Landgericht Zwickau

Zivilgericht

Aktenzeichen: **7 O 334/22**

IM NAMEN DES VOLKES

VERSÄUMNISURTEIL

In dem Rechtsstreit

- Kläger -

gegen

Meta Platforms Ireland Ltd. Facebook Ireland Limited, 4 Grand Canal Square, Dublin 2, Irland

vertreten durch den Geschäftsführer Gareth Lambe

- Beklagte -

wegen Persönlichkeitsrechtsverletzung

hat die 7. Zivilkammer des Landgerichts Zwickau durch

Richter am Landgericht Schulte als Einzelrichter

ohne mündliche Verhandlung gemäß § 331 Absatz 3 ZPO am 14.09.2022

für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von 1.000,00 EUR nebst Zinsen seit 22.07.2022 (Rechtshängigkeit) in Höhe von 5 Prozentpunkten über dem Basiszinssatz zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen Schäden zu ersetzen, die dem Kläger 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 des Klägers, 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 des Klägers 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 dem Kläger Auskunft über den Kläger 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 den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 354,62 € zu zahlen zuzüglich Zinsen seit 22.07.2022 (Rechtshängigkeit) in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

6. Die Beklagte hat die Kosten des Rechtsstreits zu tragen.

7. Das Urteil ist vorläufig vollstreckbar.

Beschluss:

Der Streitwert wird auf 11.000,00 EUR festgesetzt.

Gründe

Die Parteien streiten über Ansprüche auf Schadensersatz, Unterlassung, Auskunft und Rechtsverfolgungserstattung begründet durch Verletzungen seitens der Beklagten von Persönlichkeitsrechten und den Grundrechten sowie Grundfreiheiten der Klägerseite, insbesondere deren Recht auf Schutz personenbezogener Daten.

Die Verstöße der Beklagten gegen die DSGVO bestehen zusammenfassend darin, dass die Beklagte als Verantwortlicher, Art. 4 Nr. 7 DSGVO, im Jahr 2019 die Klägerseite betreffende personenbezogene Daten, Art. 4 Nr. 1 DSGVO,

– zum einen ohne Rechtsgrundlage, Artt. 6, 7 DSGVO, und ausreichender Informationen im Sinne von Art. 13, 14 DSGVO verarbeitet, Art. 4 Nr. 2 DSGVO,

– sowie diese Daten unbefugten Dritten zugänglich machte und hierbei die Pflichten aus Artt. 5 Abs. lit. a, lit. b, lit. c, lit. f (Grundsätze für die Verarbeitung personenbezogener Date), 25 Abs. 1, Abs. 2 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), 32 (Sicherheit der Verarbeitung), 34 Abs. 1, Abs. 2 (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person) DSGVO

– sowie Betroffenenrechte der Klägerseite gemäß Artt. 15, 17, 18 DSGVO verletzt.

A.

I.

Die Klägerseite nutzt die von der Beklagten betriebenen Social Media Plattform facebook.com, insbesondere um mit Freunden zu kommunizieren, zum Teilen privater Fotos und für Diskussionen mit anderen Nutzern.

Die Beklagte ist die Betreiberin der Webseite www.facebook.com und der Dienste auf dieser Seite (nachfolgend: Facebook). Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Auf diesen persönlichen Profilen können die Nutzer Angaben zu verschiedenen Daten zu ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können.

II.

Anfang April 2021 sind Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern im Internet öffentlich verbreitet worden. Bei den Datensätzen handelt es sich um Telefonnummer, FacebookID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus und weiterekorrelierende Daten

Bei diesem Vorfall wurden bei der Beklagten personenbezogene Daten aus dem Datenbestand von Facebook mittels des Facebook-Tools KontaktImporter (CIT, Contact-Import-Tool) „gescrapt", also aus zum Teil öffentlich zugänglichen Daten bei Facebook ausgelesen und persistiert. Diese Datensätze wurden ab April 2021 durch unbekannte Dritte im Internet verbreitet und für Interessenten bereitgestellt.

Die Telefonnummern der Benutzer konnten wegen einer Sicherheitslücke mit den restlichen Personendaten korreliert werden und waren somit Bestandteil des jeweiligen unbefugt verbreiteten Datensatzes.

Die genaue Herangehensweise mit allen Parametern ist nicht bekannt, jedoch wird seitens der Beklagten davon ausgegangen, dass das Contact-Import-Tool zur Bestimmung der Telefonnummern der einzelnen Benutzer genutzt wurde. Indem eine Vielzahl von Kontakten in ein virtuelles Adressbuch eingegeben wurde, gelang es Unbekannten, die Telefonnummern konkreten Facebookprofilen zuzuordnen, ohne dass in den entsprechenden Profilen die hinterlegten Telefonnummern öffentlich freigegeben waren. Um die Telefonnummer jeweils zu korrelieren, wurde mit Hilfe des Contact-ImportTools jede fiktive Nummer geprüft und der zugehörige Facebook-Nutzer wurde angezeigt. Auf seinem Profi wurde dieser dann besucht und von dort wurden die öffentlichen Daten gescrapt („abgeschöpft"). So wurden vermutlich alleine für die Rufnummer eines deutschen Mobilfunkanbieters, ca. 10.000.000 Anfragen gestellt.

Vereinfacht dargestellt: Ein Programm testet unzählige Kombinationen von Telefonnummern, um festzustellen, ob diese mit einem Facebook-Nutzer übereinstimmen bzw. ob diese bei Facebook hinterlegt worden ist. Ist dies der Fall, ist es dem Programm möglich, sämtliche Da-

ten des Nutzers abzufragen und zu exportieren.

III.

