielsweise

auf der Seite raidforums.com, einem Hackerforum, das unter anderem dafür verrufen ist, dass illegal abgeschöpfte Daten hinterlegt und ausgetauscht werden. Die genaue Vorgehensweise der „Scraper“ ist nicht bekannt. Der Scraping-Sachverhalt wird von den Parteien daher unterschiedlich interpretiert. Die Beklagte geht davon aus, dass mithilfe der sog. „Kontakt-Importer-Funktion“ (“Contact-Import-Tool“) Kontakte hochgeladen wurden, die Telefonnummern von Nutzern enthielten, um festzustellen, ob die Nummern mit einem Facebook-Konto verbunden sind. Soweit dies der Fall war, wurden öffentlich einsehbare Informationen aus dem betreffenden Nutzerprofil kopiert und mit der Telefonnummer verbunden. Dieses Datenpaket wurde dann im Internet weiter verbreitet. Die Klagepartei war bzw. ist vom „Datenscraping“ betroffen.

Bei der Erstregistrierung auf der Seite „Facebook“ muss jeder Nutzer bestimmte Informationen angeben, die als Teil seines Nutzerprofils immer öffentlich einsehbar sind. Beim Anlegen des Facebook-Profils muss der künftige Nutzer zudem den Datenschutz- und Cookie-Richtlinien der Beklagten zustimmen; diese sind durch eine Verlinkung getrennt abrufbar (vgl. Klage Seite 9).

Zu den „immer öffentlich“ einsehbaren Nutzerinformationen gehören Name, Geschlecht, Nutzername, Nutzer-ID, Profilbild, Titelbild und Netzwerke. Nach den Vor- bzw. Standardeinstellungen können „alle“ Personen sehen, welche Seiten der „neue“ Nutzer abonniert hat oder mit wem er befreundet ist. Auch ist für alle Informationen, die der „neue“ Nutzer in sein Profil einträgt, standardmäßig „öffentlich“ als Voreinstellung ausgewählt.
Hinsichtlich der nicht zwingend „immer öffentlichen“ Informationen bzw. Datensätze kann der Nutzer selbst entscheiden, inwieweit er sie öffentlich einsehbar machen möchte. Zu diesen Daten gehören Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse.
So kann über die sog. „Zielgruppenauswahl“ festgelegt werden, *wer* die Datenelemente im Profil des Nutzers sehen kann. Über die Möglichkeit der sog. „Suchbarkeits-Einstellungen“ wird festgelegt, ob das Profil eines Nutzers beispielsweise anhand der Telefonnummer gefunden werden kann. Soweit der Nutzer keine individuellen Einstellungen wählt, richtet sich die Einsehbarkeit seiner Informationen nach den Standard-Einstellungen.
Die „Suchbarkeits-Einstellung“ der Klagepartei war hinsichtlich der Telefonnummer im relevanten Zeitraum jedenfalls auf „öffentlich“ eingestellt.
Wählt der Nutzer keine individuellen Einstellungen, wie zum Beispiel die Zielgruppenauswahl „Freunde“, so richtet sich die Einsehbarkeit seiner Informationen nach den jeweiligen standardisierten Voreinstellungen, die wiederum abhängig sind vom jeweiligen Datensatz (z.B. „Freunde“ beim Datensatz Telefonnummer).

Neben den gewöhnlichen Funktionen auf der Facebook-Website wird von der Beklagten noch ei-

ne Messenger-App für das Smartphone betrieben, die als Schnittstelle für die Facebook-Applikation arbeitet und Nutzern die Möglichkeit eröffnet, sich gegenseitig Nachrichten zu schicken. Die Nutzer melden sich dafür mit ihren bestehenden Facebook-Profilen an. Die Messenger-App und die gewöhnlichen Funktionen von Facebook sind über denselben Zugang zum Nutzerkonto verknüpft.

Mit vorgerichtlichem Schreiben vom 14.06.2021 (Anlage K1) forderte die Klagepartei die Beklagte zur Zahlung von Schadensersatz nach Art. 82 Abs. 1 DSGVO sowie zur Unterlassung zukünftiger Zugänglichmachung ihrer Daten an unbefugte Dritte sowie zur Auskunftserteilung darüber, welche konkreten Daten abgegriffen und veröffentlicht wurden. Auf das klägerische Auskunftsersuchen antwortete die Beklagte und erteilte dem klägerischen Bevollmächtigten Auskunft in einem bestimmten Umfang (vgl. Anlagen K2 und B 16).

Die Klagepartei behauptet, Opfer des Verstoßes der Beklagten gegen zahlreiche Vorschriften der Datenschutzgrundverordnung geworden zu sein, wodurch ihr ein Schaden entstanden sei.

Die Klagepartei behauptet zum Scraping-Vorfall, dass Telefonnummern der Nutzer wegen einer Sicherheitslücke mit den restlichen Personendaten korreliert worden seien und damit Bestandteil der unbefugt verbreiteten Datensätze geworden seien. Es sei eine Vielzahl von Kontakten durch die Scraper in ein virtuelles Adressbuch eingegeben worden, wodurch es gelungen sei, die Telefonnummern konkreten Profilen zuzuordnen, ohne dass die Telefonnummern öffentlich freigegeben gewesen seien. Unter anderem seien Telefonnummern aus vorherigen Leaks, auch bei der Beklagten, verwendet worden (Replik S. 9). Mithilfe des Contact-Import-Tools (= CIT) sei jede fiktive Nummer geprüft und der zugehörige Facebook-Nutzer angezeigt worden. Dieser sei dann in seinem Profil besucht worden, die öffentlichen Daten seien abgeschöpft worden. Möglich sei dies deshalb gewesen, weil die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten Tools zu verhindern (Klage S. 23, 33 ff.). Dieses Tool verstoße gegen die DSGVO.

Neben der Telefonnummer, der Nutzer-ID, dem Namen und dem Geschlecht der Nutzer seien auch das Bundesland, das Land, die Stadt, der Beziehungsstatus und weitere personenbezogene Daten, wie zum Beispiel der Arbeitgeber, abgegriffen worden (Klage S. 6 und Replik S. 11).

Die Klagepartei trägt vor, dass die Einstellungen zur Sicherheit der Telefonnummer auf der Facebook-Seite so undurchsichtig und kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne (Klage S. 8 ff.). Gerade Sicherheit und Vertraulichkeit der

Telefonnummer seien für den Nutzer, so auch für die Klagepartei, von besonderer Wichtigkeit, insbesondere wenn die Telefonnummer zur „Zwei-Faktor-Authentifizierung“ im Registrierungsprozess genutzt werde. Im Datenmanagement bei Facebook werde die Telefonnummer auch gesondert behandelt. Es werde betont, dass standardmäßig nur der Nutzer diese einsehen könne (Klage S. 14 f.). Es werden nicht erwähnt, dass die Telefonnummer dazu verwendet werden könne, das Profil des Nutzers zu identifizieren. Die Einstellungsoption der „Suchbarkeit“ sei nicht zu erreichen, wenn nach den Einstellungsmöglichkeiten für die Telefonnummer gesucht werde. So habe es die Beklagte Unbekannten ermöglicht, die Telefonnummern der Nutzer zu identifizieren, obwohl diese geheim gehalten werden sollten. Für einen tatsächlich wirksamen Schutz hätten gleichzeitig viele Einstellungen geändert werden müssen, ohne dass dazu ausreichende Information oder Voreinstellung gewährleistet gewesen sei (Klage S. 22).

Die Klagepartei ist der Ansicht, die Beklagte verstoße gegen die Datenschutzgrundverordnung (= DS-GVO), indem sie ohne ausreichende Grundlage im Sinne der Art. 6 und 7 DS-GVO Informationen im Sinne von Art. 13, 14 DS-GVO verarbeite, Daten unbefugten Dritten zugänglich mache, sowie die Rechte der Nutzer aus Art. 15, 17 und 18 DS-GVO verletze.

Es läge bereits beim Registrierungsprozess ein Verstoß gegen die Grundsätze des nutzerfreundlichen Datenschutzes und das in der DS-GVO niedergelegten Prinzip der Datenminimierung und des „privacy by default“ (= datenschutzfreundliche Voreinstellungen) vor. Alle Informationen, die der Nutzer bei der Registrierung in sein Profil einträgt, sind standardmäßig mit der Voreinstellung „öffentlich“ belegt; aufgrund der Vielzahl an Einstellungsmöglichkeiten (näher dargestellt Klage S. 8-12), der schwer verständlichen Informationen und unklaren Angaben sei mit hoher Wahrscheinlichkeit zu erwarten, dass der Nutzer beim Registrierungsprozess diese voreingestellte Standardeinstellung „öffentlich“ beibehalte und nicht selbstständig ändere. Entgegen der Auffassung der Beklagten seien Informationen über die Verarbeitung der personenbezogenen Daten auf der Facebook-Plattform in einem Wirrwarr von Untermenüs bzw. Unterpunkten und Marketingssprache nur schwer zu finden.
Die Folge der standardmäßigen Voreinstellungen „öffentlich“ sei, dass auch die bei der Registrierung angegebene Telefonnummer öffentlich verfügbar sei. Facebook versichere insofern jedoch: „Nur du kannst deine Nummer sehen.“ (siehe Klage S. 15), was der Nutzer nur so verstehen könne, dass der Einsatz der Telefonnummer zu Sicherheitszwecken die Datensicherheit nicht weiter kompromittiere und dass durch die Angabe der Telefonnummer Dritte keine weiteren Informationen erlangen können. Auch die weiteren zur Verfügung gestellten Informationen unter dem anklickbaren Feld „Mehr dazu“ würden daran nichts ändern, denn die dort verfügbare Information „Möglicherweise verwenden wir deine Mobilnummer für diese Zwecke: ...“ (vgl. Klage S. 16) sei

uneindeutig und irreführend. Die Telefonnummer sei deshalb im Vertrauen und mit dem Ziel, mehr persönliche Sicherheit zu erreichen, auf der Plattform preisgegeben worden. Entgegen der Erwartung und für den Nutzer nicht erkennbar, seien Telefonnummern ohne den Einsatz weiterer Sicherungsmaßnahmen durch die Beklagte in großem Umfang unbekannten Dritten zugänglich gemacht worden.

