Landgericht Chemnitz

Zivilabteilung

Aktenzeichen: **1 O 429/22**

IM NAMEN DES VOLKES

ENDURTEIL

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:

gegen

Meta Platforms Ireland LimitedFacebook Ireland Ltd., 4 Grand Canal Square, Dublin 2, Irland
vertreten durch den Direktor Gareth Lambe

- Beklagte -

Prozessbevollmächtigte:

wegen Persönlichkeitsrechtsverletzung, Verstöße gegen die Datenschutz-Grundverordnung

hat die 1. Zivilkammer des Landgerichts Chemnitz durch

Vizepräsident des Landgerichts
Richterin am Landgericht
Richter

auf Grund der mündlichen Verhandlung vom 23.01.2023 am 20.03.2023

für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger einen Betrag in Höhe von 500,00 EUR nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 31.05.2022 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen Schäden zu ersetzen, die ihm 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, personenbezogene Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern.

4. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 453,87 EUR nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 31.05.2022 zu zahlen.

5. Im Übrigen wird die Klage abgewiesen.

6. Die Kosten des Rechtsstreits werden gegeneinander aufgehoben.

7. Das Urteil ist vorläufig vollstreckbar, für den Kläger hinsichtlich Ziffer 1, Ziffer 4 und wegen der Kosten nur gegen Sicherheitsleistung in Höhe von 110 Prozent des jeweils zu vollstreckenden Betrages, ansonsten hinsichtlich Ziffer 2 gegen Sicherheitsleistung in Höhe von 600 EUR und hinsichtlich Ziffer 3 gegen Sicherheitsleistung in Höhe von 3.000 EUR.
   Dem Kläger wird nachgelassen, die Vollstreckung durch die Beklagte gegen Sicherheitsleistung in Höhe von 110 Prozent des aufgrund des Urteils vollstreckbaren Betrages abzu-

wenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 Prozent des jeweils zu vollstreckenden Betrages leistet.

Beschluss:

Der Streitwert wird auf 11.000,00 EUR festgesetzt.

Tatbestand

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

Der Kläger ist Nutzer des von der Beklagten betriebenen sozialen Netzwerkes Facebook. Auf das Netzwerk kann mittels der Website-URL www.facebook.com sowie über Anwendungen („Apps“) für Mobiltelefone und Tablet-PCs (gemeinsam „Facebook-Plattform“) zugegriffen werden. Für Nutzer in der Europäischen Union wird die Facebook-Plattform von der Beklagten, einem Unternehmen nach dem Recht der Irischen Republik mit Sitz in Dublin, Irland, betrieben.

Die Facebook-Plattform soll Menschen dazu dienen, mit Familie und Freunden in Kontakt zu bleiben, neue Menschen kennenzulernen, Gemeinschaften und Gruppen beizutreten und ganz allgemeine Vorgänge in der Welt zu beobachten. Dazu ermöglicht die Plattform deren Nutzern, persönliche Profile für und über sich zu erstellen und diese mit anderen Nutzern der Plattform zu teilen. Die Nutzer können auf den persönlichen Profilen Angaben zu verschiedenen Daten ihrer Person machen. Dabei ist die Angabe der Daten Name, Geschlecht und eine von der Beklagten generierten Nutzer-ID zwingende Voraussetzung für die Registrierung bei Facebook. Diese Daten können nicht nur die Facebook-Nutzer, sondern auch alle im Internetverkehr aktiven User („alle“) einsehen. Hinsichtlich weiterer fakultativer Daten (zum Beispiel Wohnort, Geburtsdatum, Beziehungsstatus, E-Mail-Adresse und Telefonnummer), hält die Beklagte im Rahmen der sog. „Privatsphäre-Einstellungen“ unterschiedliche Einstellungsmöglichkeiten bereit. So kann der Nutzer darüber entscheiden, wie öffentlich die zusätzlich angegebenen Informationen sein sollen, indem er anstelle der standardmäßigen Voreinstellung „öffentlich“ auswählt, dass nur „Freunde“ oder „Freunde von Freunden“ auf der Facebook-Plattform die jeweiligen (fakultativen) Informationen einsehen können. Lediglich die Telefonnummer des Nutzers wird – soweit überhaupt überobligatorisch angegeben – gesondert behandelt, indem diese standardmäßig nur vom Nutzer selbst – so der Kläger – oder nur von „Freunden“ – so die Beklagte – eingesehen werden kann.

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

Der Kläger registrierte sich auf der Facebook-Plattform. Dabei gab er neben den zwingend für die Registrierung erforderlichen und stets öffentlich einsehbaren Daten Name, Geschlecht und Nutzer-ID u.a. auch seine Telefonnummer an. Die „Suchbarkeits-Einstellung“ bezüglich dieser Telefonnummer war bei dem Kläger bis zum 02.02.2021 auf „Alle“ eingestellt, danach wurde sie auf „Nur Ich“ geändert (Anlage B17). Die Telefonnummer war zu keinem Zeitpunkt öffentlich auf dem Facebook-Profil des Klägers einsehbar.
Bei der Registrierung wurde der Kläger auf die Datenschutz- und Cookierichtlinie der Beklagten hingewiesen und musste dieser zustimmen. Diesbezüglich wird auf die in der Anlage B9 zur Akte gereichten Auszüge Bezug genommen. Den Nutzern werden zudem im „Hilfebereich“, der unmittelbar auf der Facebook-Homepage verlinkt ist, Informationen über die Privatsphäre-Einstellungen zur Verfügung gestellt. Auf diese Einstellungen kann unter der Überschrift „Privatsphäre, Datenschutz und Sicherheit“ zugegriffen werden. Hinsichtlich der weiteren relevanten Inhalte im Hilfebereich und in den Einstellungen wird auf die Abbildungen in der Klageschrift sowie die Anlagen B1 bis B8 Bezug genommen.

Im Zeitraum von Januar 2018 bis September 2019 kam es auf der Facebook-Plattform zu sog. „Scraping“, also dem massenhaften, automatisierten Sammeln persönlicher Daten von Facebook-Nutzern. „Scraping“ ist eine weitverbreitete Methode, um Daten, die typischerweise öffentlich einsehbar sind, von Internetseiten durch automatisierte Softwareprogramme abzurufen und abzugreifen. Dabei lasen und persistierten Dritte Telefonnummer, Nutzer-ID, Name, Geschlecht und weitere korrelierende Daten aus zum Teil öffentlich zugänglichen Daten bei

Facebook aus. Dieses Sammeln von Daten mittels automatisierter Tools und Methoden war und ist nach den Nutzungsbedingungen der Beklagten untersagt.
Der Abruf der fraglichen Telefonnummern erfolgte hier jedoch nicht über die Facebook-Profile. Vielmehr wurden diese mittels des Contact Import Tools mit den jeweils dazugehörigen Profilen verknüpft. Diese Verknüpfung geschah auch dann, wenn die im Profil hinterlegte Nummer in der „Zielgruppenauswahl“ nicht öffentlich gemacht worden war.
Vor diesem Hintergrund luden die „Scraper“ mithilfe des „CIT“ Kontakte hoch, welche mögliche Telefonnummern von Nutzern enthielten, um festzustellen, ob diese Telefonnummern mit einem Facebook-Konto verbunden sind. Soweit sie feststellen konnten, dass eine Telefonnummer mit einem Facebook-Konto verknüpft war, kopierten sie die – per „Zielgruppenauswahl“ – öffentlich einsehbaren Informationen aus dem betreffenden Nutzerprofil und fügten die Telefonnummer den abgerufenen, öffentlich einsehbaren Daten hinzu. Der konkrete Ablauf des „Scraping-Vorfalls“ steht zwischen den Parteien im Streit; insbesondere wie die mittels des „CIT“ abgerufenen Telefonnummern in die Hände der Dritten gelangt sind.
Anfang April 2021 veröffentlichten Unbekannte nach Angaben eines Artikels des „Business Insider“ vom 03.04.2021 die Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern in einer ungesicherten Datenbank im Internet.
Die Beklagte veröffentlichte als Reaktion darauf am 06.04.2021 den Artikel „Die Fakten zu Medienberichten über Facebook-Daten“ (Anlage B10). Sie informierte nicht die Datenschutzbehörde Irish Data Protection Commission über den Vorfall. Stattdessen ergriff die Beklagte als Reaktion auf die Medienberichterstattung Maßnahmen, um Nutzern Informationen über das „Scraping“ sowie die Möglichkeiten zur Änderung ihrer Privatsphäre-Einstellungen zur Verfügung zu stellen.

Mit E-Mail des Prozessbevollmächtigten des Klägers vom 23.08.2021 forderte dieser die Beklagte zur Schadensersatzzahlung in Höhe von 500,00 EUR, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft darüber auf, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht worden waren.

Mit Schreiben vom 28.10.2021 – adressiert an die klägerischen Prozessbevollmächtigten – teilte die Beklagte mit, welche Datenkategorien nach den ihr zum Zeitpunkt der Auskunftserteilung verfügbaren Erkenntnissen in den durch Scraping abgerufenen Daten erscheinen und mit den auf dem Facebook-Profil der Klagepartei verfügbaren Informationen übereinstimmen (vorgelegt als Anlage B16).

Die irische Datenschutzbehörde verhängte gegen die Beklagte wegen des streitgegenständli-

chen Datenschutzvorfalls mit ihrer Entscheidung vom 25.11.2022 ein Bußgeld in Höhe von 17 Millionen Euro (Entscheidung vorgelegt als Anlage K4).

Der Kläger trägt vor, dass resultierend aus dem „Scraping-Vorfall“ ihn betreffende Daten abgegriffen und im Inter- sowie Darknet auf Seiten veröffentlicht worden seien, die illegale Aktivitäten begünstigen sollen. So zum Beispiel auf der Seite raidforums.com (ein Hackerforum).
Er behauptet, dass die Beklagte effektiven Datenschutz zur Gewinnmaximierung verhindere. Der Zugriff Dritter auf die Daten des Klägers sei nur deshalb erfolgt, weil die Beklagte die sie betreffenden Grundsätze und Pflichten aus der DSGVO bewusst nicht eingehalten habe.
Der gesamte Datenschutzvorfall bestehe aufgrund einer Sicherheitslücke der Facebook-Plattform. So seien die unbekannten Dritten nur wegen des nicht hinreichend gesicherten Contact Import Tools zur Korrelation zwischen Facebook-Profilen und deren Telefonnummern befähigt gewesen. Dabei habe ein Programm unzählige zufällige Zahlenfolgen in das „CIT“ eingegeben, um festzustellen, ob hinter dieser wahllosen Zahlenfolge eine mit einem Facebook-Konto verknüpfte Telefonnummer darstelle. Sei dies der Fall gewesen, habe das Programm sämtliche Daten des Nutzers abgefragt und in eine Liste exportiert.
Er behauptet weiter, dass das „Scraping“ nur möglich gewesen sei, weil die Beklagte keine ausreichenden Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten Contact Import Tools zu verhindern. So seien weder branchenübliche Sicherheitsmaßnahmen wie „Captchas“ oder eine Plausiblitätsüberprüfung der Anfragen im CIT eingerichtet gewesen. Weiter fehle zudem ein ausdrücklicher Hinweis der Beklagten, dass standardmäßig die Telefonnummer eines Nutzers von jedermann mit dessen Profil verknüpft werden kann.
Außerdem seien die Einstellungen zur Sicherheit bezüglich der Telefonnummer auf Facebook so undurchsichtig und kompliziert gestaltet, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne.
Die gesamte Facebook-Plattform sei datenschutzunfreundlich ausgerichtet. Der Registrierungsvorgang auf der Plattform sei bewusst undurchsichtig und verwirrend gestaltet. Dies diene u.a. dazu, dass Nutzer im Vertrauen und mit dem Ziel, mehr persönliche Sicherheit zu erreichen, ihre Telefonnummern preisgäben. Aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte und nicht ändere.
Eine Information über etwaige Risiken oder über die Verwendung der Telefonnummer erfolge nicht, obwohl ein Nutzer geradezu zur Verwendung des „CIT“ gedrängt werde. Dies widerspräche allerdings den Grundsätzen eines nutzerfreundlichen Datenschutzes und damit dem Prinzip der Datenminimierung und des „privacy by default“-Grundsatzes.