Möglich war dies einerseits deshalb, weil die Beklagte keinerlei Sicherheitsmaßnahmen vorhielt, um ein Ausnutzen des bereitgestellten Tools zu verhindern, und andererseits, weil die Einstellungen zur Sicherheit der Telefonnummer auf Facebook so undurchsichtig und kompliziert gestaltet sind, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen kann. Daraus resultierend wurden unter anderem auch die Klägerseite betreffende personenbezogene Daten im Internet auf Seiten veröffentlicht, die illegale Aktivitäten begünstigen sollen, z.B. auf der Seite raidforums.com. Bei der vorbenannten Website handelt es sich um ein bekanntes “HackerForum”, das unter anderem dafür verrufen ist, dass dort illegal abgeschöpfte Daten – wie vorliegend – hinterlegt und ausgetauscht werden, um diese unter anderem für kriminelle Machenschaften, wie Internetbetrug zu nutzen. Aufgrund dessen wurde der Zugang unter anderem durch die indonesische Regierung der dortigen Bevölkerung untersagt bzw. der Zugang blockiert.

Die Daten wie Name und Rufnummer können und werden insbesondere für gezielte Phishing Attacken genutzt. Die so verbreiteten Datensätze beinhalten in katalogisierter Form die Telefonnummer, FacebookID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt sowie korrelierende Daten.

Die Tragweite und das Gewicht dieses Vorfalls lassen sich besonders veranschaulichen, indem man den Prozess und die Einstellungen zur Datensicherheit für Nutzer/innen von Facebook als solches in den Blick nimmt. Dieser Prozess ist insgesamt geprägt von datenschutz-unfreundlichen Einstellungen, einer Masse an schwer verständlichen Informationen und unklarer Angaben.

Dies beginnt bei der Erstellung eines Facebook-Accounts. Dies funktioniert so, dass der angehende Nutzer die ihn betreffenden personenbezogenen Daten, Vor- und Zuname, Handynummer oder E-Mailadresse, Geschlecht und Geburtsdatum in die Registrierungsmaske einträgt. An diesem Punkt wird der Nutzer mit einer Informationsflut hinsichtlich der Nutzungsbedingungen, der Verwendung von Cookies und Datenschutzrichtlinien konfrontiert, die er über eine kleine Verlinkung im unteren Teil der Anmeldemaske erreichen kann.

Bereits hier ist unklar, weshalb zwischen Datenschutzrichtlinien und Cookie Verwendung differenziert wird, obwohl die Verwendung von Cookies ein inhärent datenschutzrechtliches Thema ist.

Nachdem die Registrierung abgeschlossen ist, wird der Benutzer auf die Startseite geführt.

Auch unmittelbar nach der Anmeldung sehen sich Nutzer mit einer Fülle an Einstellungen und weiteren Untereinstellungen konfrontiert, die über verschiedene Links zu erreichen sind.

Aufgrund der Vielzahl an Einstellungsmöglichkeiten ist mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehält und nicht selbstständig ändert.

Aus diesem Grund kommt den Voreinstellungen besondere Bedeutung zu. Nach den Grundsätzen eines nutzerfreundlichen Datenschutzes und dem in der DSGVO niedergelegten Prinzips der Datenminimierung und des „privacy by default“ (=datenschutzfreundliche Voreinstellungen) sind hier besonders datenschützende Voreinstellungen geboten. Nur so können Nutzer mündig und bewusst entscheiden, welche Daten sie für wen freigeben möchten und erlangen Kontrolle über ihre Daten.

Die Voreinstellungen der Beklagten liefern ein starkes Gegenbeispiel zu dieser gesetzlichen Vorgabe:

Unmittelbar nach der Anmeldung können bspw. bereits „alle“ Personen sehen, welche Seiten der Nutzer abonniert oder mit wem er befreundet ist. Ebenso können „alle“ den neuen Nutzer über seine E-Mail-Adresse oder seine Telefonnummer „finden“, was für das hier in Rede stehende Ereignis gesteigerte Bedeutung hat. Die Informationen sind also standardmäßig „öffentlich“ verfügbar. Schon an dieser Stelle bleibt unklar, was genau mit „finden“ gemeint ist und was dies für die Verarbeitung der Daten bedeutet.

Ebenso wird für alle Informationen, die ein Nutzer in sein Profil einträgt, standardmäßig „öffentlich“ als Voreinstellung ausgewählt.

Von gesteigerter Wichtigkeit und im Kontext einer sicheren OnlineUmgebung besonders relevant für einen Nutzer ist die Sicherheit und Vertraulichkeit seiner Telefonnummer. Das zeigt sich nicht zuletzt darin, dass trotz der aufgezeigten Undurchsichtigkeit im Datenmanagement selbst bei Facebook die Telefonnummer der Nutzer gesondert behandelt wird. So wird betont, dass standardmäßig nur der Nutzer die Telefonnummer einsehen kann.

Es ist klar ersichtlich, dass ein Nutzer, der seine Telefonnummer bei Facebook lediglich zu Sicherheitszwecken verwenden möchte, auch gesteigerten Wert auf die Vertraulichkeit seiner Telefonnummer legt. Wer so weit geht, die Telefonnummer zur zusätzlichen Sicherheit seines

Accounts einzusetzen, legt offensichtlich Wert auf die Sicherheit seines Accounts und seiner Daten. Folglich kann die Versicherung Facebooks „Nur Du kannst deine Nummer sehen“ nur so verstanden werden, dass der Einsatz der Telefonnummer zu Sicherheitszwecken die Datensicherheit nicht weiter kompromittiert und durch die Angabe der Nummer Dritte keine weiteren Informationen erlangen können.

Auch die Informationen, an die man mit dem Klicken auf „Mehr dazu“ gelangt, führen nicht dazu, dass sich an diesem Umstand etwas ändert. Dort wird lediglich näher beschrieben, wie der Sicherungsprozess mit Hilfe der „ZweiFaktor-Authentifizierung“ funktioniert. Auch ist schon die Überschrift „Möglicherweise verwenden wir deine Mobilnummer für diese Zwecke“ im besten Fall uneindeutig und im schlimmsten Fall irreführend. Mit keinem Wort wird erwähnt, dass die angegebene Nummer dazu verwendet werden kann, in irgendeiner Art das Profil des Nutzers zu identifizieren.