Das Contact-Importer-Tool (= CIT) der Beklagten verstoße gegen die Vorschriften der DS-GVO (Replik S. 6 ff.).

Der Klagepartei sei durch die unbefugte Veröffentlichung ihrer personenbezogenen Daten ein Schaden entstanden, der darin bestehe, dass ein erheblicher Kontrollverlust über die eigenen Daten entstanden sei, der zu einem Zustand großen Unwohlseins und Sorge über möglichen Missbrauch der Daten geführt habe. Die Klagepartei habe seit April 2021 vermehrt dubiose E-Mails und SMS-Nachrichten von unbekannten Adressen und Nummern erhalten (Klage S. 24).

Die Klagepartei wirft der Beklagten darüber hinaus vor, dass nach dem Vorfall aus dem Jahr 2019 zu keiner Zeit eine Information darüber erfolgt sei, dass Daten durch Dritte entwendet und veröffentlicht wurden.

Das Auskunftsschreiben der Beklagten vom 23.08.2021 sei jedenfalls nicht ausreichend gewesen. Eine konkrete Auskunft zum „Datenschutz-Vorfall“ habe es nicht gegeben (Replik S. 30).

Die Klägerin 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 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 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 887,03 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt (Bl. 77 d.A.),

die Klage abzuweisen.

Die Beklagte vertritt zunächst die Auffassung, dass die Klage weitgehend unzulässig sei. Der Klageantrag zu Ziffer 1) sei nicht hinreichend bestimmt i.S.d. § 253 Abs. 2 Nr. 2 ZPO. Die Klagepartei macht *einen* Zahlungsantrag geltend, stütze ihre Begehr jedoch auf zwei zeitlich auseinanderfallende angebliche Verstöße und damit auf unterschiedliche Lebenssachverhalte, ohne weiter zu differenzieren. Die Klageanträge zu Ziffer 2) und 3) seien zu unbestimmt, die Klagepartei habe zudem kein Feststellungsinteresse gem. § 256 Abs. 2 ZPO dargelegt. Hinsichtlich der

Einzelheiten wird Bezug genommen auf die Klageerwiderung S. 39 ff. (Bl. 114 d.A.).

Zur Begründetheit trägt die Beklagte folgendes vor:

Die Privatsphäre-Einstellungen zur Bestimmung der Einsehbarkeit der Nutzerdaten seien entgegen der Behauptung der Klagepartei - auch schon im relevanten Zeitraum - im Haupteinstellungsmenü der Facebook-Startseite nach dem Anmelden klar und leicht zu finden (vgl. Klageerwiderung S. 15/16). Die im Facebook-Konto gewählten Einstellungen zur Zielgruppenauswahl und zur Suchbarkeit würden auch in der Messenger-App übernommen. Beide Einstellungen seien nicht unabhängig voneinander. Über die zur Verfügung stehenden Privatsphäre-Einstellungen seien die Nutzer umfangreich und verständlich informiert worden; die Formulierungen seien weder uneindeutig noch irreführend (Einzelheiten Klageerwiderung S. 17ff.).

Im Zuge des stattgefundenen Scraping-Sachverhaltes seien nur solche Daten - auch der Klagepartei - von der Facebook-Plattform abgegriffen worden, die entweder „immer öffentlich“ zugänglich waren oder solche, die entsprechend der Zielgruppenauswahl des Nutzers öffentlich einsehbar waren. Im Falle der freiwilligen Hinzufügung einer Telefonnummer zum Profil sei die Standardeinstellung „Freunde“ gewesen; die Telefonnummer sei also nur für Freunde des Nutzers sichtbar gewesen (Klageerwiderung S. 14/15).
Bei dem stattgefundenen „Scraping-Sachverhalt“ handele es sich deshalb nicht um eine Sicherheitsverletzung; das Abrufen der Daten beruhe nicht auf einem Datenschutzverstoß (Einzelheiten Klageerwiderung S. 23 ff.). Die Daten seien gerade nicht durch Hacking, also infolge Eindringens unter Überwindung von Zugriffsschranken wegen einer Schwachstelle im Sicherheitssystem der Beklagten erlangt worden, sondern vielmehr durch das massenhafte automatisierte Sammeln öffentlich einsehbarer Daten durch Dritte. Das Ausmaß des Abrufes der jeweiligen Nutzerdaten hänge damit auch davon ab, welche Daten des Nutzers öffentlich waren. Scraping, also der Abruf von öffentlich einsehbaren Daten unter Verwendung der für die ordnungsgemäße Nutzung vorgesehenen Funktionen, sei allgegenwärtig im Internet und trotz des bestehenden Verbotes durch die Nutzungsbedingungen der Facebook-Plattform nicht völlig zu verhindern.

Entgegen der Behauptung der Klagepartei seien bei dem „Scraping-Vorfall“ die Telefonnummern gerade nicht von den Nutzer-Profilen abgerufen worden, sondern von den Scrapern in einem Prozess der sogenannten Telefonnummeraufzählung bereitgestellt worden (Klageerwiderung S. 27 und 36). Über die Kontakt-Importer-Funktion seien seitens der Scraper Kontakte mit möglichen Telefonnummern hochgeladen worden, um festzustellen, ob diese Nummern mit einem Facebook-Konto verbunden sind. Sei eine solche Verbindung festgestellt worden, seien die öffentlich

einsehbaren Informationen (in Übereinstimmung mit der Zielgruppenauswahl des Nutzers) aus dem betreffenden Nutzerprofil kopiert und die Telefonnummer den abgerufenen, öffentlich einsehbaren Daten hinzugefügt worden (Klageerwiderung S. 27/28).
Angesichts dessen, dass bei dem beschriebenen Sachverhalt keine Verletzung des Schutzes personenbezogener Daten vorliege, sei die Beklagte auch nicht verpflichtet gewesen, die Nutzer über diesen Scraping-Sachverhalt zu informieren. Dennoch habe die Beklagte Maßnahmen zur Information ergriffen.

Die Beklagte behauptet weiter, dass sie im relevanten Zeitraum Anti-Scraping-Maßnahmen ergriffen gehabt habe. Es seien Übertragungsbeschränkungen implementiert gewesen, die die Anzahl von Anfragen von bestimmten Daten reduzieren, die pro Nutzer oder von einer bestimmten IP-Adresse in einem bestimmten Zeitraum gestellt werden können. Die Beklagte habe auch sog. „Captcha“-Abfragen (= „Completely Automated Public Turing Test to tell Computers and Humans Apart“; auf Deutsch: Vollständig automatisierter öffentlicher Turing-Test, um Computer von Menschen zu unterscheiden) genutzt. Scraping sei dennoch nicht immer zu verhindern. Ergänzend wird auf die Ausführungen in der Klageerwiderung, S. 29-32, Bezug genommen.

Entgegen der Behauptung der Klagepartei sei sie auf ihr Auskunftsverlangen hin auch am 09.09.2022 ausführlich und individuell informiert worden (Verweis auf Anlage B 16).

Die Beklagte bestreitet das Vorliegen eines Schadens der Klägerin. Weil lediglich die öffentlich zugänglichen Daten der Klägerin abgegriffen worden seien und anderweitig im Internet erneut veröffentlicht wurden, sei eine signifikante Auswirkung auf das Risiko von Cyberkriminalität nicht gegeben. Diesem Risiko sei jede im Internet aktive Person ohnehin ausgesetzt (Einzelheiten Klageerwiderung S. 36). Die Behauptung eines erheblichen Kontrollverlustes über Daten sowie des Zustandes großen Unwohlseins und großer Sorge über möglichen Missbrauch selbiger sei weder hinreichend substantiiert noch in irgendeiner Art belegt. Ein eventueller Kontrollverlust sei der Beklagten außerdem nicht zuzurechnen.

Zur Ergänzung des Parteivortrages wird Bezug genommen auf die eingereichten Schriftsätze der Parteivertreter nebst Anlagen sowie auf das Protokoll der mündlichen Verhandlung vom 01.09.2023.

Entscheidungsgründe

Die - bis auf Klageantrag Ziffer 3. a. und b. - in zulässiger Art und Weise erhobene Klage ist im Umfang der Anträge 1., 2. und 5. begründet, im Übrigen unbegründet.

A. Zulässigkeit der Klage

Die Klage ist zulässig. Die Anwendbarkeit deutschen Rechts folgt aus Art. 6 Abs. 1 VO (EG) 593/2008 (Rom I-VO).

I.) Das angerufene Landgericht Hof ist international, sachlich und örtlich zuständig. Es kommt die EuGVVO gemäß deren Art. 1 Abs. 1 zur Anwendung. Ein ausschließlicher Gerichtsstand gemäß Art. 24 EuGVVO ist hier nicht ersichtlich. Gemäß Art. 18 Abs. 1, 2. Alt. EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner vor dem Gericht des Ortes erhoben werden, an dem der Verbraucher seinen Wohnsitz hat. Letzteres ist im Hinblick auf den Wohnsitz der Klagepartei im Bezirk des angerufenen Gerichtes der Fall. Die örtliche Zuständigkeit folgt weiter aus dem besonderen Gerichtsstand des Art. 79 Abs. 2 S. 2 DS-GVO, § 44 Abs. 1 S. 2 BDSG im Hinblick auf den Wohnsitz der Klagepartei im hiesigen Gerichtsbezirk. Die sachliche Zuständigkeit folgt aus §§ 23 Nr. 1, 71 Abs. 1 GVG, da der Streitwert über 5.000,00 EUR beträgt.

II.) Die Klage wurde - bis auf die unter Ziffer 3. gestellten Anträge - ordnungsgemäß gemäß § 253 ZPO erhoben.