Weiter behauptet der Kläger, er hätte bei Kenntnis des Umstandes, dass seine Telefonnummer seinem Facebook-Profil zuordenbar ist, ohne dass er sie öffentlich freigegeben hat, keiner Datenschutzrichtlinie der Beklagten zugestimmt und sich auch nicht auf der Facebook-Plattform registriert.

Der Kläger trägt vor, dass die von ihm im „Scraping-Vorfall“ erlangten Daten insbesondere für gezielte Betrugsangriffe (u.a. „Phishing“) genutzt würden. Zudem könne zum jetzigen Zeitpunkt noch nicht abgesehen werden, welche Dritten Zugriff auf seine Daten erhalten hätten und für welche konkreten kriminellen Zwecke die Daten missbraucht würden. Er habe daher durch den Datenschutzvorfall ungewollt in erheblichem Ausmaß die Kontrolle über seine abgegriffenen Daten verloren und werde seitdem vermehrt von Unbekannten in bösartiger Absicht via E-Mail und SMS kontaktiert. Dadurch lebe der Kläger in einem Zustand von Unwohlsein und er habe große Sorgen über einen möglichen Missbrauch seiner Daten.

Soweit vorgerichtlich Auskünfte über abgegriffene Daten mitgeteilt worden seien, wie zum Beispiel mit Schreiben vom 28.10.2021, sei diese Auskunft ungenügend. Das Antwortschreiben der Beklagten enthalte lediglich allgemein gehaltene Informationen zu den auf Facebook verarbeiteten Daten sowie einen Link zur Seite der Beklagten, auf der die über einen individuellen Nutzer gespeicherten Daten eingesehen werden können. Unabhängig davon enthalte das „Auskunftsschreiben“ der Beklagten aber auch keinerlei konkreten Aussagen dazu, welche Daten der Klägerseite im Wege des „Scrapings“ von unbekannten Dritten abgegriffen wurden. So bleibe offen, wann genau die Daten entwendet worden seien oder wie viele verschiedene Beteiligte diese Funktion hinsichtlich seiner Daten ausgenutzt hätten.

Der Kläger ist der Ansicht, dass die Beklagte gegen Art. 13, 14, 15, 24, 25, 32, 33 und 34 DSGVO verstoßen habe und ihm dadurch ein kausaler immaterieller Schaden entstanden sei, der nach Art. 82 Abs. 1 DSGVO zu ersetzen sei.

Der Kläger beantragt:

1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 EUR nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.
2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen

Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,
   a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,
   b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei 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 EUR zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt:

Die Klage wird abgewiesen.

Die Beklagte trägt vor, dass die Daten weder durch Hacking, noch durch mangelnde Sicherheitssysteme der Beklagten in die Hände der Dritten gefallen seien. Vielmehr liege lediglich ein

automatisiertes massenhaftes Sammeln ohnehin öffentlicher, und damit nicht vertraulicher Daten vor. Die so abgegriffenen Daten seien im Einklang mit den jeweiligen Privatsphäre-Einstellungen der Nutzer für jedermann öffentlich auf deren Profil einsehbar gewesen. Daten wie „Bundesland“, „Geburtsort“ und „weitere korrelierende Daten“ seien nicht durch das „Scraping“ erlangt, da diese schon nicht den Profilfeldern auf der Plattform entsprächen.
Der Kläger habe zudem ein fehlerhaftes Verständnis für den „Scraping-Vorfall“. Der Vorfall sei nicht nur durch das CIT der Beklagten, insbesondere nicht durch das wahllose Eingeben zufälliger Nummernfolgen erfolgt. Vielmehr hätten den Scrapern bereits konkrete Telefonnummern zur Verfügung gestanden, die sie nur in das CIT eingegeben hätten.

Der Kläger sei sowohl über die Einstellungsmöglichkeiten als auch über mögliche Konsequenzen seiner Einstellungen hinreichend durch die Beklagte informiert worden. Er habe sich, in Kenntnis der Datenschutzbestimmung der Beklagten, dazu entschieden bestimmte Daten öffentlich einsehbar auf seinem Facebook-Profil zu teilen. Es habe eine umfassende und verständliche Information über die Möglichkeit der Anpassung der „Suchbarkeits-Einstellungen“ und „Zielgruppenauswahl“ gegeben, woraus sich nachvollziehbar ergebe, wer bestimmte persönliche Informationen, die der Nutzer in seinem Profil hinterlegt habe, einsehen könne. Die Standard-Voreinstellungen der Beklagten seien notwendig, um den Hauptzweck der Facebook-Plattform, die Vernetzung von Menschen, zu ermöglichen.

Die Beklagte habe hinreichende technische und organisatorische Maßnahmen ergriffen, um das Risiko von „Scraping“ zu unterbinden. Der Kläger habe unsubstantiiert dazu vorgetragen, welche Maßnahmen die Beklagte konkret hätte erbringen müssen. Zudem müsse die Beurteilung der Angemessenheit der Sicherungsmaßnahmen ex ante und nicht ex post erfolgen. Es sei grundsätzlich unmöglich, das „Scraping“ öffentlich einsehbarer Daten völlig zu verhindern, ohne den Kommunikationszweck der Plattform zu unterlaufen. Zur Bekämpfung von „Scraping“ beschäftige die Beklagte ein Team von Datenwissenschaftlern, Analysten und Softwareingenieuren. Die Beklagte habe in Zusammenarbeit mit diesem External Date Misuse Team alle notwendigen Sicherheitsvorkehrungen zur Beschränkung von „Scraping“ getroffen. Ferner gehe die Beklagte grundsätzlich mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren gegen „Scraper“ und Hosting-Anbieter, also Unternehmen, auf deren Systemen die Daten zur Verfügung gestellt werden, vor.

Letztlich sei der vorgetragene Kontrollverlust des Klägers über seine abgegriffenen Daten kein erstattungsfähiger Schaden. Die abgegriffenen Daten würden nicht die Gefahr von schwerwiegenden Internetverbrechen erhöhen, da dafür weitaus sensiblere Daten benötigt werden wür-

den. Selbst wenn der Kläger einem solchen Kontrollverlust unterliege, sei dies nicht der Beklagten zuzurechnen, da vorliegend nur ohnehin öffentlich einsehbare Daten abgegriffen worden seien. Außerdem fehle es an hinreichendem Vortrag zur Kausalität der behaupteten Datenschutzverletzungen und der daraus resultierenden Folgen.

Die Beklagte ist der Ansicht, dass die klägerischen Anträge zu 1) und 3) zu unbestimmt und daher unzulässig seien. Dem klägerischen Antrag zu 2) fehle bereits das notwendige Feststellungsinteresse. Weiter sei der mit dem Antrag zu 4) geltend gemachte Auskunftsanspruch bereits außergerichtlich, nämlich mit Schreiben vom 28.10.2021 erfüllt worden.

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

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die gewechselten Schriftsätze der Parteien nebst Anlagen Bezug genommen. Die Kammer hat den Kläger persönlich informatorisch angehört. Wegen des Ergebnisses der Parteianhörung wird auf das Protokoll zur mündlichen Verhandlung vom 23.01.2023 Bezug genommen.

Entscheidungsgründe

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

A.

Die Klage ist zulässig.

I.

Insbesondere sind die klägerischen Anträge zulässig.

1.

Der klägerische Antrag zu 1) ist zulässig.

Er ist im Sinne des § 253 Abs. 2 ZPO hinreichend bestimmt.

Der Streitgegenstand wird bestimmt durch die mit dem Klageantrag begehrte Rechtsfolge und den zugrundeliegenden Lebenssachverhalt (BGH NJW 2016, 1818 Rn. 27; NJW 2010, 2210 Rn. 10). Dabei gehören alle Tatsachen zu einem Klagegrund im Sinne des § 253 Abs. 2 Nr. 2 ZPO, die nach den Maßstäben des Lebens einen einheitlichen Vorgang bilden. Unter einem Klagegrund sind somit alle Tatsachen zu verstehen, die bei einer natürlichen, vom Standpunkt der Parteien ausgehenden Betrachtungsweise zu dem vom Kläger dem Gericht unterbreiteten Tatsachenkomplex gehören (BGHZ 117, 1 (5) = NJW 1992, 1172; BGHZ 123, 137 (141) = NJW 1993, 2684; BGH NJW 1996, 3151 (3152); BGHZ 157, 47 (51) = NJW 2004, 1252 (1253).

a.
Der Klageantrag zu 1) fußt – entgegen der Ansicht der Beklagten – nicht auf zwei verschiedenen Lebenssachverhalten, welche in einem unbestimmten alternativen Verhältnis zueinander stehen.

Der Kläger begehrt mit seinem Antrag zu 1) einen Schadensersatzanspruch aufgrund des Vorgangs, der sich von seiner Registrierung bei der Facebook-Plattform über den streitgegenständlichen Datenschutzvorfall und der Veröffentlichung der daraus gewonnenen Daten bis zu einer angeblich unzureichenden Information des Klägers durch die Beklagte über diesen Vorfall zieht. Diesem Vorgang gemein sind die Daten, die der Kläger bei der Registrierung bei Facebook hinterlegt hat. Eine Aufteilung in mehrere Einzelabschnitte würde eine unnatürliche Auftrennung eines einheitlichen Lebensvorganges bilden.

b.
Der Bestimmtheit des Antrag zu 1) steht auch nicht entgegen, dass der Kläger die Höhe des begehrten Schmerzensgeldes in das Ermessen des Gerichtes gestellt hat.

Die Stellung eines nicht konkret bezifferten Zahlungsantrages ist ausnahmsweise dann zulässig, wenn die Bezifferung des begehrten Geldbetrages von einer gerichtlichen Schätzung im Sinne des § 287 ZPO oder vom billigen Ermessen des Gerichts abhängig gemacht wird. In diesem Fall hat der Kläger in seiner Klagebegründung die Berechnungs- bzw. Schätzungsgrundlage umfassend darzulegen (BGHZ 4, 138) und die Größenordnung seiner Vorstellung anzugeben (BGH, VersR 77, 861).

Der Kläger hat in seinem Antrag zu 1. einen begehrten Mindestbetrag von 1.000,00 EUR ange-

geben. Weiter hat er in seiner Klagebegründung dargestellt, auf welche Verstöße gegen die DSGVO er das begehrte Schmerzensgeld stützt.

2.
Weiter ist der mit dem Antrag zu 2) geltend gemachte Feststellungsantrag zulässig.

Er ist sowohl hinreichend bestimmt (a), als auch liegt beim Kläger das dafür erforderliche Feststellungsinteresse vor (b).

a.
Der Klageantrag muss aus sich heraus verständlich sein, den Umfang des begehrten Rechtsschutzes nennen und den Antrag so konkret bezeichnen, dass der Inhalt und Umfang der begehrten Entscheidung ersichtlich ist (MüKo ZPO/*Becker-Eberhard*, 6. Aufl. 2020, § 253 Rn. 88).

Diesen Voraussetzungen wird der Antrag zu 2) gerecht.

Soweit die Beklagte darauf abstellt, dass der Antrag unverständlich sei, da nicht erkenntlich sein soll, ob damit lediglich zukünftige oder bereits in der Vergangenheit entstandene Schäden erfasst werden sollen, kann dieser Ansicht nicht gefolgt werden. Aus dem Wortlaut des Antrags ergibt sich eindeutig, dass der Kläger damit den Ersatz zukünftiger (also momentan noch nicht entstandener) Schäden begehrt, die auf dem bereits vergangenen Ereignis des Datenschutzvorfalles beruhen. Durch den Bezug auf den „Scraping-Vorfall“ findet gerade eine Konkretisierung des Antrags statt. Eine andere Deutung verbietet sich hier.

b.
Der Kläger hat auch sein Feststellungsinteresse nach § 256 Abs. 2 ZPO hinreichend dargelegt.