Nutzer wie der Kläger gaben also im Vertrauen und mit dem Ziel, mehr persönliche Sicherheit zu erreichen, ihre Telefonnummern auf Facebook preis. Entgegen ihrer Erwartungen wurden diese Nummern aber ohne den Einsatz von weiteren Sicherheitsmaßnahmen durch die Beklagte in großem Umfang Unbekannten zugänglich gemacht. Die Unbekannten gingen dabei wie folgt vor:

Facebook bietet, damals wie heute, die Funktion an, die im Smartphone eines Nutzers gespeicherten Personenkontakte mit Nutzern auf Facebook zu synchronisieren. Wenn also ein Suchender in seinem Smartphone eine Telefonnummer als Kontakt eingespeichert hat, erlaubt es die Beklagte ihm, seine Kontakte mit den bei Facebook hinterlegten Telefonnummern abzugleichen, um die hinter den Nummern stehenden Personen als Freunde hinzuzufügen.

Bemerkenswert ist hierbei, dass es mit dieser Funktion möglich ist, FacebookProfile zu identifizieren, ohne dass die im Profil hinterlegte Nummer für die Öffentlichkeit freigegeben war. Mit anderen Worten konnte eine Telefonnummer einem Profil zugeordnet werden, ohne dass im Profil des Nutzers die Telefonnummer der Öffentlichkeit preisgegeben werden sollte. Obwohl also ein Nutzer seine Telefonnummer geheim halten wollte, ermöglichte es die Beklagte den Unbekannten, die Nummern der Nutzer zu identifizieren. Um dies zu verhindern, hätte der Nutzer an anderer Stelle in einer zweiten Option zur Einstellung, wer den Nutzer „finden“ kann, auswählen müssen, dass er nicht von der Öffentlichkeit anhand seiner Telefonnummer gefunden werden möchte. Diese Zweite Option war aber nicht zu erreichen, wenn man lediglich

nach den Einstellungsmöglichkeiten für die Telefonnummer gesucht hat. Zusätzlich war diese versteckte Option standardmäßig auf „öffentlich“ gestellt.

Durch die vielschichtigen Einstellungsmöglichkeiten wurde also ein Gefühl der Sicherheit für den Nutzer – auch für die Klägerseite – erzeugt, was im Ergebnis zu einer erheblichen Datengefährdung führte und sich diese Gefährdung auch verwirklichte.

Auf die Spitze getrieben wurde – und wird – das Ganze noch dadurch, dass neben den gewöhnlichen Funktionen der Facebook-Website auch noch eine separate, ebenfalls von der Beklagten betriebene, Messenger-App existiert. Diese App dient als Schnittstelle für die Facebook-Applikation auf Mobilgeräten und bietet eine Messenger-Funktion für Nutzer an. Nutzer melden sich dafür mit ihren bestehenden Facebook-Profilen an. Die Messenger-App und die gewöhnlichen Funktionen von Facebook sind also verknüpft über den Zugang zum selben Account. Allerdings können auch in dieser App separate Sicherheitseinstellungen vorgenommen werden. Diese Einstellungen werden unabhängig von den Einstellungen des Accounts im sonstigen Facebook-Dienst vorgenommen. Insbesondere kann hier wiederum separat eingestellt werden, ob Telefonkontakte mit dem Facebook-Dienst synchronisiert werden sollen. Dies geht sogar so weit, dass bereits bei Anmeldung in der Messenger-App angefragt wird, ob diese Synchronisierung vorgenommen werden soll. Eine Information über etwaige Risiken oder über die Verwendung der Telefonnummer erfolgt dabei nicht, obwohl ein Nutzer geradezu zur Verwendung des Kontakt-Import-Tools gedrängt wird, indem unmittelbar nach dem ersten Öffnen der App ein entsprechender Bildschirm angezeigt wird.

Insgesamt bestehen also mindestens 3 unterschiedliche Einstellungsmöglichkeiten hinsichtlich der Verwendung der Telefonnummer, die teilweise in verschiedenen Apps angewendet und teilweise räumlich getrennt dargestellt wurde. Für effektive digitale Sicherheit musste ein Nutzer aber zunächst einen Überblick über alle möglichen Einstellungen erhalten und dann von den von Facebook aufgedrängten Einstellungen abweichen, um tatsächlich die Verwendung seiner Telefonnummer zu verhindern.

Dem Nutzer – wie der Klägerseite – wurde also durch oberflächlich sichere Einstellungen ein Gefühl der Sicherheit vermittelt, während für tatsächlich wirksamen Schutz viele Einstellungen gleichzeitig hätten geändert werden müssen, ohne ausreichende Informationen hierzu oder Voreinstellungen seitens der Beklagten gewährleistet werden.

Zusammenfassend:

Diese offensichtliche Sicherheitslücke mangels bestehender Sicherheitsmechanismen nutzen

Unbekannte im Jahr 2019 gezielt aus. Indem Millionen von Telefonnummern generiert und über die von Facebook zur Verfügung gestellte Software synchronisiert wurden, konnten die Unbekannten die von ihnen wahllos erstellten Telefonnummern den Profilen von Facebooknutzern zuordnen. Auf diesem Weg wurden insgesamt ca 533 Millionen Telefonnummern von Nutzern sowie die weiter benannten personenbezogenen Daten abgegriffen und von Unbekannten im Internet veröffentlicht – wie auch die von der Klägerseite.

Dabei nimmt die Beklagte keinerlei Sicherheitsvorkehrungen gegen die Ausnutzung dieses Programms und Vorgehens vor:

Es wurden keine Sicherheitscapchas verwendet, um sicherzustellen, dass es sich bei der Anfrage zur Synchronisierung um die Anfrage eines Menschen und nicht um eine automatisch generierte handelt.