1.) Der Klageantrag zu 1. ist nicht unbestimmt. Zur Bemessung des Schmerzensgeldes ist eine Größenordnung angegeben, die konkrete Höhe ist zulässigerweise in das Ermessen des Gerichts gestellt worden; die Berechnungs- bzw. Schätzgrundlagen sind auch ausreichend dargelegt worden (vgl. dazu Greger in Zöller, ZPO, 32. Aufl. 2018, § 253 ZPO, Rn. 14 f.). Soweit die Beklagte rügt, dass die Klagepartei ihr Begehren auf mehrere zeitlich auseinanderfallende angebliche Verstöße gegen die DS-GVO stützt, zum einen nämlich auf die dem „Scraping-Vorfall“ im Jahr 2019 vorgelagerten angeblichen Verstöße der Beklagten und zum anderen auf die Verletzung von nachgelagerten Benachrichtigungspflichten, macht dies den Klageantrag nicht unzulässig. Denn letztlich ist darin ein einheitlicher, wenn auch zeitlich auseinandergezogener Lebensvorgang zu sehen, für den die Klagepartei Schadensersatz begehrt. Zu prüfen ist aufgrund des klägerseitigen Vorbringens, ob die Beklagte im Vorfeld des Scraping-Vorfalls lediglich unzureichende (oder keine) Datenschutzvorkehrungen getroffen hat, und ob sie danach ihre Nutzer nur

unzureichend bzw. intransparent informiert hat, wodurch sich der behauptete immaterielle Schaden noch intensiviert haben könnte (so auch entschieden vom LG Aachen, Urteil 26.05.2023, 8 O 267/22, Rn. 37 unter Verweis auf LG Essen, Urteil 10.11.2022, 6 O 111/22; LG Limburg, Urteil 14.04.2023, 1 O 171/22, Rn. 17). Gegenständlich ist mithin das Verhalten der Beklagten im Zusammenhang mit dem konkret beschriebenen Scraping-Vorfall aus 2019, der mit der Nichteinhaltung der notwendigen technischen Sicherheitsvorkehrungen begonnen und mit der unzureichenden Information der Betroffenen nach dem Vorfall endete (so Replik S. 35), so dass der Klagegegenstand hier hinreichend abgrenzbar und bestimmt ist.

2.) Auch hat die Klagepartei zu Antrag 2. ihr Feststellungsinteresse gemäß § 256 Abs. 2 ZPO hinreichend dargetan. Die bei der Beklagten im Jahr 2019 „abgegriffenen“ Datensätze sind noch immer im Darknet verfügbar, sodass zumindest nach der Behauptung der Klagepartei ein künftiger Schaden nicht ausgeschlossen ist. Ein Feststellungsantrag ist dann zulässig, wenn die Schadensentwicklung noch nicht abgeschlossen ist und die Klagepartei ihren Anspruch deshalb ganz oder teilweise nicht beziffern kann. Ein Feststellungsinteresse ist nur zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen. Bei den behaupteten Verstößen gegen die DS-GVO mit der behauptet dargelegten unkontrollierten Nutzung gescrapter Daten ist bei verständiger Würdigung zumindest nicht ausgeschlossen, dass irgendein materieller oder immaterieller Schaden entstehen könnte.

3.) Die unter Ziffern 3. a. und b. der Anträge erhobenen Unterlassungsklagen sind unzulässig, weil sie nicht hinreichend bestimmt sind. Denn der Beklagten ist insofern zuzugestehen, dass die Formulierung, die Beklagte habe die Zugänglichmachung personenbezogener Daten der Klägerseite zu unterlassen, ohne „die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen“, derart unklar und damit nicht hinreichend bestimmt ist, dass die Festlegung der konkret „möglichen Sicherheitsvorkehrungen“ - unzulässigerweise - in das Vollstreckungsverfahren verlagert würde (Klageerwiderung S. 43). Eine derartig weite Antragsformulierung kann nicht - auch nicht ausnahmsweise zur Gewährung effektiven Rechtsschutzes - hingenommen werden. An dieser Beurteilung ändert auch der Umstand nichts, dass es der Klagepartei nicht weiter möglich ist, die „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ näher aufzuzeigen. Aber auch das mit dem Klageantrag Ziffer 3. b. begehrte Anspruchsziel zur Unterlassung der Verarbeitung der Telefonnummer der Klagepartei, die „auf Grundlage einer Einwilligung wegen der unübersichtlichen oder unvollständigen Informationen durch die Beklagte erlangt wurde“, ist zu unbestimmt. Auch die Festlegung der beklagtenseits zu unterlassenden Verarbeitung einer bestimmten Telefonnummer würde die Prüfung, ob eine wirksame Grundlage für die Einwilligung -

ob nämlich aufgrund unübersichtlicher oder unvollständiger Information erteilt - in das Vollstreckungsverfahren verlagern.

4.) Die Zulässigkeit des Auskunftsanspruches - Ziffer 4. der Anträge - ergibt sich aus § 253 Abs. 2 Nr. 2 ZPO und wurde seitens der Beklagten nicht angegriffen.

B. Begründetheit der Klage

Die Klage ist im Hinblick auf die Anträge zu 1., 2. und 5. in dem, aus dem Tenor ersichtlichen Umfang begründet, im Übrigen ist sie unbegründet.

I.) Schadensersatzanspruch

Der Antrag Ziffer 1. ist im Umfang von 500 € begründet, soweit die Klagepartei immateriellen Schadensersatz wegen Datenschutzverstößen im Zusammenhang mit dem Scraping von Daten aus dem Jahr 2019 geltend macht. Denn es sind mehrere haftungsbegründende Verstöße der Beklagten gegen die einschlägigen Bestimmungen der DS-GVO zu bejahen.

1.) Das Gericht geht zunächst davon aus, dass im Zuge des sog. „Scraping“-Vorfalls jedenfalls die Datensätze Telefonnummer, Facebook-ID, Name und Geschlecht der Klagepartei durch die Scraper abgegriffen wurden. Die Beklagte rügte zwar, dass der Vortrag der Klägerseite zu den betroffenen Datensätzen zu ungenau sei und bestritt diesen daher. Nachdem die Klägerseite ihre Angaben in der Replik vom 10.11.2022 (siehe Bl. 175 d.A.) präzisierte und die Beklagte mehrfach darauf hinwies, dass ihr die genauen abgegriffenen Datensätze mangels Vorliegens einer Kopie der Rohdaten, die durch das Scraping abgerufen wurden, nicht bekannt sei, greift das Bestreiten der Beklagten nicht durch, sodass der diesbezügliche klägerseitige Vortrag als unstreitig zugrunde gelegt wird.
Unstreitig ist ferner, dass es sich bei den abgegriffenen Daten jeweils um solche handelte, die zum Zeitpunkt des Vorfalls auf „immer öffentlich“ einsehbar eingestellt waren. Hinsichtlich der Facebook-ID, des Namen und des Geschlechtes des Nutzers gilt dies in Folge unveränderlicher Voreinstellungen. Hinsichtlich der Telefonnummer der Klägerin war die öffentliche „Suchbarkeit“ - so die Überzeugung des Gerichtes - hingegen Folge einer unbeabsichtigten Einstellung des Nutzerkontos der Klägerin. Die in der mündlichen Verhandlung vom 01.09.2023 angehörte Klägerin vermittelte einen sehr verantwortungsbewussten und im Umgang mit ihren Daten auf Sicherheit bedachten Eindruck. Sie betonte, dass sie sich bei ihrer Erstregistrierung im Jahr 2008 durchaus

Gedanken über den Schutz ihrer Daten und über die Gefahren einer Internet-Präsenz gemacht habe (Protokoll 01.09.2023, S. 2 ff. = Bl. 398 d.A.). Die Sichtbarkeit ihrer Telefonnummer habe sie deshalb auf „privat“ eingestellt, insofern sei sie sich sicher. Dennoch habe sie später - nach dem „Scraping-Vorfall“ - festgestellt, dass die „Suchbarkeit“ ihrer Telefonnummer „öffentlich“ gewesen sei. Die Klägerin gab glaubhaft an, dass ihr die Differenzierung zwischen Sichtbarkeit und Suchbarkeit nicht bekannt gewesen sei. Das Gericht vermag dieser Argumentation ohne weiteres zu folgen, es hat an diesen Angaben der Klägerin keine Zweifel. Denn erst die Erläuterungen in der Klageerwiderung, dort Seite 13, *und* die Erörterung der verschiedenen Möglichkeiten der Profileinstellung im Rahmen der mündlichen Verhandlung vermochte die diffizilen Unterschiede greifbar deutlich zu machen. Aus sich heraus leicht verständlich ist die Differenzierung jedenfalls nicht. Hinzu kommt, wie aus der Abbildung Seite 16 der Klageerwiderung deutlich wird, dass unterschiedliche „Registerkarten“ gewählt werden müssen, um überhaupt Änderungen der Einstellungen vornehmen zu können. Neben den „Privatsphäre-Einstellungen und Tools“ mit Unterpunkten stehen auch die Menüpunkte „Allgemein“, „Sicherheit und Login“ sowie „Deine Facebook-Informationen“ zur Verfügung. Die Klagepartei hat in ihrer Klageschrift ab Seite 9 weitere Abbildungen eingefügt, die dem registrierungswilligen Nutzer als Information zur Verfügung gestellt werden. Aus diesen Abbildungen ergibt sich zwangslos, dass optimale Sicherheitseinstellungen für einen durchschnittlichen Nutzer ohne Zweifel eine Herausforderung darstellen. Es ist jedenfalls plausibel und gut nachvollziehbar, dass ein durchschnittlicher Nutzer beim Prozess der Erstregistrierung nicht bemerkt, dass seine Telefonnummer, obwohl er sie nicht preisgeben möchte, hinsichtlich der „Suchbarkeit-Einstellung“ auf öffentlich eingestellt ist und er damit von Dritten über eine Anfrage-Funktion (Kontakt-Import-Tool) über die Mobilfunknummer identifiziert werden kann.