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

Die im Zusammenhang mit dem „Scraping“ erlangten personenbezogenen Daten des Klägers sind im Jahr 2021 im Internet veröffentlicht worden. Bei verständiger lebensnaher Würdigung erscheint es somit nicht ausgeschlossen, dass der Kläger aufgrund der Veröffentlichung seiner Telefonnummer in Verbindung mit persönlichen Daten einen irgendwie gearteten Schaden durch die missbräuchliche Nutzung dieser Daten erleidet. In diesem Zusammenhang kann auch nicht ausgeschlossen werden, dass der Kläger bereits Schädigungen erlitten hat, die ihm lediglich noch nicht bekannt geworden sind. Weiter ist auch nicht davon auszugehen, dass die Schadensentwicklung ein Ende gefunden hat. Dies insbesondere vor dem Hintergrund, dass zwischen dem „Scraping“ und der Publizierung der daraus gewonnenen Daten ein Zeitraum von etwa zwei Jahren lag. Daraus wird ersichtlich, dass diesem Vorfall ein Gefährdungspotential inne liegt, welches weder in zeitlicher, noch in inhaltlicher Hinsicht vollständig ausgeschlossen werden kann.

3.
Letztlich weist auch der klägerische Antrag zu 3) die erforderliche Bestimmtheit auf, § 253 Abs. 2 ZPO.

Der Beklagten ist zuzugestehen, dass die Formulierung „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ auslegungsfähig- und bedürftig ist. Dies führt entgegen ihrer Ansicht aber nicht zu dessen Unzulässigkeit.

Ein Unterlassungsantrag darf nicht derart unklar formuliert sein, dass der Streitgegenstand und damit die Prüfungs- und Entscheidungsbefugnis des Gerichts nicht erkennbar abgegrenzt sind und somit die Beklagte sich deswegen nicht erschöpfend verteidigen kann und die endgültige Entscheidung über das begehrte klägerische Unterlassen dem Vollstreckungsgericht obliegt (BGH, Urt. v. 21.5.2015 – I ZR 183/13). Ein der Auslegung bedürftiger Antrag ist jedoch dann zulässig, wenn dies zur Gewährleistung effektiven Rechtsschutzes erforderlich ist, weil dem Kläger eine weitergehende Konkretisierung nicht möglich ist (st. Rechtsprechung, vgl nur BGH, GRUR 2017, 422; GRUR 2012, 945; GRUR 2013, 421, GRUR 2014, 791).

Gemessen an diesen Voraussetzungen ist der klägerische Antrag zu 3a) trotz seiner Auslegungsbedürftigkeit hinreichend bestimmt.

Im Zusammenhang mit der Klagebegründung wird deutlich, dass der Kläger mit dem Antrag zu 3a) die Einrichtung von Sicherheitsmechanismen von der Beklagten verlangt, die zukünftige „Scraping-Vorfälle“ vorbeugen würden. Der Kläger verweist zutreffend darauf, dass es ihm

nicht möglich ist, den aktuellen Stand der Technik bezüglich möglicher Sicherheitsmaßnahmen selbst zu ermitteln und einzuschätzen. Zudem ist es gerade die Aufgabe der Beklagten, hinreichende Sicherheitsmaßnahmen einzurichten. Dem Kläger ist es weder zuzumuten, noch darf er der Beklagten die konkrete Umsetzung der Einhaltung der gesetzlichen Sicherheitsstandards vorschreiben. Letztlich würde eine Benennung „aktueller“ Sicherheitsmaßnahmen durch den Kläger dazu führen, dass aufgrund fortschreitender technischer Entwicklungen ebendiese Maßnahmen alsbald wieder „veraltet“ wären, was wiederum erneute rechtliche Schritte des Klägers zur Folge hätte. Dies kann weder im Interesse der Parteien sein, noch wäre dies im Hinblick auf den Gedanken des effektiven Rechtsschutzes nach Art. 19 GG vertretbar.

Der Kläger hat auch ein Rechtsschutzbedürfnis hinsichtlich des Antrags zu 3a). Er kann sein begehrtes Ziel nicht auf einfachere Weise erreichen, insbesondere hat er keine andere Handhabe gegen die von der Beklagten ergriffenen Sicherheitsmaßnahmen und das dadurch erreichte Schutzniveau. Der Umstand, dass der Kläger einseitig seine Privatsphäre-Einstellungen ändern kann, rechtfertigt keine abweichende Bewertung.

Nichts Anderes kann für den Antrag zu 3b) gelten.

II.

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

1.
Das Landgericht Chemnitz ist zunächst gem. Art. 6 Abs. 1, Art. 18 Abs. 1 Alt. 2 EuGVVO international zuständig.

Ein ausschließlicher Gerichtstand 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 entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat.

a.

Gemäß Art. 1 Abs. 1 EuGVVO ist die EuGVVO sachlich anwendbar auf Zivil- und Handelssachen. Vorliegend handelt es sich um eine Zivilsache.

b.

Der Kläger ist gemäß Art. 17 Abs. 1 lit. c EuGVVO Verbraucher. Er gibt an, einen Nutzungsvertrag mit der Beklagten über die Nutzung der Facebook-Plattform mittels eines Benutzerkontos zu privaten Zwecken geschlossen zu haben. Als doppelrelevante Tatsache genügt in der Zulässigkeit das Behaupten von Tatsachen, aus denen sich ein solcher vertraglicher Anspruch ergeben kann.

c.

Die Beklagte übt eine gewerbliche Tätigkeit auf dem Gebiet der Europäischen Union dadurch aus, dass sie die Facebook-Plattform zur Nutzung anbietet.

d.

Der Kläger hat seinen Wohnort in der Stadt Hainichen in Deutschland. Insoweit ist die deutsche Gerichtsbarkeit zuständig.

2.

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

a.

Hinsichtlich des Antrags zu 1) war der dort begehrte Zahlbetrag in Ansatz zu bringen.

b.

Hinsichtlich des Feststellungsantrags zu 2) hat die Kammer einen 50%-igen Abschlag von dem mit Ziffer 1) begehrten Zahlbetrag zur Bezifferung vorgenommen.

c.

Hinsichtlich der Höhe des Antrags zu 3) hat die Kammer im Sinne des § 3 ZPO insbesondere auf Tragweite und Umfang des Streitgegenstands abgestellt.

Der Streitwert bei nicht vermögensrechtlichen Streitigkeiten ist letztlich anhand aller Umstände des Einzelfalls, insbesondere auch anhand der Einkommensverhältnisse und der Bedeutung der Sache, zu bemessen. Die Bedeutung der Sache ist auf Grund der Vielzahl der vom Kläger abgegriffenen personenbezogenen Daten und der Ungewissheit über deren weitere konkrete –

auch missbräuchliche - Verwendung erheblich.

d.
Hinsichtlich des Antrags zu 4) ist ein Streitwert von 500,- € angemessen, da es noch um restliche Auskünfte ging.

3.
Die örtliche Zuständigkeit folgt aus Art. 18 Abs. 1 2. Alt. EuGVVO.

Danach kann die Klage eines Verbrauchers gegen die Vertragspartei entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat.

Das ist hier das Landgericht Chemnitz, da der Kläger als Verbraucher (s.o.) in Hainichen und damit im Gerichtsbezirk des angerufenen Gerichts wohnt.

B.

Die Klage ist in dem aus dem Tenor ersichtlichen Umfang begründet.

I.

Dem Kläger steht gegen die Beklagte ein Schadensersatzanspruch in Höhe von 500,00 EUR gem. Art. 82 Abs. 1 DSGVO zu.

Nach dieser Vorschrift hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen.

1.
Der Anwendungsbereich der DSGVO ist sowohl persönlich, räumlich als auch sachlich hinsichtlich Art. 82 DSGVO eröffnet.

a.

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

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

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

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

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

Der Ansicht der Beklagten, dass im Rahmen des Anwendungsbereiches von Art. 82 Abs. 1 DSGVO eng auf den Begriff der „Datenverarbeitung“ abzustellen ist, ist nicht zu folgen.

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

Dies trifft auch auf die Verletzung des Art. 25 Abs. 2 DSGVO durch die Beklagte zu (vgl. Sydow/Marsch/*Mantz*, DS-GVO/BDSG 3. Aufl., DSGVO Art. 25 Rn. 77; Paal/Pauly/*Martini*, DS-GVO, 3. Aufl., Art. 25 Rn. 6).

2.
Die Beklagte hat im Zusammenhang mit dem streitgegenständlichen „Scraping-Vorfall“ als

Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO gegen Art. 13, 14, 25 Abs. 2, 32, 33 und 34 DSGVO verstoßen.

a.
Die Beklagte hat durch die Ausgestaltung ihrer standardmäßigen Voreinstellungen gegen ihr obliegende Verpflichtungen aus Art. 25 Abs. 2 DSGVO verstoßen.

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

Durch standardmäßige Voreinstellungen („privacy by default“) soll sichergestellt werden, dass nur diejenigen personenbezogenen Daten von dem Verarbeiter erhoben werden, die für den jeweiligen Verarbeitungszweck notwendig sind (Sydow/Marsch/*Mantz,* DS-GVO/BDSG 3. Aufl., DS GVO Art. 25 Rn. 3,7). Dadurch sollen die Nutzer geschützt werden, die sich nicht von selbst dazu veranlasst sehen, datenschutzfreundliche Einstellungen einzurichten, obwohl ihnen prinzipiell die Möglichkeit dazu vom Diensteanbieter eröffnet wird (Paal/Pauly/*Martini,* DS-GVO 3. Aufl., Art. 25 Rn. 13). Der Nutzer soll selbst aktiv werden, um von datenschutzfreundlichen Voreinstellungen abzurücken. So soll der Nutzer vor ihm unbewussten Datenerhebungen geschützt und eine Verfügungshoheit über seine Daten möglichst erhalten werden.

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

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

aa.

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

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

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

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

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

Nach dem eigenen Vortrag der Beklagten dient die von ihr betriebene Facebook-Plattform dazu, Menschen miteinander zu verbinden und Kommunikation zwischen ihnen zu ermöglichen. Zwar ist der Verarbeiter in der Wahl seines Verarbeitungszweckes frei (Paal/Pauly/*Martini,* DS-GVO 3. Aufl., Art. 25 Rn. 45c). Für die Erreichung dieses kommunikativen und verbindenden Verarbeitungszweckes war es nach Ansicht der Kammer jedoch nicht erforderlich, dass

die „Suchbarkeits-Einstellung“ der bei Facebook hinterlegten Telefonnummer „Alle“ war. Zwar mag es dem Verarbeitungszweck der Beklagten nützlich sein, wenn die Nutzer der Facebook-Plattform auch über ihre hinterlegte Telefonnummer aufgefunden werden können. Für die Kammer erscheint es aber fernliegend, dass sich der kommunikative und verbindende Zweck der Facebook-Plattform ohne die Auffindbarkeit eines Facebook-Users über seine Telefonnummer nicht erreichen lässt. Das Wissen um eine Mobilfunknummer einer anderen Person spricht bereits deutlich dafür, dass sich diejenigen Personen bereits kennen. Selbst wenn dies nicht namentlich der Fall sein sollte, ließe sich eine Kontaktaufnahme unter Zuhilfenahme ebendieser Telefonnummer bewerkstelligen, ohne dass dafür auf die Facebook-Plattform und deren CIT zugegriffen werden müsste. Eine Suche über Facebook erübrigt sich in diesem Fall. Die Möglichkeit der Suche eines anderen Facebook-Nutzers mittels dessen Telefonnummer stellt somit lediglich einen zusätzlichen Nutzer-Service dar, der zur Erreichung der selbst deklarierten Zwecke der Beklagten nicht erforderlich ist und darüber hinaus auch Datenmissbrauch mittels Scraping ermöglicht.

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

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

dd.
Die rechtliche Bewertung der Kammer wird indiziell auch durch die Entscheidung der irischen Datenschutzbehörde DPC gestützt.

Diese hat am 28.11.2022 gegen die Beklage u.a. wegen eines Verstoßes gegen Art. 25 Abs. 2 DSGVO ein Bußgeld in Höhe von 265 Mio. Euro verhängt.

b.