Ebenso wenig wurde ein Mechanismus zur Überprüfung der Plausibilität der Anfragen bereitgehalten, etwa indem ungewöhnlich viele Anfragen derselben IP-Adresse auf einmal geblockt werden oder Adressbücher mit auffälligen Telefonnummerabfolgen (z.B. 000001, 000002 usw.) automatisch abgelehnt werden. Dadurch war es denkbar einfach, das System für kriminelle Zwecke zu missbrauchen.

Dies wiegt umso schwerer vor dem Hintergrund, dass das Abgreifen von Daten durch automatisierte Verfahren zu dubiosen Zwecken (s.g. „Scraping“) eine bekannte und weit verbreitete Methode zur Informationsgewinnung ist.

Die Veröffentlichung der Daten hat weitreichende Folgen für die Klägerseite.

Die Zuordnung von Telefonnummern zu weiteren Daten wie Mail-Adresse oder Anschrift eröffnet böswilligen Akteuren eine weite Bandbreite an Möglichkeiten wie bspw. Identitätsdiebstahl, die Übernahme von Accounts oder gezielte Phishing-Nachrichten. Insbesondere sogenannte „Sim-Swap“Angriffe werden durch die Verknüpfung von Telefonnummern zu weiteren Nutzer-Accounts eröffnet. Durch derartige Angriffe ist es Kriminellen möglich, Passwörter zu ändern, die durch telefonnummernbasierende Authentifizierung geschützt sind.

Abgegriffen und veröffentlicht wurden unter anderem die Namen, die Facebook-IDs, die Wohnorte, die Geburtsdaten und Geburtsorte und die Mobilfunknummer der 500 Millionen Facebook-Nutzer/innen.

Unter den betroffenen Personen befand sich auch der Kläger. Auch von ihm wurden Daten

wie Telefonnummer, Name, Wohnort und Mailadresse abgegriffen. Ob noch mehr Daten entwendet wurden, lässt sich mangels ausreichender Auskunft durch die Beklagte Auskunftsanspruch) noch nicht angeben.

Die Klägerseite erlitt deswegen einen erheblichen Kontrollverlust über ihre Daten und verblieb in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch ihrer sie betreffender Daten. Dies manifestierte sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen.

Darüber hinaus erhält die Klägerseite seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese enthaltenen oder Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks. Oft werden auch bekannte Plattformen oder Zahlungsdienstleister wie Amazon oder Paypal impersoniert und durch Angabe der entwendeten Daten versucht, ein gesteigertes Vertrauen zu erwecken. Das hat dazu geführt, dass die Klägerseite nur noch mit äußerster Vorsicht auf jegliche Emails und Nachrichten reagieren kann und jedes Mal einen Betrug fürchtet und Unsicherheit verspürt.

IV.

Aber nicht nur die fehlenden Informationen und der sorglose Umgang sowie die mangelhafte Sicherheit der Daten ist der Beklagten vorzuwerfen. Auch der Umgang mit der Situation, nachdem die Ausnutzung dieser Sicherheitslücke bekannt wurde, ist nicht ordnungsgemäß verlaufen.

Der Vorfall ereignete sich bereits im Jahr 2019. Die Beklagte informierte die Klägerseite jedoch zu keinem Zeitpunkt darüber, dass ihre Informationen durch Dritte entwendet und veröffentlicht wurden. Weder eine persönliche Benachrichtigung noch eine allgemein öffentliche Bekanntmachung über den Datenklau fand statt.

Die Beklagte unterließ es auch, die zuständige Datenschutzbehörde, Irish Data Protection Commission, über den Vorfall zu informieren.

V.

Mit vorgerichtlichem Schreiben der Klägerseite wurde die Beklagte unter Darlegung der Sach- und Rechtslage zur Zahlung von lediglich 500,- Euro Schadensersatz nach Art. 82 Abs. 1 DS-GVO im Sinne einer schnellen und einfachen vorgerichtlichen Erledigung, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft darüber aufgefordert, welche konkreten Daten im April 2019 abgegriffen und veröffentlicht wurden.

Die Beklagte hat in Ihren gleichlautenden Schreiben sowohl den Schadensersatz in Höhe von 500,00 Euro, als auch den Unterlassungsanspruch zurückgewiesen.

In diesem Schreiben teilte die Beklagte mit, dass sich unter den abgegriffenen und veröffentlichten Daten auch Daten der Klägerseite befanden.

Dieses Auskunftsschreiben ist allerdings als Antwortschreiben der Beklagten insgesamt unzureichend. Das enthielt lediglich allgemein gehaltene Informationen zu den auf Facebook verarbeiteten Daten sowie einen Link zur Seite der Beklagten, auf der die Daten über einen individuellen Nutzer gespeicherten Daten eingesehen werden können. Dieses Vorgehen allein ist schon nicht geeignet, dem nach Art. 15 DSGVO umfassenden Auskunftsanspruch gerecht zu werden.

Unabhängig davon enthielt das „Auskunftsschreiben" der Beklagten aber auch keinerlei konkrete Aussagen dazu, welche Daten der Klägerseite im Wege des Scrapings von unbekannten Dritten abgegriffen wurden. So bleibt etwa offen, wann genau die Daten entwendet wurden oder wie viele verschiedene Beteiligte diese Funktion hinsichtlich der Daten der Klägerseite ausgenutzt haben.

Hinsichtlich des weiteren Vorbringens des Klägers wird auf die Ausführungen in der Klageschrift vom 6.05.2022 verwiesen

B.

I.

Die Klage ist zulässig. Insbesondere ist das Landgericht für die Sache zuständig.

Die sachliche Zuständigkeit richtet sich nach § 71 GVG iVm. § 23 Nr. 1 GVG. Danach sind die Landgerichte für alle Streitigkeiten zuständig, für die nicht bereits die Amtsgerichte zuständig sind. Die Amtsgerichte sind für Ansprüche, deren Gegenstand an Geld oder Geldeswert die Summer von 5.000,00 Euro nicht übersteigt, zuständig.