2.) Soweit die Klagepartei ihre Telefonnummer im Rahmen der Registrierung zur „Zwei-Faktor-Authentifizierung“ angab, sollte dies jedoch gerade eine höhere Sicherheit gewährleisten. Die Registrierung sollte über einen, auf die Telefonnummer gesandten Code, abgeschlossen werden. Auf den Umstand, dass mit der Angabe der Telefonnummer ohne Vornahme entsprechender Privatsphäre-Einstellungen - in einem gesonderten Untermenü auf der Facebook-Seite - die Telefonnummer „öffentlich suchbar“ ist, nach der Diktion der Beklagten also „von Personen gesucht bzw. gefunden werden kann, die die Telefonnummer nicht im Profil des Nutzers sehen können“, wurde nicht hingewiesen. In der Verarbeitung der Telefonnummer im Rahmen der „Suchbarkeit“ liegt damit eine rechtswidrige Verarbeitung der Daten der Klagepartei durch die Beklagte.
Grundsätzlich gilt im Anwendungsbereich der DS-GVO, dass jede Datenverarbeitung rechtswidrig ist, wenn nicht eine der in Art. 6 DS-GVO genannten Bedingungen für eine rechtmäßige Daten-

verarbeitung erfüllt ist. Die rechtswidrige Datenverarbeitung kann sodann - wie hier - Schadensersatzansprüche nach Art. 82 DS-GVO auslösen (s. Albers/Veit in BeckOK Datenschutzrecht, Wolff/Brink, 42. Edition 01.11.2021, DS-GVO Art. 6, Rn. 115 m.w.N.).

3.) Vorliegend ist nicht festzustellen, dass die von der Beklagten vorgenommene Verarbeitung der Telefonnummer der Klägerseite zur Auffindbarkeit, also „Suchbarkeit“ durch Dritte rechtmäßig gewesen ist. Weder liegt eine wirksame Einwilligung nach Art. 6 Abs. 1a) DS-GVO dazu vor, noch war die Verarbeitung für die Erfüllung des zwischen den Parteien geschlossenen Vertrags erforderlich nach Art. 6 Abs. 1b) DS-GVO, noch ist festzustellen, dass die Verarbeitung zur Wahrung der berechtigten Interessen der Klägerseite oder von Dritten erforderlich war, Art. 6 Abs. 1f) DS-GVO.

a) Eine wirksame Einwilligung der Klagepartei in die Nutzung ihrer Mobilfunknummer für die Suchbarkeit durch Dritte liegt nicht vor. Wirksame Einwilligungen in Datenverarbeitungsvorgänge müssen nach Art. 4 Nr. 11 DS-GVO freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich, sowie durch Erklärung oder eine sonstige eindeutige bestätigende Handlung erfolgen. Stillschweigen oder vorausgewählte Buttons genügen diesen Anforderungen ebenso wenig wie sogenannte „Opt out“-Varianten zur Einholung einer Einwilligung (vgl. dazu z.B. BGH, Urteil 28.05.2020, I ZR 7/16, Rn. 31 ff. und Albers/Veit in BeckOK Datenschutzrecht, Wolff/Brink, 42. Edition 01.11.2021, DS-GVO Art. 6, Rn. 38). Denn in diesen Fällen kann nicht ausgeschlossen werden, es liegt aufgrund der Informationsdichte sogar nahe, dass der Nutzer die dem voreingestellten Ankreuzkästchen beigefügte Information gar nicht gelesen hat.

b) Aufgrund des im vorliegenden Fall festzustellenden Umstandes, dass die „Suchbarkeit“ für Dritte anhand der Telefonnummer des Nutzers auf „Alle“ voreingestellt war, kann das Vorliegen einer wirksamen Einwilligung in die Verarbeitung der Telefonnummer nicht bejaht werden. Insbesondere trägt die Beklagte nicht vor, dass und wie die Klägerseite in der erforderlichen *aktiven Weise* ihre Einwilligung zu der gegebenen Nutzung „Suchbarkeit der Telefonnummer“ erteilt hat. Es ist nicht vorgetragen oder sonst ersichtlich, dass die Klagepartei im Rahmen der Erstregistrierung eine entsprechende Einwilligung abgegeben hat, zumal sie hinsichtlich der Sichtbarkeit ihre Telefonnummer die einschränkende Auswahl „privat“ getroffen hatte. Zwar wurde die Klagepartei im Kontext der Erstregistrierung unstreitig auf die Nutzungsbedingungen und die Datenschutzrichtlinie der Beklagten hingewiesen, die sie auch akzeptiert hat. Dass damit, also im Akzeptieren dieser beiden Dokumente auch erklärt wird, dass Einverständnis mit der Freigabe der Telefonnummer im Rahmen der *Sucharbeit* besteht, behauptet die Beklagte selbst nicht. Selbst wenn je-

doch in den Nutzungsbedingungen oder der Datenschutzrichtlinie ein Hinweis auf die Verarbeitung der Telefonnummer als Suchbarkeits-Kriterium enthalten wäre, würde dies wiederum nicht den Anforderungen des Art. 4 Nr. 11 DS-GVO genügen: die Elemente, in die eingewilligt werden soll, müssen sich von anderen Sachverhalten klar unterscheiden (vgl. Albers/Veit in BeckOK Datenschutzrecht, Wolff/Brink, 42. Edition 01.11.2021, DS-GVO Art. 6, Rn 36). Gerade das war hier nicht der Fall, wie sich aus der glaubwürdigen Angabe der Klagepartei in der mündlichen Verhandlung ergab: ein Unterschied zwischen Sichtbarkeit und Suchbarkeit war der Klagepartei bei der Registrierung nicht bewusst. Die Vokabeln „Sichtbarkeit“ einerseits und „Suchbarkeit“ andererseits sucht man auf der Internetseite der Beklagten auch vergeblich.
Eine wirksame Einwilligung kann auch nicht daraus abgeleitet werden, dass dem Nutzer eine Vielzahl an Möglichkeiten zur Änderung der Voreinstellungen auf diversen Unterseiten der Internet-Plattform angeboten wird. Die DS-GVO verlangt nicht lediglich die Möglichkeit, Voreinstellungen *nachträglich* zu ändern, sondern sie fordert die aktive und eindeutige Einwilligung von Anfang an. Eine Einwilligung der Klagepartei von Anfang an lag hier nicht vor, sodass auch dahinstehen kann, ob die seitens der Beklagten angebotenen Möglichkeiten der nachträglichen Änderungen der Privatsphäre-Einstellungen hinreichend einfach und übersichtlich zu finden waren; diese reichen eben gerade nicht aus.

c) Die hier unstreitig im relevanten Zeitraum 2019 vorliegende „öffentliche“ Suchbarkeit des Profils der Klagepartei durch Dritte anhand der Telefonnummer war auch nicht für die Erfüllung des zwischen den Parteien geschlossenen Vertrags erforderlich, Art. 6 Abs. 1b) DS-GVO. Erforderlichkeit im Sinne der DS-GVO kann nicht schon dann angenommen werden, wenn die konkret in Frage stehende Datenverarbeitung für die Erfüllung des konkreten Vertrages nur irgendwie „nützlich“ oder „dienlich“ ist (Albers/Veit in BeckOK Datenschutzrecht, Wolff/Brink, 42. Edition 01.11.2021, DS-GVO Art. 6, Rn. 44 m.w.N.). Es muss vielmehr ein unmittelbarer Zusammenhang zwischen der Verarbeitung und dem konkreten Zweck des Vertragsverhältnisses bestehen (vgl. Albers/Veit in BeckOK Datenschutzrecht, a.a.O.). Die Beklagte hat hierzu nichts Sachdienliches vorgebracht. Insbesondere die Schilderung, wonach „Jane“ als neue Nutzerin isoliert wäre, wenn ihre Suchbarkeitseinstellung nicht auf „Alle“ vorkonfiguriert wäre (Klageerwiderung Seite 55 = Bl. 130 d.A.), überzeugt nicht.
Die öffentliche Suchbarkeit eines Nutzers anhand seiner Telefonnummer ist nicht essenziell für den Vertragszweck, der zwar auf Seiten der Beklagten darin besteht, möglichst viele Daten des Nutzers zu generieren, der andererseits aber auch darin besteht, dass der Nutzer diverse Beiträge auf der Plattform der Beklagten veröffentlicht, wozu nicht zwingend die Preisgabe der Telefonnummer des Nutzers erforderlich ist. Die Beklagte darf jedenfalls nicht durch die Beschreibung ih-

res Leistungsangebotes, nämlich „Menschen die Möglichkeit zu geben, Gemeinschaften zu bilden und die Welt näher zusammenzubringen“ (vgl. auch Klageerwiderung S. 55), die Nutzerinteressen hintanstellen und allein ihr Interesse an der Vermarktung der erlangten Daten in den Vordergrund rücken (ähnlich auch: BGH, Beschluss 23.06.2020, KVR 29/19, Rn. 110). Die Auffindbarkeit des Nutzerprofils anhand der hinterlegten Telefonnummer ist für die Vertragsabwicklung im Ergebnis höchstens nützlich, keinesfalls hingegen notwendig. Diese Würdigung wird auch unterstrichen durch die Tatsache, dass der Nutzer die Funktion der „öffentlichen“ Suchbarkeit in seinen Profileinstellungen deaktivieren kann, ohne dass die weitere Vertragsdurchführung hierdurch in Frage gestellt würde.

d) Darüber hinaus lässt sich auch nicht feststellen, dass die streitgegenständliche Datenverarbeitung der Telefonnummer der Klagepartei zur Wahrung ihrer berechtigten Interessen oder derer dritter Personen tatsächlich erforderlich war (Art. 6 Abs. 1f) DS-GVO). Die Beklagte schweigt hierzu.

e) Die Klagepartei erklärte in der mündlichen Verhandlung vom 01.09.2023 glaubhaft, dass sie die Privatsphäre-Einstellungen im Hinblick auf die *Suchbarkeit* ihrer Telefonnummer nicht auf „öffentlich“ gestellt hätte, wenn ihr die Trageweite dieser Einstellung bekannt gewesen wäre. Nach Bekanntwerden ihrer Betroffenheit vom „Scraping- Vorfall“ änderte sie die ihr dadurch erst bekannt gewordene Einstellung zur Suchbarkeit anhand der Telefonnummer auf „nicht-öffentlich“. Das Gericht vermag keinen Grund dafür zu erkennen, dass die Klagepartei diese Wahl - zur *Suchbarkeit* ihrer Telefonnummer - nicht schon bei dem Vorgang der Erstregistrierung getroffen hätte, wenn hierzu die Abgabe der Einwilligungserklärung im Sinne des Art. 6 Abs. 1 a) i.V.m. Art. 4 Nr. 11 DS-GVO abgefragt worden wäre. Denn bei der Anlegung ihres Nutzerprofils stellte sie ihre Telefonnummer auch nur auf „privat“ *sichtbar* ein.
Unter Zugrundelegung der Definition des „Scraping-Vorfalls“, wie ihn die Beklagte darstellt, wonach nämlich nur öffentlich zugängliche Datensätze von der Plattform der Beklagten abgegriffen wurden, wäre die Telefonnummer der Klagepartei bei entsprechender Einholung einer Einwilligung zur Verarbeitung der Telefonnummer im Rahmen der Sucharbeit nicht in die Hände der Scraper gefallen und hätte folglich auch nicht im Darknet veröffentlicht werden können. Die Klägerin hätte nämlich, hiervon ist das Gericht überzeugt, ihre Einwilligung zur öffentlichen Suchbarkeit ihrer Telefonnummer aktiv nicht erteilt.