Die Beklagte hat die ihr nach Art. 13 DSGVO auferlegten Informations- und Aufklärungspflichten verletzt. Sie hat den Kläger zum Zeitpunkt der Erhebung seiner Mobilfunknummer nicht im ausreichende Maße über die Zwecke der Erhebung bzw. Verarbeitung seiner Telefonnummer aufgeklärt.

aa.

Nach Art. 13 DSGVO treffen den Verantwortlichen eines Datenverarbeitungsprozesses zum Zeitpunkt der Erhebung von personenbezogenen Daten umfangreiche Informationspflichten. Diese Pflichten bestehen gegenüber der Person, deren personenbezogene Daten erhoben und verarbeitet werden.

Eine Verletzung dieser Pflicht besteht bereits dann, wenn der Verantwortliche der betroffenen Person nicht bereits bei Datenerhebung die nach Art. 13 Abs. 1 und 2 DSGVO erforderlichen Informationen vollständig und inhaltlich korrekt mitteilt.

Nach Art. 13 Abs. 1 lit. c) betrifft diese Informations- und Mitteilungspflicht auch die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen. Nach Erwägungsgrund 60 der DSGVO erfordern die Grundsätze einer fairen und transparenten Verarbeitung, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird.

Der Kläger gab im Rahmen seiner Registrierung auf der Facebook-Plattform seine Mobilfunknummer u.a. zum Zweck der Einrichtung einer „Zwei-Faktor-Authentifizierung“ an.

Bei der Mobilfunknummer des Klägers handelt es sich um ein personenbezogenes Datum gemäß Art. 4 Nr. 1 DSGVO. Bei der Hinterlegung der Telefonnummer in seinem Facebook-Profil wurde der Kläger durch die Beklagte darüber informiert, dass diese für verschiedene Zwecke benutzt wird (Anlagen B5, 6, 7, 9, 18, 19 und 20).

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

(1)

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

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

(2)
Eine solche Aufklärung lässt sich zunächst nicht aus der Datenschutzrichtlinie der Beklagten (Anlage B9) entnehmen.

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

(3)
Weiter kann eine im Sinne des Art. 13 Abs. 1 lit. c DSGVO hinreichende Information der Beklagten gegenüber dem Kläger hinsichtlich der Verwendung der Telefonnummer für das CIT auch nicht in dem Reiter „Handy-Einstellungen“ (S. 15 der Klage vom 23.03.2022) und dem Unterreiter „Mehr dazu“ (S. 16 der Klage vom 23.03.2022) gesehen werden.

Der Bereich „Handy-Einstellungen“ enthält allgemein gefasste Informationen über die Verwendungsmöglichkeiten der bei Facebook hinterlegten Mobilnummer. Im Bereich „Mehr dazu“ erfolgt der Hinweis, dass durch die Hinterlegung der Telefonnummer diese mit dem Nutzer-Profil verknüpft ist, dass die Nummer für Sicherheitsfeatures („zweistufige Authentifizierung oder SMS Warnungen“), um Menschen kennenzulernen oder für Werbezwecke verwendet wird. Auf den beiden Reitern findet sich demnach weder ein konkreter noch ein abstrakter Hinweis auf die Verwendung der preisgegebenen Telefonnummer für das CIT der Beklagten.

Am Ende des Reiters „Mehr dazu“ finden sich Verlinkungen zu „Du kannst festlegen, wer dei-

ne Telefonnummer sehen kann“, worunter sich Angaben zur „Zielgruppenauswahl“ finden und „wer auf Facebook nach dir suchen kann“. Dort findet sich unter anderem die Angabe: „Mit den Einstellungen Wer kann dich anhand der angegebenen Telefonnummer finden? und Wer kann dich anhand der angegebenen E-Mail-Adresse finden? legst du fest, wie deine Handynummer oder E-Mail-Adresse genutzt wird, um dich anders als über die Suche zu finden, z. B. wenn jemand deine Kontaktinformationen vom Handy auf Facebook hochlädt.“ Das ist der einzig auffindbare Hinweis, der konkret auf die mögliche Verwendung der hinterlegten Telefonnummer für das CIT abstellt.

Nach Ansicht der Kammer wird diese Information jedoch nicht der der Beklagten obliegenden Informationspflichten nach Art. 13 Abs.1 lit. c DSGVO gerecht.

In diesem Rahmen muss der Verantwortliche, hier die Beklagte, der betroffenen Person, hier dem Kläger, mitteilen, zu welchem Zweck sie ihre personenbezogenen Daten, hier die klägerische Mobilfunknummer, verarbeiten will. Die Mitteilung über die Zwecke der Verarbeitung der erhobenen personenbezogenen Daten ist für die Transparenz der Verarbeitung von hoher Bedeutung (Paal/Pauly/Paal/*Hennemann* DSGVO 3. Aufl., Art. 13 Rn 16). Die Angaben dazu müssen nicht nur vollständig, sondern auch so detailliert sein, dass sich der Kläger ausmalen kann, mit welcher Datenverarbeitung er zu rechnen hat (Kühling/Buchner/*Bäcker*, DSGVO 3. Aufl., Art. 13 Rn 25; Ehmann/Selmayr/*Knyrim* DSGVO 2. Aufl., Art. 13 Rn 37).

Diesen Anforderungen wird die Beklagte vorliegend nicht gerecht. Sie verweist lediglich auf weitere Einstellungsmöglichkeiten, in denen reguliert werden kann, wie die hinterlegte Mobilnummer genutzt werden kann, um Facebook-Nutzer anders, als über die Suche zu finden; zum Beispiel, wenn jemand die „Kontaktinformationen“ vom seinem „Handy auf Facebook“ hochlädt.

Einerseits stellt die Beklagte hier nur allgemein auf Kontaktinformationen ab, ohne konkret auf die Verwendung der hinterlegten Mobilnummer einzugehen. Weiter wird daraus nicht ansatzweise die Verwendung der vom User hinterlegten Mobilnummer für das CIT ersichtlich. Dem Nutzer, der gerade im Zuge ist, seine personenbezogenen Daten preiszugeben, wird nicht hinreichend deutlich gemacht, dass jedermann, der zufällig oder nicht über diese Handynummer verfügt, durch das von der Beklagten bereitgestellte CIT sein Facebook-Profil ausfindig machen kann. Vielmehr impliziert die Formulierung „vom Handy auf Facebook hochlädt“ ein gewisses Näheverhältnis zwischen der die Kontaktinformation hochladenden Person und der diese Information betreffenden Person. Nach Ansicht der Kammer setzt das Vorhandensein

von „Kontaktinformationen“ privater Personen im Telefon einer anderen zumindest ein Mindestmaß von gegenseitiger Kenntnis voraus.

Die Möglichkeit, dass durch die Preisgabe der Telefonnummer über das CIT der Beklagten auch durch einen völlig Fremden ein Facebook-Profil ermittelt werden kann, wird dadurch nach Ansicht der Kammer unvollständig und intransparent dargestellt.

Im Übrigen findet sich kein Hinweis auf die Bedeutung der „Suchbarkeitseinstellungen“ in dem oben beschriebenen Zusammenhang.

Weitere Verlinkungen wie „Suche über die Telefonnummer“ und „Weitere Infos dazu, wie du festlegst, mit wem du deine E-Mail-Adresse oder Handynummer teilst“ oder „Privatsphäre, Datenschutz und Sicherheit“ -> „Deine Privatsphäre“ -> „Bestimme, wer dich finden kann“ erhalten keine Angaben zum CIT. Der bloße Verweis auf Einstellungsmöglichkeiten ersetzt nicht die detaillierte Darlegung des Verwendungszweckes der hinterlegten Mobilnummer (s.o.).

(4)
Ein detaillierter Hinweis der Beklagten der Verwendung der vom Nutzer hinterlegten Mobilfunknummer kann auch nicht in der von der Beklagten verfassten Informationen aus dem „Hilfebereich“, vorgelegt als Anlage B5 und 6 gesehen werden.

Selbst wenn man dies jedoch annehmen wollte, würden diese Informationen jedoch nicht zum einzig relevanten Zeitpunkt, dem Zeitpunkt der Datenerhebung (Paal/Pauly/Paal/*Hennemann* DSGVO 3. Aufl., Art. 13 Rn 12) gegenüber der betroffenen Person ergehen. Die von der Beklagten im „Hilfebereich“ zur Verfügung gestellten Informationen sind diesem Zeitpunkt nämlich nachgeschaltet.

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

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

c.

Die Beklagte hat weiter keine hinreichenden Sicherheitsmaßnahmen zur Verhinderung des streitgegenständlichen „Scraping-Vorfalls“ mittels des CIT vorgehalten und somit gegen Art. 32, 24, 5 Abs. 1 lit. f) DSGVO verstoßen.

aa.

Gemäß Art. 32 Abs. 1 DSGVO hat die Beklagte als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO 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.

Die von der Beklagten hinsichtlich des CIT behaupteten Schutzmaßnahmen werden diesen Anforderungen nicht gerecht.

Art. 32 DSGVO formt den allgemeinen Grundsatz der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit. f) DSGVO näher aus und konkretisiert die Datensicherheitsmaßnahmen des Art. 24 DSGVO. Regelungsgegenstand ist dabei die Datensicherheit, wobei Verarbeitungsprozessen ein angemessenes Schutzniveau für die Sicherheit personenbezogener Daten abverlangt wird. Durch geeignete technische und organisatorische Maßnahmen sollen nach Art. 32 DSGVO vor allem personenbezogene Daten davor geschützt werden, dass Dritte diese unbefugt oder unrechtmäßig verarbeiten. Denn nur wenn der Nutzer sich sicher sein kann, dass seine Daten nicht von unbefugten Dritten abgegriffen werden können, kann er auf die Wahrung seines Rechts vertrauen, dass es ihm obliegt, ob und innerhalb welcher Grenzen er persönliche Lebenssachverhalte offenbart. Art. 32 DSGVO legt dem Verantwortlichen daher im Interesse der Verarbeitungssicherheit Gewährleistungspflichten auf (Paal/Pauly/*Martin,i* DSGVO 3. Aufl. Art. 32 Rn. 1a).

Bei der Implementierung von nach Art. 32 Abs. 1 DSGVO geeigneten technischen und organisatorischen Maßnahmen sind wie bereits dargelegt der Stand der Technik, Implementierungskosten, Art und Umfang, Umstände und Zweck der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen als Faktoren zu berücksichtigen. Die Beklagte als Verantwortliche muss die Risiken ihrer jeweiligen Verarbeitung reflektieren und risikoadäquate Maßnahmen ergreifen, um ein möglichst hohes Maß an Verarbeitungssicherheit zu erreichen (Paal/Pauly/*Martini,* DSGVO 3.

Aufl. Art. 32 Rn. 3). Dabei hat sie nach Erwägungsgrund 4 der DSGVO die Grundsätze der Verhältnismäßigkeit zu beachten. Die oben genannten Abwägungsfaktoren sind dabei in die Prüfung der Verhältnismäßigkeit einzustellen, aber nicht notwendigerweise absolut zu befolgen (Gola/Heckmann/Piltz, DSGVO 3. Aufl., Art. 32 Rn. 13).

Dabei ist aber auch zu beachten, dass Art. 32 Abs. 1 DSGVO den Verantwortlichen nicht zu einem absoluten Schutz der personenbezogenen Daten verpflichtet. Das Schutzniveau muss dem jeweiligen Einzelfall angemessen sein, wobei Risiken nicht gänzlich ausgeschlossen werden können und dies auch nicht das maßgebliche Ziel der umzusetzenden Maßnahme ist (Gola/Heckmann/*Piltz*, DSGVO 3. Aufl., Art. 32 Rn. 11; Paal/Pauly/*Martini*, DSGVO 3. Aufl., Art. 32 Rn. 46).