Der hier zugrunde gelegte Streitwert beträgt 11.000,00 Euro. Dieser setzt sich zusammen aus dem Schadensersatzanspruch über 1.000,00 Euro und dem Unterlassungsanspruch. Der Unterlassungsanspruch ist mit 10.000 Euro anzusetzen. Der Streitwert bei nicht vermögensrechtlichen Streitigkeiten ist anhand aller Umstände des Einzelfalls, insbesondere auch anhand der Einkommensverhältnisse und der Bedeutung der Sache, zu bemessen. Bei der Be-

klagten handelt es sich um einen multinationalen Konzern mit hohen Einkommen, die Bedeutung der Sache ist auf Grund der schwerwiegenden Folgen für die Klägerseite gravierend, sodass ein Streitwert von 10.000 Euro angemessen ist. (ähnlich LG Frankfurt, Beschluss vom 15. 10. 2020 2-03 O 356/20; LG Dresden, Beschluss vom 23.01.2013, 4 W 1363/12).

Die örtliche Zuständigkeit richtet sich nach Art. 18 Abs. 1 2. Alt EuGVVO. Danach 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.

Das angerufene Gericht ist zudem nach Art. 79 Abs. 2 S. 2 DSGVO, § 44 Abs. 1 S. 2 BDSG örtlich zuständig (besonderer Gerichtsstand). Die Klägerseite (betroffene Person) hat ihren gewöhnlichen Aufenthaltsort, Wohnsitz im Bezirk des angerufenen Gerichts.

II.

Die Klage ist auch schlüssig begründet.

Die Beklagte war nach Durchführung des schriftlichen Vorverfahrens und fruchtlosem Ablauf der gesetzten Notfrist antragsgemäß entsprechend der in der Klageschrift vom 6.05.2022 formulierten Anträge zu verurteilen.

Der Kläger hat gemäß Art. 82 Abs. 1 DSGVO gegen die Beklagte einen Anspruch auf Schadensersatz in Höhe von 1.000,00 Euro nebst Zinsen gemäß §§ 288 Abs.1, 291 BGB und Rechtsanwaltskosten. Die geltend gemachten Ansprüche auf Unterlassung folgen aus §§ 1004 Abs. 1 S. 2, 823 Abs. 1 BGB, §§ 1004 Abs. 1 S. 2, 823 Abs.2 BGB in Verbindung mit DSGVO bzw. aus Art. 17 DSGVO, auf Auskunft aus Art. 15 DSGVO.

1. Schadensersatz

Nach Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schadenentstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

a) Verletzung

Das Verhalten der Beklagten begründet mehrere Verstöße gegen die DSGVO.

aa) Zunächst hat die Beklagte die Klägerseite nicht im ausreichenden Maße über die Verarbeitung sie betreffender personenbezogener Daten, die sie dort angegeben hat, informiert bzw. aufgeklärt. Insbesondere die skizzierte Art der Belehrung über die Verwendung und Geheimhaltung der Telefonnummer stellt einen Verstoß gegen die DSGVO dar.

Die in Art. 5 Abs. 1 lit. a) DSGVO verankerten Grundsätze von Treu und Glauben und der Transparenz fordern eine Verarbeitung in einer für die betroffene Person nachvollziehbaren Weise. In diesem Sinne lassen sich die Transparenzvorschriften der DSGVO direkt aus dem Gebot von Treu und Glauben gem. Art. 8 Abs. 2 S. 1 GRCh (Charta der Grundrechte der Europäischen Union) ableiten.

Artt. 13 und 14 DSGVO sehen Informationspflichten vor, die allgemein auf die Verarbeitung von personenbezogenen Daten der Betroffenen abstellen. Beide Normen begründen eine aktive Pflicht für den Verantwortlichen, die erforderliche Transparenz (in aktiver Art und Weise) herzustellen. Nach dem Erwägungsgrund 60, im Folgenden ErwGr, machen es die Grundsätze einer fairen und transparenten Verarbeitung erforderlich, dass die betroffene Person von dem Verantwortlichen über die Existenz desVerarbeitungsvorgangs und seine damit verfolgten Zwecke unterrichtet wird. Der Verantwortliche ist gehalten, der betroffenen Person alle weiteren Informationen zur Verfügung zu stellen, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung sowie Information des Betroffenen zu gewährleisten.

Diese Informationspflicht ist als Ausdruck einer fairen und transparenten Verarbeitung von personenbezogenen Daten zu verstehen. Eine faire und transparente Verarbeitung bedingt eine Unterrichtung der betroffenen Person nicht nur über die Existenz des Verarbeitungsvorganges, den Verantwortlichen und die Zwecke der Verarbeitung (vgl. ErwGr 60) an sich, sondern darüber hinausgehend insbesondere auch über weitere, mit der Datenverarbeitung zusammenhängende Absichten und Rechtsfolgen. Die Informationspflicht bzw. die mitgeteilten Informationen fördern damit (auch) eine effektive Rechtsdurchsetzung, insbesondere in Bezug auf die Betroffenenrechte aus dem dritten Abschnitt der DSGVO (vgl. Art. 15 ff.).

Dieser Informations- und Aufklärungspflicht, die sich unmittelbar aus der DSGVO ergibt und darin auch klar gefordert wird, wird die Beklagte in keiner Weise gerecht. Die Klägerseite hatte so nicht die Möglichkeit in informierter Art und Weise über die Preisgabe ihrer personenbezogenen Daten zu entscheiden.

Bei den abgegriffenen und veröffentlichten Daten handelt es sich um personenbezogene im Sinne Art. 4 Nr. 1 DSGVO. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Mit Hilfe der betroffenen abgegriffenen und veröffentlichten Daten kann die Klägerseite eindeutig identifiziert werden.