4.) Darüber hinaus ist die Beklagte auch der ihr nach Art. 13 DS-GVO auferlegten Informations- und Aufklärungspflicht nicht in vollständigem Umfang nachgekommen. Die Beklagte hat die Kla-

gepartei zum Zeitpunkt der Erhebung des Datensatzes Mobilfunknummer nicht ausreichend über die Zwecke der Verarbeitung dieser Nummer aufgeklärt. Die Aufklärungspflicht kann nicht deshalb unterbleiben, weil sich ein Facebook-Nutzer freiwillig in die unendliche Weite des Internets begibt und dort seine Daten preisgibt.

a) Nach Art. 13 Abs. 1 c) DS-GVO war die Beklagte verpflichtet, die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, zum Zeitpunkt der Erhebung der Daten mitzuteilen. Die Mitteilung über die Zwecke der Verarbeitung ist für die Transparenz der Datenverarbeitung aus Sicht der betroffenen Person von entscheidender Bedeutung und steht im Zusammenhang mit dem Grundsatz der Zweckbindung, wonach personenbezogene Daten grundsätzlich nur für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen (vgl. Paal/Hennemann in Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Art. 13, Rn. 16 m.w.N.). Dieser Anforderung ist die Beklagte jedenfalls hinsichtlich der Verwendung der Mobilfunknummer für die von ihr verwendete „Kontakt-Importer-Funktion“ nicht hinreichend nachgekommen (so auch LG Stuttgart, Urteil 26.01.2023, 53 O 95/22, Rn. 58 ff.). Die Beklagte selbst beschreibt die „Kontakt-Importer-Funktion“ so: Kontakte können von einem Mobilfunkgerät auf Facebook hochgeladen werden, um sie dann auf der Facebook-Plattform zu finden und mit ihnen in Kontakt zu treten (Klageerwiderung S. 27). Die Beklagte ermöglicht einem Nutzer mit anderen Worten einen Abgleich der in seinem Smartphone gespeicherten Kontakte mit den auf Facebook registrierten Nutzerprofilen. Je nachdem, ob die Facebook-Profile mit einer „suchbaren“ Mobilfunknummer verknüpft sind, ist das Auffinden über die Telefonnummer möglich. Bei einer „öffentlichen“ Suchbarkeit der Telefonnummer kann jedermann über das „Kontakt-Importer-Tool“ mit dem Facebook-Nutzer in Verbindung treten.

b) Aus den vorgelegten Unterlagen ergibt sich nicht, dass insoweit eine ausreichende Aufklärung durch die Beklagte erfolgt ist. Insbesondere die im Rahmen der Klageerwiderung (Seite 20 = Bl. 95 d.A.) aufgezeigten Informationen über die Zwecke der Verarbeitung der Telefonnummer lassen eine verständliche und damit ausreichende Aufklärung nicht erkennen. Durch die Information „*Möglicherweise* verwenden wir deine Mobilnummer für diese Zwecke: … Um dir Personen, die du kennen könntest, vorzuschlagen, damit du dich mit ihnen auf Facebook verbinden kannst“ wird gerade ein gegenteiliger Eindruck erweckt, dass nämlich der Nutzer selbst „Freunde“ finden kann und nicht durch andere aufgrund der angegebenen Telefonnummer gefunden wird. Beim Nutzer wird der Eindruck erweckt, dass die „öffentliche“ Einsehbarkeit der Telefonnummer eine nützliche Einstellung ist, mithilfe derer andere Facebook-Nutzer gefunden werden können. Tatsächlich liegt jedoch genau die gegenteilige Konstellation vor: der seine Telefonnummer preisgebende Nutzer soll durch Dritte gefunden werden. Die Information, die die Beklagte gibt, ist unzweifelhaft selektiv

und damit unvollständig (so überzeugend auch LG Stuttgart, Urteil 26.01.2023, 53 O 95/22, Rn. 62). Vollständig wird die Information auf der Facebook-Seite zur Verarbeitung der Mobilfunknummer auch nicht dadurch, dass abschließend der Hinweis erteilt wird, man möge „beachten, dass man kontrollieren könne, wer die eigene Telefonnummer sehen könne“, oder gar durch den alles krönenden Hinweis auf die Datenrichtlinie.

c) Das Gericht hat im vorliegenden Fall keinerlei Zweifel daran, dass die Klagepartei bei einer vollständigen und unmissverständlichen Aufklärung über die Verarbeitung der Telefonnummer zur „Suchbarkeit“ eine andere Einstellung gewählt hätte. Wäre die Klagepartei bei Erstregistrierung konkret und auch transparent darüber aufgeklärt worden, dass ihr Nutzerprofil im Falle der Beibehaltung der standardisierten Voreinstellung zur Sucharbeit „öffentlich“ anhand ihrer Telefonnummer von jedermann, also auch von fremden Dritten, gefunden werden kann, hätte sie zweifelsfrei eine andere Einstellung gewählt, nämlich die Einstellung „privat“, so wie sie dies hinsichtlich der Sichtbarkeit der Telefonnummer im Nutzerprofil gewählt hat. Sie wäre dann nicht Opfer des „Scraping- Vorfalls“ geworden.

5.) Über die vorstehend bereits festgestellten Verstöße gegen die Datenschutz-Grundverordnung hinaus, hat die Beklagte zudem gegen ihre Pflichten aus Art. 32 DS-GVO zur Ergreifung geeigneter technischer und organisatorischer Schutzmaßnahmen verstoßen, was wiederum eine Schadensersatzpflicht nach Art. 82 DS-GVO begründen kann (vgl. Jandt in Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 32 Rn. 40a).

a) Nach Art. 32 Abs. 1 Hs. 1 DS-GVO haben der Verantwortliche und der Auftragsverarbeiter 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. Das Gebot soll insbesondere personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen davor schützen, dass Dritte diese unbefugt oder unrechtmäßig verarbeiten oder es unbeabsichtigt zu einem Verlust, einer Zerstörung oder Schädigung der Daten kommt (Martini in Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 32, Rn. 2 m.w.N.). Aus dem Gesetzeswortlaut lässt sich entnehmen, dass die Wirksamkeit der zu ergreifenden Maßnahmen an den anderenfalls drohenden Schäden auszurichten sind. Die Auswahl der geeigneten technischen und organisatorischen Maßnahmen hat mit anderen Worten die Balance zwischen dem Schutzniveau, das dem Stand der Technik entspricht und dem Risiko

zu finden (Paulus in BeckOK Datenschutzrecht, Wolff/Brink/v.Ungern-Sternberg, 45. Edition 01.11.2021, Art. 32, Rn.7). Auch die Beklagte hat das erkannt (vgl. Klageerwiderung S. 52 = Bl. 127 d.A.).

b) In Fällen der vorliegenden Art ist nach Auffassung des Gerichts bei den vorzunehmenden Maßnahmen und dem damit verbundenem notwendigen Schutzniveau ein hoher Maßstab anzulegen. Denn durch das nicht gänzlich vermeidbare „Scraping“ werden - wie hier - nicht nur massenhaft Daten erhoben, die ohnehin öffentlich zugänglich sind, es werden außerdem Verknüpfungen zu den Konten der betroffenen Nutzer und den darin enthaltenen Daten erstellt, im Ergebnis also ganze Datenpakete einschließlich der ohne Einwilligung „öffentlich“ einsehbaren Telefonnummer zusammengestellt. Die Gefahr, dass diese Datensätze einschließlich der Telefonnummer dann millionenfach veröffentlicht werden, was sich 2019 auch realisiert hat, war und ist nach wie vor immens hoch (so auch LG Lübeck, Urteil 25.05.2023,15 O 74/22, Rn. 76 m.w.N.). Gerade bei weltweit genutzten sozialen Netzwerken wie dem der Beklagten war „Scraping“ auch aus einer ex-ante-Sicht zu erwarten gewesen (vgl. LG Lübeck, a.a.O. m.w.N.). Der Beklagten war diese Thematik unzweifelhaft auch bekannt, trägt sie doch selbst vor, dass „Scraping“ im Internet allgegenwärtig sei (Klageerwiderung S. 25 = Bl. 100 d.A.).