Die Geeignetheit der Maßnahmen muss ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau bieten. In diesem Rahmen ist abzuwägen, wie groß die Risiken sind, die den Schutzgütern der betroffenen Personen drohen und als wie wahrscheinlich das Risiko eines Schadenseintrittes anzusehen ist. Daraus folgt, dass je größer die zu erwartenden Schäden sind, umso wirksamer die ergriffenen Schutzmaßnahmen sein müssen.

bb.
Die Beklagte ist der anhand der oben genannten Kriterien vorzunehmenden Risikoabwägung nicht hinreichend nachgekommen. Das von ihr zum Zeitpunkt des „Scraping-Vorfalls“ vorgehaltene Schutzniveau war in der Gesamtbetrachtung der Umstände des Einzelfalls nicht ausreichend. Dies gilt auch dann, wenn man die von der Beklagten vorliegend behaupteten „Anti-Scraping-Maßnahmen“ als wahr unterstellt.

(1)
Das von der Beklagten vorgehaltene CIT ermöglichte im hier relevanten Zeitraum unbekannten Dritten den unbefugten Zugang auf personenbezogene Daten im Sinne des Art. 32 Abs. 2 DSGVO.

Beim unbefugten Zugriff auf Daten geht die maßgebliche Handlung von den Datenempfängern (hier den „Scrapern“) aus (vgl. Kühling/Buchner/*Jandt* DSGVO 3. Aufl., Art. 32 Rn. 349). Die Beklagte hat durch das CIT die grundsätzliche Möglichkeit des Abrufs von personenbezogenen Daten (Mobilfunknummer und öffentlich einsehbare Daten auf dem Facebook-Profil des Klägers) durch die „Scraper“ ermöglicht.

Nach dem Vortrag der Beklagten soll das CIT zum Auffinden von persönlichen Kontakten wie Freunden und Familie auf der Facebook-Plattform genutzt werden. Die konkrete technische Ausgestaltung ermöglichte es jedoch Dritten, dass diese entgegen der Nutzungsbedingungen der Beklagten das CIT missbräuchlich nutzen konnten. Den „Scrapern“ war es möglich, mittels massenhafter Anfragen von deutschen Mobilfunknummern im CIT eine systematische Verknüpfung dieser Nummern zu den dazugehörigen persönlichen Profilen auf der Plattform der Beklagten herzustellen. So konnte der Datensatz „Telefonnummer“ mit den im Facebook-Profil befindlichen Informationen der jeweiligen Nutzer angereichert werden. Dadurch entstand ein kombinierter Datensatz, der später im sog. „Darknet“ veröffentlicht wurde und potenzielle Täter in die Lage versetzt, dass sie missbräuchliche Aktivitäten wie Phishing, Sim-Swap, Identitätsdiebstähle oder allgemeinen Datenmissbrauch begehen.

Das so von der Beklagten mittels des CIT geschaffenen Missbrauchsrisiko bezüglich der auf der Facebook-Plattform hinterlegten persönlichen Daten und der daraus folgenden Risiken der betroffenen Person erfordern ein dementsprechend hohes Schutzniveau. Die Höhe des hier geforderten Schutzniveaus rechtfertigt sich auch vor dem Hintergrund, dass hier nicht „nur“ auf erhobene und gespeicherte Daten zugegriffen wurde, sondern die Beklagte gerade eine Zugriffsmöglichkeit auf diese Daten geschaffen hat. Dabei kann die Beklagte nach der Ansicht der Kammer auch nicht damit gehört werden, dass es sich bei den abgegriffenen Daten nur um ohnehin öffentliche Daten der Nutzer handelte. Einerseits kann dies schon dahingehend in Frage gestellt werden, dass die Registrierung eines Nutzers bei Facebook zwingend davon abhängt, dass er diese „immer öffentlichen“ Daten angibt und damit eine zielgerichtete Veröffentlichung dieser Daten durch den Nutzer für das gesamte Internet insgesamt abwegig erscheint. Die Beklagte übersieht aber andererseits auch, dass vorliegend die nicht öffentlich einsehbare Mobilfunknummer des betroffenen Nutzers mittels des CIT mit seinen weiteren Daten verknüpft werden konnte. So wurde nicht nur die vorher nach der „Zielgruppenauswahl“ nicht öffentlich einsehbare Telefonnummer in die Öffentlichkeit gezwungen, sondern durch das CIT wurde den „Scrapern“ überhaupt erst ein massenweises Abgreifen und Zuordnen der öffentlichen Profildaten ermöglicht. Anders gesagt erscheint es nach Ansicht der Kammer vorliegend als äußerst fernliegend, dass die „Scraper“ ohne das CIT vorliegend manuell einzelne Facebook-Profile aufgesucht hätten und die dort öffentlichen Daten in gleicher Art abgegriffen hätten, insbesondere vor dem Hintergrund, dass ihnen dazu die Namen und damit die Auffindbarkeit abzugreifender Profile gefehlt hätte.

(2)

Hier bestand eine besonders hohe Gefahr der Veröffentlichung der zusammengetragenen Da-

ten, insbesondere die Verknüpfung von Name und Telefonnummer. Dies bestätigt sich vor allem vor dem Hintergrund des hier gegenständlichen „Scraping-Vorfalls“.

Weiter zu beachten ist auch, dass „Scraping“ schon nach dem Vortrag der Beklagten keine neue unerwartete Missbrauchsmethode darstellt, sondern vielmehr von der Beklagten als Betreiberin eines globalen sozialen Netzwerkes mit mehreren Milliarden Nutzern aus der ex-ante-Sicht schlicht zu erwarten gewesen ist. Im Hinblick darauf, wie naheliegend das Risiko einer „Scraping-Attacke“ für die Beklagte war, musste sie dahingehend ein angemessenes Schutzniveau für die personenbezogenen Daten ihrer Nutzer vorhalten.

Ebendies hat die Beklagte aber nicht vorgetragen.

Soweit die Beklagte darauf abstellt, dass sie gegen Scraper repressiv mittels Unterlassungsschreiben, etwaigen Kontosperren oder Gerichtsverfahren vorgehe, ist bereits anzumerken, dass diese Maßnahmen dem eigentlichen Missbrauch nachgelagert und damit bereits nicht mehr geeignet sind, den Zugriff auf die Daten und deren anschließende Veröffentlichung zu verhindern.

Zwar trägt die Beklagte weiter die teilweise Einschränkung des CIT vor. Zum Beispiel in der Form, dass ein EDM-Team, Übertragungsbeschränkungen des CIT oder dahingehende CAPTCHA-Abfragen implementiert wurden. Diese genannten Maßnahmen sind grundsätzlich auch geeignet den Schutz persönlicher Daten zu fördern. In Anbetracht des oben beschriebenen hohen Missbrauchsrisikos des CIT waren jedoch nach Ansicht der Kammer darüberhinausgehende Sicherheitsmaßnahmen erforderlich. Insbesondere gelingt es der Beklagten nicht zu begründen, warum es zu dem streitgegenständlichen Datenschutzvorfall kam, obwohl – nach ihrer Ansicht – ausreichende Maßnahmen gegen einen Scraping-Missbrauch bestanden.

Der Beklagten ist insoweit zuzustimmen, dass die vorliegende Betrachtung ex-ante erfolgen muss, jedoch rechtfertigt das nicht den Einsatz ungenügender Sicherungsmittel zum damaligen Zeitpunkt. So werden CAPTCHA-Abfragen bereits gängiger Weise bei weniger sensibler Daten verwendet. Das EDM-Team wird nach Vortrag der Beklagten erst dann tätig, wenn Hinweise auf einen „Scraping-Vorfall“ bestehen. Die Übertragungsbeschränkung war offensichtlich nicht ausreichend, um ein massenhaftes Abgreifen von Daten bei der Beklagten mittels CIT zu verhindern. Dabei ist weder ersichtlich, noch wird von der Beklagten vorgetragen, weshalb sie davon ausgehen durfte, dass gerade diese Sicherheitsmaßnahmen einen für diesen Einzelfall angemessenen Schutz bieten sollte.

(3)
Von der Beklagten wären daher im Hinblick auf die Sicherung des von ihr zur Verfügung gestellten CIT über die bereits implementierten Sicherheitsmaßnahmen hinausgehende Absicherungen gegen einen Scraping-Missbrauch notwendig gewesen.

So hätte die Beklagte beispielsweise das CIT so ausgestalten können, dass es gänzlich Fremden nicht oder nur äußerst erschwert möglich gewesen wäre, mittels ihnen unbekannten Telefonnummern eine Verbindung zu einem Facebook-Profil herzustellen. Beispielsweise hätte die Abfrage mittels des CIT zusätzlich zur angeforderten Telefonnummer auch noch die Angabe eines Namens erfordern können. Diese Angabe hätte zumindest impliziert, dass der die Mobilfunknummer hochladende CIT-Nutzer eine irgendwie geartete persönliche Beziehung zu der gesuchten Person aufweist (so auch LG Paderborn, Urteil vom 19.12.2022 - 2 O 236/22). Zwar kann nicht mit Sicherheit ausgeschlossen werden, dass auch dieser Name durch „Scraper“ zufallsgeneriert werden würde und dann passend zu einer zufälligen Nummer ein Suchergebnis auswirft. Jedoch würde dies eine zusätzliche Variable und damit eine zusätzliche Hürde darstellen und den Scraping-Prozess somit zumindest erschweren. Außerdem ist ein absoluter Schutz gegen Scraping weder nach übereinstimmenden Parteivortrag möglich, noch von Art. 32 Abs. 1 DSGVO gefordert. Zudem ist darin auch keine Beschränkung des Zweckes des von der Beklagten zur Verfügung gestellten CIT zu erkennen.

Die Beklagte implementierte weder einer zuvor genannten Schutzmaßnahme vergleichbare, noch eine von den klägerseits als tauglich angesehenen Begrenzungsmaßnahmen im relevanten Zeitraum. Vielmehr nahm die Beklagte den „Scraping-Vorfall“ erst als Anlass zur Nachbesserung ihres Sicherheitsniveaus, indem sie beispielweise einen „Social Connection Check“ einführte und in dem als Anlage B 11 vorgelegten Artikel „Scraping nach Zahlen“ „eine Reihe von Verbesserung“ nach dem gegenständlichen Vorfall aufführte.

(4)
Es ist letztlich auch nicht ersichtlich, weshalb weitergehende Schutzmaßnahmen des CIT für die Beklagte mit einem im Vergleich zum gewonnenen Schutzniveau unverhältnismäßigen Aufwand verbunden gewesen wäre.

Nach Ansicht der Kammer konnte von einem global agierenden IT-Unternehmen erwartet werden, dass es relativ leicht umsetzbare Maßnahmen gegen eine ihr bekannte Missbrauchsvorgehensweise vornimmt. Im Übrigen trägt die Beklagte auch nicht vor, dass ein erhöhtes Si-

cherheitsniveau für sie unverhältnismäßig belastend gewesen wäre, sondern nur, dass dies die Funktionalität der Plattform eingeschränkt hätte.

d.
Der Beklagten fällt zudem eine Verletzung ihrer Meldepflicht nach Art. 33 DSGVO zur Last.

Nach Art. 33 Abs. 1 S. 1 DSGVO meldet der Verantwortliche die Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der gemäß Art. 55 DSGVO zuständigen Aufsichtsbehörde. Diese Pflicht zur Meldung entfällt dann, wenn die eingetretene Verletzung nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Der Mindestinhalt der Meldung wird in Art. 33 Abs. 3 DSGVO normiert.

aa.
Die zuständige Datenschutzbehörde im Sinne des Art. 55 war die Irish Data Protection Commission DSGVO. Eine Meldung an sie erfolgte durch die Beklagte unstreitig nicht.

bb.
Weiter liegt eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 33 Abs. 1 DSGVO vor. Darunter ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, zu verstehen.