Meldet sich ein Nutzer mit seinem Account auf der Social-Media-Plattform der Beklagten an, besteht für diesen die Möglichkeit, unter "Einstellungen" seine Telefon- bzw. Mobilfunknummer anzugeben.

Einen Hinweis, wie und wofür diese genutzt wird gibt es nicht. Es wird also nicht offengelegt, für welchen Zweck, in welcher Form und in welchem konkreten Umfang sie die Telefon- bzw. Mobilfunknummer ihrer Nutzer konkret nutzen wollen und werden. Auch der weitere Textverlauf lässt eine eindeutige und konkrete Beschreibung der von ihnen beabsichtigten Nutzung der Mobilfunknummer vermissen. Insbesondere wird nicht eindeutig über die Tragweite der jeweiligen Privatsphäreeinstellungen informiert. Ein Hinweis darauf, dass auch als privat eingestellte Nummern durch externe Programme abgeglichen werden können, erfolgt nicht. Ebenso wenig wird eindeutig darüber informiert, dass das öffentliche Teilen der Telefonnummer die Möglichkeit eröffnet, dass durch automatische Software eine Kategorisierung und Abgreifung durch böswillige Dritte erfolgen kann.

Unabhängig davon besteht für den Nutzer die Möglichkeit, seinen Account durch eine sogenannte „Zwei-Faktor-Authentifizierung“ mittels Übermittlung der eigenen Mobilfunknummer an die Beklagte zu sichern.

Auch an dieser Stelle wird lediglich unzureichend über den Umfang der Nutzung und vor allem hinsichtlich der zugrundeliegenden konkreten Zwecke, aufgeklärt.

Diese Ausführungen sind nicht ausreichend, um dem Zweck der oben genannten Artikel der DSGVO, nämlich die Entscheidung über die Preisgabe der eigenen personenbezogenen Daten in informierter Weise treffen zu können, gerecht zu werden.

Weder der Umfang einer vom Nutzer zu erteilenden Einwilligung, noch eine ausreichende In-

formation darüber, zu welchen konkreten Zwecken diese Daten von der Beklagten darüber hinaus noch verarbeitet werden, wird in ausreichendem Maße, dem Transparenzgebot genügend, erläutert.

Bereits die Aussage, dass die Daten nur „möglicherweise“ für diese Zwecke verwendet werden ist zu unpräzise. Eine genaue Beschreibung, unter welchen Bedingungen die Nummer verwendet wird, unterbleibt. Auch in den genannten Beispielen bleibt offen, wie genau die Telefonnummer verwendet wird, wer sie einsehen kann und an wen sie weitergeleitet wird. Dem Nutzer wird es nicht ermöglicht, eine Folgenabschätzung vor Übermittlung seiner Mobilfunknummer an die Beklagte dahingehend vorzunehmen, was mit seiner Mobilfunknummer sonst noch außerhalb der Nutzung im Rahmen der sog. „Zwei-Faktoren-Authentifizierung“ geschieht („Verwendung für andere Zwecke“). Dem Nutzer ist lediglich bekannt, dass er seine Mobilfunknummer zum Zwecke der Authentifizierung, nämlich der sog. „Zwei-FaktorenAuthentifizierung“ übermittelt. Dies wiegt an dieser Stelle umso schwerer, da gerade bei der Verwendung der Telefonnummer zur Zwei-Faktor-Authentifizierung bei Nutzern/innen der Wunsch nach mehr Sicherheit im Vordergrund steht und eine folgenreiche Veröffentlichung seiner Daten besonders unerwartet ist.

Darüber hinaus wird nur per Unterverlinkung darüber informiert, dass die Telefonnummer auch dazu verwendet werden kann, dass andere Nutzer das Profil mit der angegebenen Nummer „finden“ können. Diese Option ist zunächst zu schwer aufzufinden. Sie ist nur unter dem Reiter „Deine Privatsphäre → Bestimme, wer dich finden kann“ zu finden, nicht jedoch im Rahmen der Angaben zur Verwendung der Telefonnummer.
Davon unabhängig sind aber auch die dort angegebenen Informationen nicht ausreichend oder klar verständlich. Zwar wird klargestellt, dass „finden“ abhängig von den Einstellungen des Nutzers auch bedeuten kann, dass bei Eingabe der Telefonnummer in die Suchzeile der Website das zugehörige Nutzerprofil angezeigt werden kann. Es wird allerdings nicht eindeutig darauf hingewiesen, dass „finden“ auch bedeutet, dass die automatische Software zum Kontakte importieren unmittelbar auf das jeweilige Profil verweist. Vor allem wird aber nicht darauf hingewiesen, dass dies auch dann möglich ist, wenn die Telefonnummer auf „nicht öffentlich“ bzw. „privat“ gestellt wurde. Eine solche Information wäre aber bei dieser Sachlage zwingend erforderlich, da die Einstellung „privat“ unmissverständlich impliziert, dass nur der Nutzer das Profil anhand der Telefonnummer identifizieren kann, andere Dritte aber keinerlei Zugriff auf oder Bezug zu dieser Nummer haben. Demgemäß konterkariert es geradezu die vorher für die Telefonnummer gewählte strenge Privatsphäreeinstellung, wenn zwar die Telefonnummer nicht im Profil angezeigt wird, aber standardmäßig trotzdem jedermann das Profil anhand der

Telefonnummer identifizieren kann.

Derartige Belehrungen hat die Beklagte nicht beigebracht, sodass nicht ausreichend über die Verwendung der Telefonnummer belehrt wurde.

bb) Weiterhin hat die Beklagte im Jahr 2019 die personenbezogenen Daten ihrer Nutzer, so auch die der Klägerseite, nicht im ausreichenden Maße und nicht den Anforderungen der DS-GVO entsprechend, geschützt.