c) Hinsichtlich der ergriffenen Schutzmaßnahmen i.S.d. Art. 32 Abs. 1 Hs. 1 DS-GVO trifft die Beklagte eine sekundäre Darlegungs- und Beweislast, da die primär darlegungsbelastete Klagepartei keine nähere Kenntnis der maßgeblichen Umstände und auch keine Möglichkeit zur weiteren Sachaufklärung hinsichtlich der Schutzmaßnahmen der Beklagten hat, während die Beklagte aufgrund ihrer Sachnähe hierzu unschwer vortragen kann. Die Beklagte hat nach dieser Maßgabe konkret vorzutragen, welche Schutzmaßnahmen sie im einzelnen ergriffen hat. Dies hat sie nicht getan. So sind insbesondere die Ausführungen in der Klageerwiderung (Seite 30/31) und im Schriftsatz vom 11.07.2023 (Duplik; dort S. 22 = Bl. 313 ff. d.A.), wonach die Beklagte „Captchas“, „Übertragungsbeschränkungen“ und „Bot-Erkennung“ eingesetzt habe, zu pauschal und einer Einlassung oder gar Überprüfung, ob diese Maßnahmen dem erhöhten Maßstab der Sicherungsmaßnahmen genügen, nicht zugänglich. Auch die Beschreibung weiterer, im Einzelnen jedoch unklar bleibender Maßnahmen, wie zum Beispiel des „Social Connection Check“ oder der „PYMK-Funktion“ (Klageerwiderung S. 23 und 24), ist unbehelflich, zumal der Vortrag der Beklagten erkennen lässt, dass diese vermeintlichen Sicherungsmaßnahmen erst *nach* dem streitgegenständlichen „Scraping- Vorfall“ ergriffen wurden. Es ist jedenfalls im Ergebnis weder hinreichend zur Funktionsweise noch zur konkreten Ausgestaltung der *vorher* vorliegenden Sicherungsmaßnahmen vorgetragen worden. Eines richterlichen Hinweises hierzu bedurfte es nicht, da gerichtsbekannt ist, dass weitere Einlassungen oder Darlegungen der Beklagten unter Ver-

weis auf angebliche Geschäftsgeheimnisse betreffend die Übertragungsbeschränkungen u.a. nicht erfolgen werden, ohne dass jedoch hinreichend preisgegeben wird, welche konkreten Geheimnisse zu schützen sind (dazu OLG Köln, Urteil 05.11.2020, 7 U 35/20, Rn. 56 m.w.N.). Soweit die Beklagte auf ergriffene Sicherungsmaßnahmen nach dem „Scraping- Ereignis“ hinweist, drängt sich die Frage auf, aus welchem Grund offenbar doch mögliche Sicherungsmaßnahmen nicht schon vor dem streitgegenständlichen Vorfall ergriffen worden sind, wo der Beklagten ausweislich ihres eigenen Vortrages das allgegenwärtige Problem des Scrapings bekannt gewesen ist (vgl. nochmals Klageerwiderung S. 25 = Bl. 100 d.A.).

d) Unter Berücksichtigung der vorstehenden Ausführungen ist bei der Beurteilung der streitgegenständlichen Ansprüche zugrunde zu legen, dass ausreichende Sicherheitsvorkehrungen nach Art. 32 DS-GVO im relevanten Zeitraum nicht installiert waren, sodass es infolgedessen erst zu dem millionenfachen Abgreifen der Nutzerdaten kommen konnte. Denn gerade das in der Klageerwiderung (dort Seite 27/28) beschriebene Vorgehen der Scraper, mithilfe der sog. Kontakt-Importer-Funktion fingierte Telefonnummern hochzuladen, um festzustellen, ob die Telefonnummern mit einem Facebook-Konto verbunden sind, dessen öffentlich zugängliche Daten dann abgegriffen wurden, indiziert das Fehlen ausreichender Sicherheitsvorkehrungen. Erst das durch die Beklagte selbst bereitgestellte Tool der „Kontakt-Importer-Funktion“ eröffnete überhaupt die Möglichkeit der Verbindung der angefragten Telefonnummer mit einem Facebook-Konto. Dass nicht nur redliche Nutzer von dieser Möglichkeit Gebrauch machen, war der Beklagte zweifelsfrei bekannt, sodass sie nur einzelne Telefonnummer-Abfragen hätten zulassen dürfen; massenhafte Anfragen zu Telefonnummern hätten verhindert werden müssen.

6.) Ob die Beklagte auch den Grundsatz „privacy by design“ bzw. „privacy by default“ (also der datenschutzfreundlichen Voreinstellungen) verletzt hat, kann wegen der bereits bejahten Verstöße gegen die Datenschutz-Grundverordnung dahinstehen. Allein aus einem Verstoß gegen Art. 25 DS-GVO kann wegen des rein organisatorischen Charakters dieser Norm ohnehin ein Anspruch nach Art. 82 Abs. 1 DS-GVO nicht begründet werden (vgl. Hartung in Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 25, Rn. 31; so entschieden vom LG Paderborn, Urteil 19.12.2022, 3 O 99/22, Rn. 112). Die Vorschrift entfalte danach ihren Regelungscharakter bereits vorgelagert, also *vor* dem eigentlichen Beginn der Datenverarbeitung. Art. 82 Abs. 2 DS-GVO setzt jedoch voraus, dass der Schaden „*durch* eine Verarbeitung“ ausgelöst wurde.

7.) Aus eben diesen Erwägungen heraus kann auch offenbleiben, ob die Beklagte nach dem relevanten „Scraping-Vorfall“ ihre Meldepflichten aus Art. 33, 34 DS-GVO verletzt und weder die Aufsichtsbehörde gemäß Art. 33 DS-GVO noch die betroffene Nutzer entsprechend ihrer Verpflichtung aus Art. 34 Abs. 1 DS-GVO informiert hat. Denn auch auf diese - wohl zu bejahenden - Verstöße lässt sich ein immaterieller Schadensersatzanspruch vorliegend nicht stützen, weil nicht überzeugend angenommen werden kann, dass die etwaige Verletzung dieser Pflichten für den geltend gemachten Schaden der Klagepartei überhaupt noch (mit-)kausal geworden ist oder diesen zumindest vertieft hat. Vielmehr steht fest, dass das streitgegenständliche „Scraping“ der Daten mit der öffentlichen Einstellung der Daten im Darknet erstmals offenbar geworden ist und sich der Schaden darin bereits verwirklicht hat. Dass eine in der Folge unterlassene Information hierüber den damit bereits eingetretenen Schaden in Gestalt der Verletzung des allgemeinen Persönlichkeitsrechtes der Klagepartei konkret weiter vertieft hätte, lässt sich nicht feststellen. Überdies ist nicht ersichtlich, dass der Gefahr, die sich aus den bereits rechtswidrig zirkulierenden Daten ergab, zum Zeitpunkt der unterstellt unterlassenen Information noch hätte begegnet werden können (so LG Lübeck, Urteil 25.05.2023, 15 O 74/23, Rn. 84).

8.) Die Beklagte hat die oben festgestellten haftungsbegründenden Verstöße gegen die DS-GVO auch zu vertreten. Die ihr nach Art. 82 Abs. 3 DS-GVO eingeräumte Möglichkeit zur Exkulpation ist nicht gelungen.

Die konkrete Konfiguration der Voreinstellungen in den Nutzer-Profilen war ebenso wie die technischen Funktionen zur Nutzung der Telefonnummern seitens der Beklagten im Rahmen ihres Geschäftsbetriebes bewusst so gestaltet bzw. vorgesehen (so auch LG Lübeck, Urteil 25.05.2023, 15 O 74/22, Rn. 87). Im Rahmen ihres umfangreichen Vortrages hat die Beklagte durchaus erkennen lassen, dass sie die technische Möglichkeit des Abgreifens von Daten durch die von ihr gewählte Architektur der Facebook-Plattform (insbesondere Zugriff auf Nutzer-Profile aufgrund voreingestellter öffentlicher Suchbarkeit der Telefonnummer über das Kontakt-Importer-Tool) geschaffen hat. Der Beklagten war bewusst, dass Daten-Scraper bestimmte Funktionen (wie eben die Kontakt-Importer-Funktion) missbrauchen können.
Aus diesem Grunde wäre es ihre Pflicht gewesen, das unbefugte massenhafte Abgreifen der Daten zu unterbinden. Das Gericht verkennt dabei nicht, dass die Beklagte mit entsprechenden Maßnahmen bzw. Vorkehrungen ihrem eigenen Verständnis von der Facebook-Plattform in gewisser Weise zuwider hätte handeln müssen, dem Interesse der Nutzer an der Wahrung datenschutzrechtlicher Belange hätte dies - gemäß der DS-GVO - aber sehr wohl entsprochen.

Die Beklagte muss sich damit zumindest Fährlässigkeit vorwerfen lassen. Dies gilt auch im Hinblick auf die fehlende Erfüllung der Sorgfaltsanforderungen. Substantiierter Vortrag, der den Fahrlässigkeitsvorwurf entkräften könnte, würde zumindest Angaben dazu voraussetzen, aufgrund welcher konkreten Erkenntnisse ex ante davon hätte ausgegangen dürfen, dass - und ggf. welche - Maßnahmen zur Erfüllung des Art. 32 DS-GVO ausreichend sein könnten. Derartiges hat die Beklagte nicht vorgetragen. Ergänzend wird auf obige diesbezügliche gerichtliche Ausführungen Bezug genommen.