Es genügt dabei eine objektive Schutzverletzung. Ob der Verantwortliche die Datenschutzverletzung als solche erkennt und einstuft, ist im Rahmen des Art. 33 DSGVO unbeachtlich (BeckOK DatenschutzR/*Brink,* DSGVO Stand 01.02.2022, Art. 33 Rn. 27, 29). Umfasst sind davon also unbeabsichtigte Verletzungen wie Datenlecks, Hackerangriffe, Datendiebstähle oder das Abgreifen von Daten sowie die Zweckentfremdung von Daten bei bestehenden Zugriffsrechten (Ehmann/Selmayr/*Hladjk*, DSGVO 2. Aufl., Art. 33 Rn. 5; Schaffland/Wiltfang/*Schafflang/Holthaus*, Datenschutz-Grundverordnung Werkstand: 1. Ergänzungslieferung 2023, Art. 33 Rn. 9; Spindler/Schuster/*Laue*, DSGVO 4. Aufl., Art. 33 Rn. 7). Die Schutzverletzung kann dabei auch durch gezielte Angriffe von Dritten ausgehen (Ehmann/Selmayr/*Klabunde,* DSGVO 2. Aufl, Art. 4 Rn. 58). Die Verletzung des Schutzes personenbezogener Daten erfolgte dabei auch unter der Verletzung der Datensicherheit nach Art. 32 DSGVO (s.o.).

Eine solche Schutzverletzung ist durch das „Scrapen“ mittels des CIT bei der Beklagten zu sehen. Durch diesen Vorfall wurden, entgegen der Nutzungsbedingung der Beklagten, eine immense Anzahl an Daten abgegriffen und anschließend in einer nicht gesicherten Datenbank im Internet veröffentlicht. Damit wurden Daten, die auf den jeweiligen persönlichen Profilen der Facebook-Nutzer angegeben wurden, zweckentfremdet, um damit kriminellen Aktivitäten Vorschub zu leisten. Zwar waren die Daten Name, Facebook-ID und Geschlecht des Klägers vorliegend aufgrund seiner Privatsphäreeinstellungen auf seinem Profil öffentlich einsehbar. Jedoch liegt in der Verknüpfung dieser öffentlichen Daten mit der nicht öffentlich einsehbaren Mobilfunknummer des Klägers mittels des CIT und der anschließenden Veröffentlichung dieses Datensatzes im Internet ohne den Willen des Klägers ein Vorfall, der mit einem Datenleck oder Hackerangriff vergleichbar ist und somit eine Verletzung des Schutzes personenbezogener Daten darstellt (so auch LG Paderborn, Urteil vom 19.12.2022 - 2 O 236/22).

Der Umstand, dass „Scraping“ durch die Leitlinien des Europäischen Datenschutzausschusses nicht ausdrücklich als eine Verletzung des Schutzes persönlicher Daten genannt ist, ist unbeachtlich, da die Leitlinien nicht abschließend sind.

cc.
Die Meldepflicht der Beklagten nach Art. 33 Abs. 1 DSGVO war vorliegend auch nicht einzuschränken.

Die Verletzung des Schutzes personenbezogener Daten führt vorliegend zu einem Risiko für die Rechte und Freiheiten des Klägers. Dieses Risiko ist nach Erwägungsgrund 85 der DSGVO anzunehmen, wenn der betroffenen Person der Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile drohen.

Hier ist bereits beim Kläger ein Kontrollverlust über seine abgegriffenen Daten eingetreten (siehe dazu weiter unten).

e.
Weiter hat die Beklagte gegen Art. 34 Abs. 1 DSGVO verstoßen, indem sie als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO den Kläger als betroffene Person nicht unverzüglich von der

Verletzung des Schutzes seiner personenbezogenen Daten benachrichtigt hat, obwohl die Verletzung ein hohes Risiko für die persönlichen Rechte und Freiheiten des Klägers zur Folge hatte.

aa.
Nach Art. 34 DSGVO ist das Opfer der Sicherheitsverletzung im Sinne des Art. 4 Nr. 12 DS-GVO im Rahmen einer individuellen Adressierung ohne schuldhaftes Zögern nach Offenbarung der Verletzung zu informieren. Eine öffentliche Bekanntmachung reicht nicht aus (Paal/Pauly/*Martini,* DSGVO 3. Aufl., Art. 34 Rn. 47).

Der Kläger hat als von der Sicherheitsverletzung im Sinne des Art. 4 Nr. 12 DSGVO betroffene Person des „Scraping-Vorfalls“ (s.o.) keine individualisierte Benachrichtigung der Beklagten erhalten.

bb.
Die Verletzung des Schutzes der personenbezogenen Daten des Klägers hat voraussichtlich ein hohes Risiko für seine persönlichen Rechte und Freiheiten im Sinne des Art. 34 Abs. 1 DSGVO zur Folge.

Ein solches Risiko liegt vor, wenn zu erwarten ist, dass bei ungehindertem Geschehensablauf mit hoher Wahrscheinlichkeit ein Schaden für den Betroffenen eintritt. Dieses Risiko hat sich mit dem Schadenseintritt beim Kläger (siehe dazu auch unten) bereits realisiert. In diesem Fall ist es nicht maßgeblich, ob die Verletzung auch droht, einen hohen Schaden herbei zu führen (vgl. Paal/Pauly/*Martini,* DSGVO 3. Aufl., Art. 34 Rn. 30).

cc.
Für die Beklagte streitet auch keine Ausnahme nach Art. 34 Abs. 3 DSGVO.
Die Benachrichtigungspflicht entfällt vorliegend nicht schon nach Art. 34 Abs. 3 lit. a DSGVO, da die Beklagte keine geeigneten Sicherheitsvorkehrungen zum Schutz des CIT vor dessen missbräuchlicher Verwendung getroffen hat. Als geeignet kann eine Sicherheitsvorkehrung nur dann angesehen werden, wenn die Vorkehrungen ein hohes Risiko einer Sicherheitsverletzung ausschließen (Paal/Pauly/*Martini,* DSGVO 3. Aufl., Art. 34 Rn. 38). Dies war hier aber gerade nicht der Fall (s.o.).

Weiter war auch eine Benachrichtigung durch die Beklagte nicht nach Art. 34 Abs. 3 lit. c DS-GVO entbehrlich. Dies wäre nur dann der Fall, wenn die Benachrichtigung mit einem unver-

hältnismäßigen Aufwand für die Beklagte verbunden gewesen wäre.

Grundsätzlich kann sich bei einer Vielzahl von betroffenen Person ein unverhältnismäßig hoher Kosten- und Zeitaufwand des Benachrichtigungsverpflichteten ergeben. Sind jedoch die betroffenen Personen und deren E-Mail-Adressen dem zur Benachrichtigung Verpflichteten, wie vorliegend bekannt, kann nicht von einem unverhältnismäßigen Aufwand ausgegangen werden (Gola/Heckmann/*Reif,* DSGVO 3. Aufl., Art. 34 Rn. 17). Zwar kann die Pflicht zur individuellen Benachrichtigung auch dann entfallen, wenn die Betroffenen vergleichbar wirksam über eine öffentliche Publikation informiert werden. Eine Publikation auf der eigenen Homepage muss so exponiert und deutlich erkennbar sein, dass der betroffene Personenkreis quasi nicht umhinkommt, die Meldung auch tatsächlich wahrzunehmen (Gola/Heckmann/*Reif,* DSGVO 3. Aufl., Art. 34 Rn. 17). Eine Meldung im einem Blogeintrag erfüllt diese Kriterien gerade nicht (Artikel-29-Datenschutzgruppe, WP 250 rev.01 (Stand 6.2.2018), S. 24).

Bereits nach dem eigenen Vortrag ist die Beklagte diesen Anforderungen hier nicht gerecht geworden. Einerseits waren ihr sowohl die vom „Scraping-Vorfall“ betroffenen Personen und zwangsläufig deren E-Mail-Adressen bekannt, sodass eine individuelle Benachrichtigung für die Beklagte keinen unverhältnismäßig großen Aufwand nach sich gezogen hätte. Weiter veröffentlichte die Beklagte ihre (ersten) Erkenntnisse und Informationen lediglich in dem Artikel „Die Fakten zu Medienberichten über Facebook-Daten“ vom 06.04.2021 (Anlage B 10). Dieser wurde von der Beklagten lediglich auf ihrer Website im sog. „Newsroom“ und nicht so prominent platziert, dass er eine individuelle Benachrichtigungspflicht entbehrlich gemacht hätte.

dd.
Das Schreiben der Beklagten vom 28.10.2021 (Anlage B 16) erfolgte erst auf explizite Nachfrage des Klägers und damit keinesfalls „unverzüglich“.

f.
Der Beklagten fällt jedoch kein Verstoß gegen Art. 15 DSGVO zur Last, da dem Kläger eine Auskunft über seine von der Beklagten verarbeiteten personenbezogenen Daten mit Schreiben vom 28.10.2021 erteilt wurde.

aa.
Der Kläger hatte sich unter Zuhilfenahme der hiesigen Prozessbevollmächtigten mit Schreiben vom 04.08.2021 (K 1) an die Beklagte gewandt und Auskunft hinsichtlich konkret formulierter Fragen wegen des „im April 2021 bekannt gewordenen Datenschutzvorfall“ verlangt (K

1, S. 11). Die Fragen betreffen dabei die Verarbeitung personenbezogener Daten des Klägers durch die Beklagte und inwieweit Daten des Klägers vom streitgegenständlichen „Scraping-Vorfall“ betroffen waren.

bb.
Der Beklagten fällt dahingehend jedoch kein Pflichtverstoß zur Last, da sie mit Antwortschreiben vom 28.10.2021 der ihr nach Art. 15 DSGVO obliegende Pflicht zur Auskunft gegenüber dem Kläger vollständig nachgekommen ist.

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

Entscheidend ist damit, dass die erteilte Auskunft vom 28.10.2021 erkennbar den (berechtigten) Auskunftsanspruch des Klägers inhaltlich vollständig beantworten soll (so auch LG Paderborn, Urteil vom 19.12.2022 – 3 O 99/22).

Die Beklagte hat mit dem Schreiben vom 28.10.2021 dem Kläger mitgeteilt, dass sie keine Kopie der durch den „Scraping-Vorfall“ abgerufenen Daten hat. Dennoch stellte sie Datenpunkte zur Verfügung, die nach ihrem Verständnis in den durch Scraping abgerufenen Daten erscheinen. Darüber hinaus teilte sie dem Kläger mit, dass sie davon ausgehe, dass auch die klägerische Telefonnummer betroffen ist. Bezüglich der Verarbeitung personenbezogener Daten des Klägers durch sie verweist sie mittels Zurverfügungstellung eines Links auf die Möglichkeit, dass der Kläger diese Informationen jederzeit selbst einholen kann.
Die Beklagte hat damit im Gesamtbild dem Kläger konkludent angezeigt, seine Auskunft vollständig beantwortet zu haben. Ein darüber hinaus gehender Anspruch und somit eine Pflichtverletzung der Beklagten gegen Art. 15 DSGVO besteht nicht.

3.
Dem Kläger ist nach Auffassung der Kammer ein immaterieller Schaden in Höhe von 500,00 EUR gemäß Art. 82 Abs. 1 DSGVO entstanden.

a.

Der Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO dient nicht nur dem Ausgleich erlittenen Schadens, sondern auch repressiven und präventiven Zwecken, indem er Verstöße sanktioniert, weiteren Verstößen präventiv vorbeugt und vor zukünftigen Verstößen abschreckt (BeckOK DatenschutzR/*Quaas,* DS-GVO Stand: 01.08.2022, Art. 82 Rn. 1).

Der Kläger ist dabei als natürliche Person, der ein immaterieller Schaden entstanden ist (s.u.) anspruchsberechtigt, die Beklagte als Verantwortliche (s.o.) anspruchsverpflichtet.

b.
Es kann vorliegend dahinstehen, ob für eine Ersatzpflicht nach Art. 82 Abs. 1 DSGVO bereits ein Verstoß gegen eine Norm der DSGVO genügt (so: BAG, Beschluss vom 26.08.2021 – 8 AZR 253/20 (A)), oder ein konkreter Schaden des Klägers vorliegen muss (zum Ganzen OLG Frankfurt a.M., Urteil vom 02.03.2022 – 13 U 206/20).