Der Grundsatz der Integrität und Vertraulichkeit aus Art. 5 Abs. 1 lit. f DSGVO fordert, dass die Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Datenschutzkonformität setzt also, neben der Zulässigkeit der Verarbeitung personenbezogener Daten, welche in Art. 6 der DSGVO grundsätzlich geregelt ist, die Sicherheit der Verarbeitung voraus.

Nach der Definition in Art. 4 Nr. 12 DSGVO ist eine Verletzung des Schutzes personenbezogener Daten bei einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, anzunehmen.

Um die Sicherheit der personenbezogenen Daten im oben genannten Sinne und angemessenes Schutzniveau zu gewährleisten, fordert Art. 32 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 von dem Verantwortlichen und dem Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen.

Art. 32 DSGVO steht in einem engen Zusammenhang zu Art. 24 und 25 der DSGVO, die sich im Kapitel „Allgemeine Pflichten“ des Verantwortlichen finden. Art. 24 DSGVO ist die Generalnorm für den technischen und organisatorischen Datenschutz. Sie verpflichtet den Verantwortlichen generell dazu, durch technische und organisatorische Maßnahmen die Anforderungen der Verordnung umzusetzen. Art. 32 DSGVO stellt im Vergleich dazu eine Konkretisierung dar, als sich aus der Maßnahmenkatalog ergibt, dass der Zusammenschau mit dem

Maßnahmekatalog ergibt, dass er technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit einfordert.

Art. 25 Abs. 1 DSGVO wiederum spezifiziert Art. 24 DSGVO dahingehend, dass er insbesondere auf den Zeitpunkt der Festlegung der Mittel der Verarbeitung abstellt und somit präventiv wirkt. In der Konzeptionsphase können vor allem die Grundsätze der Rechtmäßigkeit, Zweckbindung, Datenminimierung und der Speicherbegrenzung realisiert werden.

Zum anderen bildet Art. 32 DSGVO zusammen mit den Art. 33 und 34 DSGVO den Abschnitt „Sicherheit der Verarbeitung".

Die Daten der Klägerseite waren bei der Beklagten nach dem damaligen Stand der Technik nicht ausreichend geschützt.

Die Beklagte, als Verantwortlicher nach Art. 4 Nr. 7 DSGVO, hatte offensichtlich bis zum April 2019 keine geeigneten technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit ihrer Nutzer implementiert, die einen solchen Datenklau verhindert hätten.

Anders als die Beklagte in ihren vorgerichtlichen Antwortschreiben behauptet, handelt es sich bei den entwendeten Daten nicht lediglich um ohnehin öffentlich einsehbare Daten, zu denen Kriminelle lediglich eine Telefonnummer selbstständig beigesteuert haben. Die Beklagte versucht damit wohl anzudeuten, dass es sich nicht um eine Sicherheitslücke handele, sondern die Daten lediglich im Wege des gewöhnlichen Betriebsablaufs verwendet und nur im Wege der vom Nutzer gewählten Parameter veröffentlicht wurden. Gegen dieses Verständnis spricht zunächst schon der Umstand, dass die Beklagte erst nach Bekanntwerden der Existenz des oben beschriebenen Datenlecks im Jahr 2019, diese Sicherheitslücke geschlossen hat.

Die Beklagte führt dazu in dem von ihr veröffentlichten Artikel

„Informationen zu aktuellen Meldungen bezüglich Facebook-Daten" (abrufbar unter

https://about.fb.com/news/2021/04/facts-on-news-reports-aboutfacebook-data/) selbst aus:

„Sobald wir auf diesen Umstand aufmerksam wurden, haben wir Maßnahmen ergriffen, um zu verhindern, dass böswillige Akteure mithilfe von Software unsere App imitieren, um Zugang zu einer großen Menge von Telefonnummern zu erhalten und diese mit Facebook-Nutzern abzugleichen. "

Weiter führte sie aus:

„Für uns hat es höchste Priorität, die Daten unserer Nutzer zu schützen. Deswegen arbeiten wir mit Nachdruck daran, die ausgelesenen Datensätze offline zu nehmen. Wir gehen außerdem – wo immer dies möglich ist – weiterhin rigoros gegen böswillige Akteure vor, die unsere Dienste missbrauchen. Wir können zwar nicht immer verhindern, dass ausgelesene Daten wie diese erneut in Umlauf geraten oder dass neue Daten an anderer Stelle auftauchen – wir haben jedoch ein eigenständiges Team, das sich dieser wichtigen Arbeit widmet."

Diese „wichtige Arbeit", folglich das Schließen einer so offensichtlichen Sicherheitslücke, hätte jedoch bereits weitaus früher vorgenommen werden müssen. Als Verantwortlicher, welcher dieses soziale Netzwerk entwickelt und programmiert hat, war die Beklagte veranlasst, über Ihr großes Sicherheits- und Programmiererteam bereits vor dem nunmehr bekanntgewordenen und bereits vor dem 2019 durchgeführten „Scraping" diese Schwachstelle zu lokalisieren und diese Möglichkeit des Datenabgriffs bzw. der Datenzusammenführung nach dem Stand der Technik durch die Sicherstellung von wirksamen Sicherheitsmaßnahmen – wie nach dessen Bekanntwerden auch geschehen – zu verhindern und das Level der von der DSGVO geforderten Datensicherheit zu gewährleisten.

Dies unterließ die Beklagte jedoch offensichtlich, da ansonsten der Datenklau, so wie er von statten gegangen ist, nicht hätte stattfinden können. Dabei handelt es sich beim Scraping um eine weit verbreitete Methode fremde Daten in großem Umfang unberechtigt abzugreifen. In dem von der Beklagten veröffentlichen Artikel „Informationen zu aktuellen Meldungen bezüglich Facebook-Daten" schreibt diese selbst, dass das Auslesen von Daten (auch „Scraping" genannt) eine weit verbreitete Methode ist, die sich oft auf automatisierte Software stützt, und mit deren Hilfe öffentlich zugängliche Informationen aus dem Internet extrahiert werden können.