9.) Ein ersatzfähiger Schaden der Klagepartei im Sinne von Art. 82 Abs. 1 DS-GVO ist gegeben.

a) Die Entstehung eines, im Rahmen des Art. 82 Abs. 1 DS-GVO im Grunde auch ersatzfähigen materiellen Schadens hat die Klagepartei nicht dargetan.

b) Sie hat jedoch einen immateriellen Schaden erlitten. Ein solcher liegt zwar nicht schon vor bei der bloßen Verletzung einer Norm der DS-GVO (dazu grundlegend EuGH, Urteil 04.05.2023, C-300/21), wohl aber bei Verletzung absolut geschützter Rechtsgüter durch Verstöße gegen die DS-GVO. Die Vorschriften der §§ 249 ff. BGB können insofern herangezogen werden (Quaas in BeckOK Datenschutzrecht, Wolff/Brink/v.Ungern-Sternberg, 45. Edition 01.05.2023, Art. 82, Rn. 28b). In Betracht kommt etwa eine Verletzung des Rechts auf körperliche Unversehrtheit ebenso wie eine Verletzung des Rechts auf informationelle Selbstbestimmung als besondere und ebenfalls absolut geschützte Ausprägung des allgemeinen Persönlichkeitsrechts (vgl. dazu Slizyk, Handbuch Schmerzensgeld, 19. Auflage 2023, Rn. 244-249). Das hier befasste Gericht schließt sich der zwischenzeitlich auch überwiegend vertretenen Auffassung an, wonach die erlittene Verletzung eine gewisse Erheblichkeitsschwelle nicht überschreiten muss (EuGH, Urteil 04.05.2023, C-300/21, Rn. 45).

c) Eine für die Bejahung eines Schadens ausreichende Verletzung des allgemeinen Persönlichkeitsrechts in der Ausprägung des Rechts auf informationelle Selbstbestimmung liegt hier vor. Dieses Recht der Klagepartei wurde und wird bis heute fortlaufend verletzt. Die Daten der Klagepartei wurden infolge der oben näher dargelegten Verstöße gegen mehrere Tatbestände der DS-GVO auf Internetseiten, so beispielsweise der Seite „raidforums.com“, verbreitet, sodass es der Klagepartei nicht mehr möglich ist, selbst und eigenverantwortlich darüber zu entscheiden, wo und ob sie diese Daten offenbaren möchte. Dieser Verletzung misst das Gericht dabei auch ein erhebliches Gewicht zu.

d) Die Klagepartei wurde in der mündlichen Verhandlung vom 01.09.2023 zu den Auswirkungen des „Scraping-Vorfalls“ angehört. Zuzugeben ist insofern, dass auch Internet-Nutzer, die nicht auf Facebook angemeldet sind, dubiose Anrufe aus diversen Callcentern oder sog. Phishing-E-Mails, zum Beispiel von Paket-Lieferdiensten, erhalten. Allein diese Anrufe stellen eine nicht zu unterschätzende Gefahr dar, unabhängig davon, dass sie als Störung der Privatsphäre einzustufen sind. Aufgrund der Tatsache, dass die Klägerin jedoch Yogalehrerin ist und zu diesem Zweck eine eigene Seite betreibt, auf der sie entsprechende Kurse anbietet, besteht die begründete Sorge, dass im Zeitalter der fortschreitenden Technik und der Weiterentwicklung künstlicher Intelligenz die Daten der Klägerin mit einer Nachbildung ihres Gesichtes und ihrer Stimme zusammengefügt werden. Auf der Hand liegt hierdurch das Risiko und die Gefahr eines nicht durch die Klagepartei autorisierten Auftretens im Internet, möglicherweise mit Nachteilen für die Klagepartei selbst. Ein Schaden ist ohne Zweifel anzunehmen.

e) Der Schaden beruht auch kausal auf den oben festgestellten Verstößen; es wird auf die jeweils dort dargelegten Kausalitätserwägungen Bezug genommen. Unzweifelhaft wäre es nicht zum Abgreifen der Daten der Klagepartei und zu deren Verbreitung im Darknet gekommen, wenn die Beklagte die oben aufgeführten Datenschutz-Verstöße nicht begangen hätte (siehe jeweils dort).

f) Soweit die Beklagte im Übrigen meinen sollte, dass die Mobilfunknummer der Klagepartei freiwillig auch auf anderen Internet-Plattformen öffentlich zugänglich sei, ein Schaden der Klagepartei also nicht vorliege, ändert dieser Umstand zum einen nichts daran, dass die hier streitgegenständlichen Daten im Darknet - nur - aufgrund des „Scraping-Vorfalls“ veröffentlicht wurden. Zum anderen hat die Klagepartei zutreffend in der mündlichen Verhandlung vom 01.09.2023 darauf hingewiesen, dass es einen Unterschied mache, ob die Telefonnummer freiwillig auf einer themenbezogenen Seite (hier dem Online-Yoga-Studio der Klägerin) sichtbar sei, die nur bei einer zielgerichteten Suche gefunden werde, oder ob die Mobilfunknummer ohne das Wissen der Klagepartei als „öffentliches“ Suchkriterium auf der Seite eines sozialen Netzwerkes Verwendung finde, ohne dass auf den konkreten Zweck der Datenverwendung (hier „Suchbarkeit“) hingewiesen worden sei.

10.) Die Höhe des Schadensersatzes beziffert das Gericht mit 500,00 €, wobei es diesen Betrag für angemessen, aber auch für ausreichend hält, um den immateriellen Schaden auszugleichen und gleichzeitig der erforderlichen Abschreckungswirkung Rechnung zu tragen sowie dabei die besonderen Umstände des Falles zu würdigen.

a) Dem Gericht steht bei der Bemessung des Schadensersatzes gemäß § 287 ZPO ein Ermessen zu. Auf die vorstehenden Erwägungen zur Beeinträchtigung der Klägerin wird Bezug genommen. Zu berücksichtigen war ferner, dass der Beklagten gleich mehrere Verstöße gegen die DS-GVO zur Last zu legen sind.

b) Nicht schadensersatzerhöhend wurde der Umstand der behaupteten verspäteten Auskunft bewertet. Denn soweit die Klagepartei ausweislich des als Anlage K1 vorgelegten Schreibens vom 14.06.2021, dort Seite 11, diverse Auskünfte einforderte, ist nach Auffassung des Gerichtes ein Anspruch aus Art. 15 DS-GVO nicht gegeben. Aus dem Aufforderungsschreiben (Anlage K1) ergibt sich, dass die begehrten Auskünfte nicht die Verarbeitung personenbezogener Daten durch die Beklagte betreffen, sondern Informationen zu der unbefugten Datenerhebung durch unbekannte Dritte im Rahmen des „Scraping-Vorfalls“. Soweit es der Beklagten hingegen möglich war, Auskunft zu erteilen, hat sie dies in ihrem als Anlage K2 vorgelegten Schriftsatz vom 23.08.2021 getan. Die Beklagte verwies die Klagepartei hinsichtlich der verarbeiteten personenbezogenen Daten maßgeblich auf die Selbstbedienungstools der Facebook-Seite (Anlage K2, Seite 3 unten). Diese Erfüllungshandlung war ausreichend um den Erfüllungserfolg zu gewährleisten, zumal ergänzend ausführlich auf die Zwecke der Datenverarbeitung hingewiesen wurde. Soweit der Beklagten im Hinblick auf die Verursacher des „Scraping-Vorfalls“ eine Auskunft mangels - nicht widerlegbarer - eigener Kenntnis nicht möglich war, hat sie dies auch deutlich gemacht. Soweit hingegen Auskünfte möglich waren, wurden diese erteilt.

c) Anhaltspunkte, aus denen sich die Berechtigung der Erhöhung des ursprünglich eingeforderten Schadensersatzes in Höhe von 500 € (vgl. Anschreiben 14.06.2021 = Anlage K1) auf nunmehr klageweise geforderte 1.000 € ergeben könnte, sind nicht dargelegt.

II.) Feststellungsantrag

Der Klageantrag zu Ziffer 2. der Klage ist begründet. Die Klagepartei hat einen Anspruch auf Feststellung der Eintrittspflicht der Beklagten für künftige Schäden materieller oder immaterieller Art.

Künftige Schäden der Klagepartei, die auf die oben näher dargelegten Verstöße der Beklagten gegen die Datenschutz-Grundverordnung zurückzuführen sind, sind nicht ausgeschlossen, sie sind nicht einmal fernliegend, da die im Rahmen des 2019 geschehenen „Scraping-Vorfalls“ abgegriffenen Daten auf unabsehbare Zeit im Internet, insbesondere im Darknet, verfügbar sein werden

und auch nicht festgestellt werden kann, wohin diese Daten zwischenzeitlich verbreitet wurden und in wessen Hände sie gelangt sind. Vom Eintritt einer *gewissen Wahrscheinlichkeit* eines Schadenseintritts ist die Bejahung des Feststellungsantrages nach obergerichtlicher Rechtsprechung nicht abhängig (so BGH, Urteil 17.10.2017, VI ZR 423/16, Rn. 49 m.w.N.).

III.) Unterlassungsantrag

Unabhängig davon, dass der unter Ziffer 3. lit. a. und b. der Klage erhobene Unterlassungsantrag unzulässig ist, wäre er jedenfalls auch als unbegründet abzuweisen.

Der Klagepartei steht insbesondere kein Unterlassungsanspruch dahin zu, eine Datenverarbeitung ohne Erfüllung der Informationspflichten hinsichtlich der Funktionsweise der „Kontakt-Importer-Funktion“ und der Verwendung von Telefonnummern zu unterlassen. Zwar hat die Beklagte - wie oben ausgeführt - gegen die DS-GVO verstoßen, als sie im Zusammenhang mit der Registrierung nicht ausreichend nach Art. 13, 14 DSGVO über die Nutzung der mitgeteilten Mobilfunknummer im Rahmen der „Suchbarkeit“ informiert hat und die Klagepartei damit in ihren Rechten verletzt hat. Insofern ist jedoch eine Wiederholungsgefahr als Voraussetzung eines Unterlassungsanspruches ausgeschlossen, weil die Klägerseite im Verlauf des Rechtsstreits zum einen sämtliche Informationen erhalten hat, die die streitgegenständliche Art und Weise der Datenverarbeitung betreffen. Zum anderen ist ihr zwischenzeitlich auch bekannt geworden, dass ihre Telefonnummer durch den Einsatz des „Kontakt-Import-Tools“ verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert wird.

IV.) Auskunftsanspruch

Der Klageantrag Ziffer 4., gerichtet auf Erteilung der Auskunft, welche Daten die Beklagte verarbeitet, „namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt durch Scraping oder das Kontakt-Import-Tool erlangt werden konnten“, ist unbegründet. Der Klagepartei steht eine derartige Auskunft weder aus Art. 15. DS-GVO noch aus dem Nutzungsvertrag i.V.m. § 242 BGB zu.