Der Kläger erlitt nach Ansicht der Kammer einen Schaden in Form eines Kontrollverlustes über seine während des „Scraping-Vorfalls“ abgegriffenen Daten.

aa.
Der Begriff des Schadens soll nach dem Erwägungsgrund 146 S. 3 DSGVO „im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht.“. Vom Schadensbegriff des Art. 82 Abs. 1 DSGVO ist damit auch das Unwohlsein des Betroffenen umfasst, welches daraus resultiert, dass personenbezogene Daten Dritten unbefugt bekannt geworden sind (OLG Frankfurt a. M. Urteil vom 14.04.2022 – 3 U 21/20; LG München I, Urteil vom 20.1.2022 – 3 O 17493/20; LAG Hamm Urteil vom 11.5.2021 – 6 Sa 1260/20; LAG Baden-Württemberg, Urteil vom 25.02.2021 – 17 Sa 37/20).

Dies gilt umso mehr dann, wenn nicht ausgeschlossen werden kann, dass die fraglichen Daten nicht auch weiterverwendet werden. Die schadensersatzrechtliche Sanktionierung rechtfertigt sich dadurch, dass der Verlust über die Kontrolle der personenbezogenen Daten für die Betroffenen zu einem Gefühl von Ausgesetztheit gegenüber unbekannten Dritten führt, ohne dass die Betroffenen eine eigene Einflussmöglichkeit darauf haben. Die Betroffenen werden im Ergebnis damit zu einem Objekt der Datenverarbeitung reduziert (Kühling/Buchner/*Bergt*, DSGVO 3. Aufl., Art. 82 Rn. 18b).

Der Erwägungsgrund 75 zur DSGVO benennt den Kontrollverlust ausdrücklich als zu erwar-

tendes Risiko der Verarbeitung personenbezogener Daten, das zu einem Schaden bei den Betroffenen führt, indem es dort heißt: „Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere (…) wenn die betroffenen Personen (…) daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren“.

Würde ein Schaden erst dann angenommen werden, wenn es durch das Abgreifen der Daten zu einer vertieften vermögens- oder persönlichkeitsrechtlichen Verletzung des Betroffenen kommt, würde das dem weit auszulegenden Schadensbegriff und dem damit verbundenen individuellen Ausgleichsanspruch entgegenstehen (vgl. OLG Koblenz Urteil vom 18.05.2022 – 5 U 2141/21).

Als weitere Schäden in diesem Zusammenhang kommen zudem Angst, Stress und Zeiteinbußen in Betracht.

An die Darlegung dieses Schadens dürfen keine überhöhten Anforderungen gestellt werden. Gerade für Persönlichkeitsrechtsverletzungen ist es typisch, dass keine bezifferbare Vermögensminderung eintritt, sondern sich der Schaden vielmehr in seelischem Unwohlsein ausdrückt (Dickmann r + s 2018, 345 (353)). Dabei kann nicht vom Betroffenen erwartet werden, dass er konkrete Angaben dazu macht, wie sich der Kontrollverlust auf seine persönliche Lebensgestaltung ausgewirkt hat (Kühling/Buchner/*Bergt*, DSGVO 3. Aufl., Art. 82 Rn. 18b).

bb.
Der Kläger hat infolge des streitgegenständlichen „Scraping-Vorfalls“ und dem damit einhergehenden Kontrollverlust über seine dabei abgegriffenen Daten ein Unwohlsein erlitten.

Dies steht zur Überzeugung der Kammer aufgrund der informatorischen Anhörung des Klägers in der mündlichen Verhandlung vom 23.01.2023 fest.

Der Kläger gab an, dass er sich Sorgen darum gemacht habe, was mit seinen Daten nach dem „Scraping-Vorfall“ passiere. Insbesondere habe er befürchtet, dass seine Daten für missbräuchliche und betrügerische Zwecke verwendet würden. So zum Beispiel in Form von „Phishing-SMS“ oder „Scam-Anrufen“.

Nach Ansicht der Kammer sind die Schilderungen des Klägers glaubhaft. Er legt ohne Belas-

tungseifer gegenüber der Beklagten inhaltlich nachvollziehbar seine eigenen Erfahrungen dar. Er räumt dabei auch ein, Dinge nicht mehr zu wissen und beschränkt sich insbesondere nicht darauf, lediglich den Vortrag aus der Klageschrift zu wiederholen. Sein Vortrag gestaltete sich bildhaft und ohne inhaltliche Widersprüche.

cc.
Dieser Kontrollverlust hat sich auch in an den Kläger adressierten betrügerischen Anrufen und SMS in dem Zeitraum nach dem streitgegenständlichen Datenschutzvorfall manifestiert.

Dabei gab der Kläger an, dass er etwa ein Jahr, nachdem ihm der fragliche „Scraping-Vorfall“ durch Internetmedien bekannt wurde, vermehrt sogenannte „Scam“ -und „Spam-SMS“ auf sein Mobiltelefon erhalten habe. Er beschrieb dabei, dass der Inhalt dieser Nachrichten zum Teil so ausgestaltet gewesen sei, dass er Sendungsbenachrichtigungen von Paketdienstleistern mit weiterführenden Links erhalten habe, obwohl er gar keine Versandbestellungen bei diesen Dienstleistern aufgegeben hätte. Weiter habe er Anrufe von ihm unbekannten Nummern erhalten. Diese Art von Benachrichtigungen hätte er vor 2022 nicht erhalten. Die Anzahl der Anrufe und Nachrichten sei ab Oktober 2022 drastisch gesunken.

Die Kammer folgt auch diesen Ausführungen des Klägers. Er konnte im Rahmen der informatorischen Anhörung ohne Übertreibungen Art und Umfang der missbräuchlichen Benachrichtigungen lebendig beschreiben. Seine Aussage wird auch dadurch glaubhaft, dass er selbst einräumt, dass die SMS und Anrufe wieder abgeebbt sind, obwohl ein anderer Vortrag für seine Rechtsposition vorteilhafter gewesen wäre.

Soweit die Beklagte die Kausalität der Benachrichtigungen zum streitgegenständlichen Datenschutzvorfall bestreitet, kann dem vorliegend seitens des Gerichts nicht gefolgt werden. Zwar ist der Beklagten grundsätzlich zuzustimmen, dass die von dem Kläger beschriebenen SMS und Anrufe kein auf die Facebook-Plattform begrenztes Problem darstellen. Jedoch erfolgten diese Benachrichtigungen hier in plausibler zeitlicher Nähe zum Scraping bei der Beklagten. Weiter führte der Kläger überzeugend aus, dass er vor dem Vorfall – zumindest in der Quantität – nicht mit derartigen SMS und Anrufen konfrontiert war.

dd.
Die vom Kläger beschriebenen Anstrengungen im Wege der Nachverfolgung des Datenschutzvorfalles rechtfertigen nach Ansicht der Kammer jedoch keine schadensersatzrechtliche Sanktionierung der Beklagten.

Der Kläger gibt an, dass er Zeit aufgewendet habe, um Informationen über den streitgegenständlichen Vorfall zu gewinnen.

Selbst diesen Vortrag als wahr unterstellt, ist damit keine Einschränkung des Klägers in seiner privaten Lebensführung verbunden, die einen Schadenersatzanspruch gegen die Beklagte rechtfertigen würde. Nach seiner eigenen Angabe ist ihm der Datenschutzvorfall über Internetmedien bekannt geworden und das bereits bevor er mit dessen Auswirkungen konfrontiert wurde. Weitere zeitintensive Maßnahmen, die der Kläger durch das „Scraping“ seiner Daten ergreifen musste, sind nicht ersichtlich. Insbesondere hat der Kläger keine aufwendigen technischen Sicherungsmaßnahmen gegen eventuelle Betrugsmaßnahmen unternommen. Die Rechtsverfolgung und -durchsetzung erfolgte durch die hiesigen Prozessbevollmächtigen und war somit für den Kläger nicht mit nennenswertem (zeitlichen) Aufwand verbunden.

ee.
Soweit die Beklagte bestreitet, dass die im Rahmen des „Scraping-Vorfalls“ erlangten Daten im Darknet veröffentlicht wurden, rechtfertigt dies keine andere Bewertung.

Der hier schadensersatzauslösende Kontrollverlust des Klägers über dessen Daten verwirklichte sich bereits im Moment des Datenschutzvorfalls. Ab diesen Zeitpunkt sind aus Sicht des Klägers Daten im Kenntnis- und Verfügungsbereich ihm unbekannter Dritter. Die weitere Handhabung dieser Daten gestaltet sich für den Kläger ebenso willkürlich wie unkontrollierbar.

c.
Die nach den überzeugenden Ausführungen des Klägers sich aus dem „Scraping-Vorfall“ ergebenden Konsequenzen für ihn stellen nach Ansicht der Kammer eine über die Bagatellgrenze hinausreichende Beeinträchtigung dar.

Die über einen längeren Zeitraum erfolgten Anrufe und SMS, bei denen der Kläger bei eigener Unachtsamkeit mit negativen Konsequenzen rechnen musste, übersteigen das Maß einer lediglich unerheblichen Lästigkeit bei Weitem.

d.
Der erlittene Kontrollverlust des Klägers über seine im Rahmen des Scraping abgegriffenen persönlichen Daten ist kausal auf die oben beschriebenen Verletzungen der DSGVO durch die Beklagten zurückzuführen.

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

Eine alleinige Kausalität der Verstöße ist dabei nicht erforderlich, Mitursächlichkeit ist ausreichend (LAG Baden-Württemberg, Urteil vom 25.02.2021 -17 Sa 37/20, ZD 2021). Insoweit stellt es keinen kausalitätsdurchbrechenden Umstand dar, dass der Kläger seine Datenschutzeinstellungen nach seiner erstmaligen Registrierung bei der Facebook-Plattform nicht geändert hat.

e.
Der vom Kläger erlittene immaterielle Schaden war vorliegend auf 500,00 EUR zu bemessen.

Diese Summe erachtet des Gerichts im Rahmen des von ihm ausgeübten Ermessens nach § 287 Abs. 1 ZPO (vgl. BAG NJW 2022, 2779) als ausreichend, um sowohl der Ausgleichs- und Genugtuungsfunktion des Schadensersatzes gerecht zu werden und außerdem als hinreichend, um dem präventiven Charakter der Norm zu genügen.

aa.
Nach dem Erwägungsgrund 146 S. 6 der DSGVO soll der Betroffene einen vollständigen und zugleich wirksamen Ersatz für den von ihm erlittenen Schaden erlangen.

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

Unter Berücksichtigung der Erwägungsgründe 75 und 85 der DSGVO muss weiter beachtet werden, dass dem Schadenersatzanspruch auch eine abschreckende Wirkung gegenüber dem Verantwortlichen zukommen soll, um somit eine effektive Durchsetzung der DSGVO sicherzustellen.

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

bb.
Zu Lasten der Beklagten war zu berücksichtigen, dass ihr eine Vielzahl von Verstößen gegen die DSGVO zur Last fällt und in diesem Zusammenhang ein Kontrollverlust des Klägers über dessen personenbezogene Daten verursacht wurde, dessen Ausmaß und Umfang derzeit offen ist.

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

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

Eine besonders hohe persönliche Betroffenheit des Klägers vermag die Kammer jedoch nicht festzustellen.
Der Kläger hat, weder nachdem er Kenntnis über den „Scraping-Vorfall“ über Internetmedien erlangt, noch im Rahmen der Informationengewinnung durch die Einreichung seiner Klageschrift und der dieser zugrundeliegenden Begründung, Anstrengungen unternommen, um sich gegen aus dem Datenschutzvorfall drohende Missbrauchsrisiken zu schützen. So änderte der Kläger seine abgegriffene Telefonnummer nicht. Weiter hat er auch nicht sein Facebook-Profil gelöscht oder sonstige Schutzmaßnahmen ergriffen. Die Änderung der „Suchbarkeits-Einstellung“ seiner Telefonnummer erfolgte nach dessen eigenem Vortrag unabhängig vom fraglichen „Scraping-Vorgang“.

In der Gesamtschau wiegt der objektiv eingetretene Kontrollverlust des Klägers subjektiv nicht

so schwer, dass sich dieser zu Schutzmaßnahmen seiner Daten vor zukünftigen Missbräuchen veranlasst sah.