1.) Ein Auskunftsanspruch nach Art. 15 DS-GVO besteht nicht. Denn die Tatbestandsmerkmale dieser Vorschrift decken den genannten Antrag nicht ab. Soweit die Klägerseite Auskunft dazu verlangt, „welche Daten zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontakt-Import-Tools erlangt werden konnten“, ist die Auskunft mit anderen Worten

nicht von Art. 15 DS-GVO erfasst. Es handelt sich weder um eine Information über die *durch die Beklagte verarbeiteten* personenbezogenen Daten der Klägerseite i.S.d. Art. 15 Abs. 1 DS-GVO, noch wird Auskunft über Meta-Informationen zu diesen Daten (= Verarbeitungszwecke, Datenkategorien, Empfänger/-kategorien, Speicherdauer, Herkunft der Daten etc.) gemäß Art. 15 Abs. 1, 2. Hs., Teil 2 DS-GVO begehrt. In der Sache begehrt die Klagepartei vielmehr Informationen zu der unbefugten Datenerhebung durch unbekannte Dritte, die sie gemäß Art. 15 DS-GVO jedoch nicht von der Beklagten verlangen kann. Zweck der Vorschrift des Art. 15 DS-GVO ist es vielmehr, den Betroffenen durch den Auskunftsanspruch in die Lage zu versetzen, von einer Verarbeitung der ihn betreffenden Daten Kenntnis zu erhalten und diese auf ihre Rechtmäßigkeit hin zu überprüfen (vgl. Schmidt-Wudy in BeckOK Datenschutzrecht, 43. Edition 01.2.2023, DS-GVO, Art. 15 Rn. 2). Zweifeln begegnet eine Auslegung des Art. 15 DS-GVO dahingehend, dass Auskunftsrechte der Art bejaht werden, dass im Hinblick auf einen erfolgten Datenabfluss und im Nachgang eines solchen, Informationen zur wirtschaftlichen Verwertung der Daten, so sie denn überhaupt möglich sind, gegeben werden müssen.

2.) Unterstellt, ein derartiger Auskunftsanspruch wäre anzunehmen, so ist er durch Erfüllung erloschen, § 362 Abs. 1 BGB.

a) Gemäß Art. 15 Abs. 1, 2. Hs. Teil 1 DS-GVO muss der Klagepartei Auskunft zu den durch die Beklagte verarbeiteten personenbezogenen Daten erteilt werden. Die Beklagte ist dabei gemäß Art. 4 Ziff. 7 DS-GVO „Verantwortlicher“ i.S.d. Art. 15 DS-GVO. „Verarbeitung“ der Daten umfasst gemäß Art. 4 Ziff. 2 DS-GVO jeden, mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Das Auskunftsrecht umfasst dabei alle Daten, die bei dem Verantwortlichen vorhanden sind (Bäcker in Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 15, Rn. 8). Das Auskunftsrecht besteht überdies auch hinsichtlich der Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen gemäß Art. 15 Abs. 1 Hs. 2 c) DS-GVO.

b) Die nach vorstehenden Ausführungen erforderliche Mitteilung hat die Beklagte durch das als Anlage K2 vorgelegten Schreiben vom 23.08.2021 in angemessener Weise vorgenommen. Die Klagepartei wurde auf das Selbstbedienungstool auf der Facebook-Seite verwiesen und es wurde

ausgeführt, welche personenbezogenen Daten verarbeitet wurden und werden. Diese Erfüllungshandlung ist ausreichend gewesen, um den Erfüllungserfolg zu gewährleisten.

c) Soweit der Antrag der Klagepartei nun im Sinne eines neuen Auskunftsbegehrens nach Art. 15 Abs. 1 DS-GVO, gerichtet auf Auskunft über sämtliche, die Klagepartei betreffende personenbezogene Daten, die die Beklagte verarbeitet, auszulegen wäre, ist wiederum der in der Klageerwiderung (Seite 82 = Bl. 157 d.A.) enthaltene Verweis auf die Selbstbedienungstools unter den Menüpunkten „Access Your Information“ und „Download Your Information“ ausreichend, denn dort erhält die Klagepartei einen Zugriff auf die personenbezogenen Daten gemäß Art. 15 DS-GVO.

d) Im Hinblick auf die begehrten Informationen zu den Empfängern der durch das „Scraping“ erlangten Daten, muss auf die obigen Ausführungen Bezug genommen werden. Zum Einen hat sich die Beklagte zulässigerweise auf die Mitteilung der potentiellen Empfänger (= „jedermann“) beschränkt. Zum anderen ist eine nähere Identifizierung der Empfänger der Daten unwiderlegbar nicht möglich.

3.) Auch aus dem zwischen den Parteien bestehenden Vertrag i.V.m. § 242 BGB ergibt sich nichts anderes. Auch insofern hat die Beklagte bereits in dem Schreiben vom 23.08.2021 an die Klagepartei (Anlage K2) ausreichende Auskünfte erteilt. Auf den Inhalt der Anlage K2 wird Bezug genommen. Sie hat ausgeführt, auf welcher Weise - ihren Erkenntnissen nach - die unbekannten Dritten im Rahmen des „Scrapings“ vorgingen und welche einzelnen Daten bei dieser Vorgehensweise - weil öffentlich einsehbar - abgeschöpft werden konnten. Auch den relevanten Zeitraum des „Scraping-Vorfalles“ teilte die Beklagte mit. Weitere Auskünfte vermag die Klägerseite vorliegend nicht zu verlangen, nachdem das „Scraping“ - unstreitig - von außen erfolgt ist und unwiderlegbar auch bei der Beklagten dazu keine näheren Erkenntnisse vorliegen. Im Ergebnis ist also festzustellen, dass die Beklagte der Klagepartei alle Informationen mitteilte, die ihr selbst im Zuge des Scraping-Vorfalls zur Verfügung standen. Weitere Angaben kann sie nicht machen. Sie ist hierzu auch nicht verpflichtet.

V. Nebenentscheidungen

1.) Der Klägerseite steht ein Anspruch auf Ersatz vorgerichtlicher Rechtsanwaltsgebühren in Höhe von 159,94 € zu. Die vorgerichtlichen Rechtsanwaltskosten sind dabei Teil des gemäß Art. 82 Abs. 1 DS-GVO zu ersetzenden Schadens. Die Hinzuziehung eines Rechtsanwalts zur Durch-

setzung der klägerischen Ansprüche ist unzweifelhaft angesichts der Komplexität der Materie erforderlich gewesen. Ausgehend von einem Wert des berechtigten Verlangens der Klägerseite von bis zu 1.000,00 € zum Zeitpunkt der außergerichtlichen Tätigkeit ergibt dies Kosten in Höhe von 159,94 €, die sich wie folgt errechnen: 1,3 Geschäftsgebühr nach Nr. 2300 VV RVG = 114,40 € zzgl. Post- und Telekommunikationspauschale Nr. 7002 VV RVG = 20,00 € zzgl. 19% MwSt = 25,54 €.

2.) Der Zinsanspruch folgt aus §§ 288, 291 BGB i-V.m. § 187 BGB. Die Klage wurde ausweislich der DHL-Sendungsverfolgung, Bl. 73 d.A., am 09.05.2022 zugestellt.

3.) Der **Streitwert** war auf **7.000,00 €** festzusetzen. Das Gericht hat sich dabei maßgeblich auf §§ 3 ff. ZPO gestützt. Der Wert des Antrages Ziffer 1. ergibt sich aus dem klägerseits angegebenen immateriellen (Mindest-)Ersatzbetrag in Höhe von 1.000,00 €. Entgegen der Auffassung der Klagepartei (vgl. Klageschrift S. 27) ist auch dem Klageantrag Ziffer 2. auf Feststellung der Ersatzpflicht hinsichtlich künftiger Schäden ein eigener wirtschaftlicher Wert beizumessen, wobei das Interesse der Klagepartei gemäß § 3 ZPO auf mindestens 500,00 € zu schätzen gewesen ist (vgl. dazu auch OLG Bamberg, Beschluss vom 23.05.2023, 8 UH 5/23 unter Verweis auf OLG Stuttgart, Beschluss vom 03.01.2023, 4 AR 4/22, Rn. 23). Die in Antrag Ziffer 3. unter Buchstaben a. und b. zusammengefassten Unterlassungsanträge betreffen jeweils nichtvermögensrechtliche Streitigkeiten i.S.d. § 48 GKG, sodass auf die Umstände des Einzelfalls abzustellen ist. Das Gericht hat - wiederum in Anlehnung an einen gleichgelagerten Fall, der dem Beschluss vom 23.05.3023 zugrunde lag - in Übereinstimmung mit dem OLG Bamberg für die Unterlassungsanträge insgesamt einen Gebührenstreitwert von insgesamt 5.000,00 € festgesetzt.
Der Wert des Auskunftsantrages Ziffer 4. der Klage war nach § 3 ZPO auf 500,00 € zu schätzen. Der Klageantrag Ziffer 5. (Ersatz der vorgerichtlichen Rechtsanwaltskosten) wirkt sich nicht streitwerterhöhend aus.

4.) Die Kostenentscheidung ergibt sich aus § 92 Abs. 1 Satz 1, 2. Alt. ZPO. Die Klagepartei obsiegt mit ihren Anträgen zu Ziffer 1. teilweise in Höhe von 500,00 € und zu Ziffer 2., der ebenfalls ein Obsiegen im Umfang von 500,00 € ergibt. Das Obsiegen entspricht bei einem Streitwert von 7.000,00 € damit einem Anteil von 14,3 %; die diesbezüglichen Kosten hat die Beklagte zu tragen. Die übrigen 85,7 % der Kosten fallen der Klagepartei selbst zu Last.

5.) Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt für beide Parteien aus §§ 708 Nr. 11, 711 ZPO.

gez.

[redacted]
Richterin am Landgericht

Verkündet am 02.10.2023

gez.
[redacted]
Urkundsbeamtin der Geschäftsstelle

Für die Richtigkeit der Abschrift
Hof, 02.10.2023

[redacted]
Urkundsbeamtin der Geschäftsstelle