Weiter war zu berücksichtigen, dass dem Kläger bisher kein vermögensrechtlicher Nachteil entstanden ist.

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

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

Weiter ist zu sehen, dass es gerade im Interesse der Beklagten war, dass der Kläger die voreingestellten Datenschutzeinstellungen nicht ändert, da dies schon nach ihrem Vortrag Hinblick auf den Sinn und Zweck der Facebook-Plattform nicht gewünscht war. Realisieren sich dann aber die aus diesen Voreinstellungen resultierenden Gefahren – wie hier – kann dies nicht zu Gunsten desjenigen berücksichtigt werden, der diese Voreinstellungen vorgegeben und darüber hinaus über deren Gefahren nicht hinreichend aufgeklärt hat.

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

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

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

Im Zusammenhang des Zugriffs unberechtigter Dritter auf personenbezogene Daten liegt regelmäßig dann kein Verschulden des Verantwortlichen vor, wenn in dieser gemäß den Bestimmungen der DSGVO alle erforderlichen Sicherheitsmaßnahmen ergriffen hat (Paal/Pauly/*Frenzel,* DS-GVO 3. Aufl., Art. 82 Rn. 15). Erfolgt der Zugriff auf die Daten jedoch auf bekannten oder zumindest erkennbaren Angriffswegen, kann sich der Verantwortliche nicht entlasten (Kühling/Buchner/*Bergt,* DS-GVO 3. Aufl., Art. 82 Rn. 54).

Der Zugriff auf die klägerischen Daten erfolgte hier mittels des CIT durch Scraping. Nach dem Vortrag der Beklagten stellt Scraping eine „gängige Praxis dar“ und war ihr somit bekannt. Auch wenn der Beklagten zuzustimmen ist, dass ein völliger Schutz gegen Scraping-Angriffe nicht möglich ist, befreit sie das jedoch nicht von der Pflicht, alle erforderlichen Sorgfaltsmaßnahmen dagegen zu treffen. Dies konnte die Beklagte im hiesigen Prozess nicht nachweisen.

Die Beklagte vermag nicht konkret vorzubringen, wann sie welche Maßnahmen gegen das von ihr bekannte Risiko des Scrapings vorgenommen hat. Soweit sie vorträgt, dass sie das Scraping-Risiko ständig überwacht und kontinuierliche Maßnahmen entwickelt habe, um gegen Scraping vorzugehen, ist dieser Vortrag zu pauschal gehalten. Insbesondere wird daraus nicht deutlich, dass und warum die Beklagte davon ausgehen durfte, dass die von ihr getroffenen Maßnahmen zum jeweiligen Zeitpunkt das einzig erforderliche Sicherheitsinstrument waren.

Nach dem eigenen Vortrag der Beklagten konnte diese zunächst nicht die Scraping-Angriffe auf ihr CIT zurückführen. Die nach dieser Erkenntnisgewinnung eingeleiteten Maßnahmen waren offensichtlich ungeeignet, um einen Scraping-Missbrauch des CIT maximal einzuschränken. Insbesondere zeigt die schrittweise Implementierung immer weiterer Sicherheitsmaßnahmen, dass die Beklagte das Scraping-Risiko entweder unterschätzt hat, oder nicht bereit war, ihre Funktionalitäten im erforderlichen Maß zu Gunsten der Sicherheit ihrer Nutzer zu beschränken. In beiden Fällen muss jedoch angenommen werden, dass die Beklagte nicht alle erforderlichen Sicherheitsmaßnahmen gegen Scraping getroffen hat.

Soweit die Beklagte vorträgt, dass sie die ihr aus der DSGVO ergebenden Pflichten nicht verletzt habe, verfängt dieser Vortrag schon vor den obigen Ausführungen nicht.

4.
Der Zinsanspruch folgt aus §§ 288, 291 BGB, § 187 Abs. 1 BGB analog.

Eine Zustellung der Klageschrift kann mangels anderer Anhaltspunkte nicht vor der Anzeige der Verteidigungsbereitschaft der Beklagtenvertreter am 30.05.2022 angenommen werden.

II.

Der klägerische Antrag zu 2) ist begründet.

Es ist vorliegend nicht ausgeschlossen, dass der Kläger in Zukunft durch die Verstöße der Beklagten gegen die DSGVO weitere – auch materielle – Schäden erleidet.

III.

Dem Kläger steht gegen die Beklagte ein Anspruch auf Unterlassung der Zugänglichmachung seiner personenbezogenen Daten gegenüber unbefugten Dritten, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, überwiegend zu.

Die weiter begehrte Unterlassung ist unbegründet.

1.
Die DSGVO sieht als solche keinen gesonderten Anspruch auf weitergehende Unterlassung vor. Teilweise wird der Unterlassungsanspruch daher aus Art. 17 Abs. 1 lit. d DSGVO (BGH, Urteil vom 13.12.2022 - VI ZR 60/21), teilweise aus § 823 Abs. 2 BGB, § 1004 BGB analog (OLG München, Urteil vom 19.01.2021 — 18 U 7243/19) hergeleitet. Eine Entscheidung kann hier dahinstehen, da zumindest Einigkeit über das Bestehen eines weitergehenden Unterlassungsanspruchs – unabhängig von der Anspruchsgrundlage – herrscht (vgl. dazu OLG Frankfurt a. M., Urt. v. 14.4.2022 – 3 U 21/20).

Die vom Kläger begehrten Unterlassungsansprüche sind auch nicht nach Art. 79 Abs. 1 DSGVO gesperrt. Die Norm soll lediglich die gerichtliche Durchsetzung eines bestehenden materiell-rechtlichen Anspruchs sicherstellen, verhält sich aber nicht dazu, ob und unter welchen Voraussetzungen ein solcher materieller-rechtlicher Anspruch entstehen kann.

2.

Der mit dem klägerischen Antrag zu 3 a) begehrte Anspruch auf Unterlassung ist im tenorierten Umfang begründet.

Der Kläger kann von der Beklagten die Unterlassung verlangen, seine personenbezogenen Daten (Telefonnummer, Facebook-ID, Familienname, Vorname, Geschlecht, Stadt, Beziehungsstatus) ohne hinreichende Sicherheitsmaßnahmen über das CIT zugänglich zu machen.

a.

Die Beklagte hat in vielfacher Hinsicht gegen die ihr obliegenden Pflichten aus der DSGVO verstoßen (s.o.). Dies insbesondere dadurch, dass sie kein ausreichendes Sicherheitsniveau vorgehalten hat, um die personenbezogenen Daten des Klägers vor einem unbefugten Zugriff durch Scraping zu schützen.

In diesem Zugänglichmachen der klägerischen personenbezogenen Daten ist eine Verarbeitung im Sinne des Art 4 Nr. 2 DSGVO zu sehen, für die vorliegend keine Rechtsgrundlage bestand (s.o.).

Dahingehend besteht auch keine Duldungspflicht des Klägers. Zwar hat dieser die später abgegriffenen Daten freiwillig bei seiner Registrierung auf der Facebook-Plattform angeben. Darin ist jedoch keine Einwilligung in das Zugänglichmachen ebendieser Daten gegenüber unbefugten Dritten zu sehen (s.o.).

b.

Eine dahingehende Wiederholungsgefahr wird aufgrund der bisherigen Datenschutzverstöße der Beklagten widerleglich vermutet (vgl. BeckOGK/*Spohnheimer,* BGB Stand: 01.11.2022, § 1004 Rn. 269). Diese Vermutung konnte die Beklagte nicht widerlegen. Vielmehr legt der Umstand, dass die Beklagte trotz Kenntnis der Anfälligkeit des CIT für Scraping-Angriffe nicht sofort die notwendigen Sicherheitsmaßnahmen ergriffen und darüber hinaus nicht zeitnah nach dem Vorfall darüber informiert hat, eine Wiederholung von Datenschutzverstößen durch die Verwendung des CIT nahe. Die Wiederholungsgefahr wird auch nicht durch die von der Beklagten vorgetragenen Sicherheitsfeatures, insbesondere den „Social Connection Check“ ausgeräumt.

c.

Der Unterlassungsanspruch ist hinsichtlich der Kategorien „Bundesland“ und „Land“ unbegründet. Die Beklagte hat wiederholt bekräftigt, dass diese Kategorien für die Darstellung auf einem Facebook-Profil nicht vorhanden sind, so zuletzt in der mündlichen Verhandlung vom 23.01.2023. Eine solche Angabe ist auch nicht aus dem Screenshot des (öffentlich) einsehbaren Facebook-Profils des Klägers (Anlage B15) ersichtlich.

Diesem Vortrag ist der Kläger weiter nicht in qualifizierter Weise entgegengetreten.

d.
Die Ordnungsmittelandrohung ergibt sich aus § 890 ZPO.

3.
Der mit dem Antrag zu 3 b) geltend gemachte Unterlassungsanspruch besteht nicht.

Zwar hat die Beklagte gegen Art. 13, 14 DSGVO verstoßen, indem sie nicht hinreichend über die Verarbeitung und Benutzung der vom Kläger angegebenen Mobilfunknummer im Zusammenhang mit dem CIT aufgeklärt hat.

Dieser Pflichtverstoß kann jedoch in der Zukunft für den Kläger keine nachteiligen Folgen verursachen. Der Kläger erlangte im Wege seiner Prozessführung alle notwendigen Informationen über die Art und Weise der fraglichen Datenverarbeitung (so auch LG Paderborn, Urteil vom 19.12.2022 – 3 O 99/22; LG Ulm, Urteil vom 16.02.2023 – 4 86/22).
Den Wissensstand von dem der Kläger die weitere Verarbeitung seiner Telefonnummer im Zusammenhang mit dem CIT abhängig macht, erlangte er bereits. Zudem ist es ihm zumindest nach den Ausführungen der Klageerwiderung möglich, seine „Suchbarkeits-Einstellung“ entsprechend seines begehrten Datenschutzniveaus anzupassen.

IV.

Der klägerische Antrag zu 4) ist unbegründet.

Einen grundsätzlich bestehenden Anspruch nach Art. 15 DSGVO des Klägers gegen die Beklagte hat diese mit Schreiben vom 28.10.2021 (Anlage B 16) nach Ansicht der Kammer nach § 362 BGB erfüllt.

Mit ebendiesem Schreiben hat die Beklagte gegenüber dem Kläger kenntlich gemacht, dass

sie davon ausgeht, dass diese Antwort abschließend ist (s.o.). Einen weiteren, über die erteilte Antwort hinausgehenden, Auskunftsanspruch steht dem Kläger nicht zu.

V.

Der Ersatz vorgerichtlicher Rechtsanwaltskosten ist von Art. 82 Abs. 1 DSGVO umfasst.

Zur effektiven Durchsetzung der klägerischen Ansprüche war aufgrund der Schwierigkeit der Sach- und Rechtslage die Hinzuziehung eines Rechtsbeistandes erforderlich und notwendig.

Ausgehend von den zu berücksichtigenden Gegenstandswerten der berechtigen klägerischen Anträge ist vorliegend ein Wert bis 4.000,00 EUR anzunehmen. Dabei war auch der zu diesem Zeitpunkt berechtigte, da noch nicht erfüllte, Auskunftsanspruch einzustellen.

Damit ergeben sich Gebühren von 453,87 EUR (1,3-fache Geschäftsgebühr zuzüglich der Pauschale nach Nr. 7002 VV RVG und 19% MwSt).

Der Zinsanspruch rechtfertigt sich aus §§ 288, 291 BGB, § 187 Abs. 1 BGB, wobei auch hier auf das Datum der Verteidigungsanzeige vom 30.05.2022 abzustellen war.

C.

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

Die Streitwertentscheidung beruht auf § 48 GKG i.V.m. §§ 3, 4, 5 ZPO. Dabei wurde der Antrag zu 1) mit 1.000,00 EUR, der Antrag zu 2) mit 500,00 EUR, der Antrag zu 3) mit 5.000,00 EUR (je 2.500,00 EUR) und der Antrag zu 4) mit 500,00 EUR bemessen.

Vizepräsident des Landgerichts	Richterin am Landgericht	Richter