Die Beklagte war sich dieses offenbar weit verbreiteten Phänomens also durchaus auch bewusst.

Technische Maßnahmen, die eine solche Suche begrenzen oder von anderen Kriterien und Voraussetzungen abhängig machen, wurden dennoch nicht getroffen. Insbesondere wurden (und werden weiterhin) keine „Sicherheitscapchas", die garantieren, dass es sich bei der Person, die die Suchanfrage stellt, um einen Menschen und nicht um automatische Software handelt, verwendet.

cc) Unabhängig von etwaigen Sicherheitslücken verstößt die Beklagte mit den von ihr vorgenommenen Einstellungen zur Privatsphäre gegen die in Art. 25 DSGVO niedergelegten Grundsätze der „Privacy by Design" und „Privacy by default".

Danach ist der Verantwortliche im Vorfeld einer jeden Datenverarbeitung verpflichtet, die entsprechenden organisatorischen und technischen Maßnahmen zu treffen, um den Anforderungen der DSGVO gerecht zu werden.

Dies beinhaltet insbesondere die Pflicht nach Art. 25 Abs. 2 DSGVO, datenschutzfreundliche Voreinstellungen bereitzuhalten, die die Verwendung der Daten der Nutzer minimiert.

Darunter fällt auch, die möglichst datenschutzfreundlichste Variante als Standardeinstellung vorzusehen.

Dem ist die Beklagte nicht nachgekommen, indem bei den allermeisten der vom Nutzer angegebener Daten standardmäßig eine öffentliche Verbreitung vorgesehen ist und Nutzer aktiv tätig werden müssen, um die Einstellung auf „privat“ zu ändern. Ebenso wenig datenschützend ist es, dass standardmäßig „jedermann“ ein Profil mit Hilfe der hinterlegten Telefonnummer „finden“ kann: die Möglichkeit, eine Nummer einem Profil zuzuordnen, führt zwangsläufig zu einer reflexartigen Offenlegung der Telefonnummer, wie anschaulich im in Rede stehenden Datenleck gezeigt wurde.

Die Beklagte hat darüber hinaus auch gegen die in Art. 25 Abs. 2 S 2 aE DSGVO normierte Pflicht, die personenbezogenen Daten der Betroffenen nur einer möglichst geringen Zahl von Personen zugänglich zu machen, verstoßen. Aus Art. 25 Abs. 2 S. 2 aE DSGVO ergibt sich die Pflicht des Verantwortlichen, sicherzustellen, dass, unabhängig von den von Nutzern gewählten Einstellungen, nur ein möglichst kleiner Personenkreis Zugriff auf die personenbezogenen Daten der Nutzer hat. Dies beinhaltet auch, sicherzustellen, dass trotz einer öffentlichen Verfügbarkeit der personenbezogenen Daten nur diejenigen Zugriff darauf haben, die die Daten im Wege der gewöhnlichen Funktionen des sozialen Netzwerks nutzen wollen. Dies wird besonders in Art. 25 Abs. 2 S. 3 DSGVO verdeutlicht. Indem die Beklagte keine Maßnahmen gegen das Abfragen der Daten durch automatische Programme, z.B. im Wege des beschriebenen „Scapings“, getroffen hat, hat sie einer unübersichtlich weiten Zahl von Personen Zugang zu den Nutzerdaten gewährt und damit gegen das Prinzip des beschränkten Zugangs „per default“ verstoßen.

dd) Die Beklagte hat darüber hinaus weder der Klägerseite noch die zuständige Aufsichtsbehörde, die Irish Data Protection Commission, von dem Datenschutzverstoß informiert. Sie ist somit weder ihrer Informationspflicht nach Art. 34 noch nach Art. 33 DSGVO nachgekommen.

Dem Wortlaut des Art. 33 Abs. 1 S. 1 DSGVO ist unmittelbar zu entnehmen, dass der Verantwortliche zu einem „unverzüglichen Handeln“ ab Kenntniserlangung von der Verletzung des

Schutzes von personenbezogenen Daten verpflichtet ist.

In Art. 34 DSGVO findet sich im Wortlaut zwar kein vergleichbarer Zeitpunkt, denknotwendig ist hinsichtlich des Beginns der Frist zur Benachrichtigung der betroffenen Personen der gleiche Maßstab anzusetzen wie auch bei Art. 33 Abs. 1 S. 1 DSGVO. Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person zur Folge, so ist der Betroffene unverzüglich nach der Kenntniserlangung zu benachrichtigen.

Bei der Beurteilung der Unverzüglichkeit der Benachrichtigung – ebenso wie bei der Meldung nach Art. 33 DSGVO – müssen die Art und Schwere der Schutzverletzung und deren Folgen und nachteiligen Auswirkungen auf die Betroffenen berücksichtigt werden (ErwGr 86). Wenn das Risiko eines unmittelbar drohenden Schadens begrenzt werden muss, ist eine sofortige Benachrichtigung der betroffenen Person geboten; geht es darum, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Schutzverletzungen in der Zukunft zu treffen, kann eine längere Benachrichtigungsfrist gerechtfertigt sein (ErwGr 87).

Auch die Behebung eines Datenschutzverstoßes wie z.B. eine Sicherheitslücke zu schließen, hat unverzüglich, d.h. ohne schuldhaftes Zögern, nach Kenntniserlangung zu erfolgen. Dies ergibt sich bereits aus dem Umkehrschluss, dass nur eine rechtmäßige Datenverarbeitung zulässig ist, da dem Verantwortlichen die Datenverarbeitung untersagt ist.

Eine Datenverarbeitung ist jedoch nur rechtmäßig, wenn sie auf einer Rechtsgrundlage beruht und der Verantwortliche auch den sonstigen Pflichten zum Schutz der Daten aus der DSGVO nachkommt.

Die Beklagte kann sich auch nicht auf Art. 34 Abs. 3 DSGVO berufen, wonach eine Benachrichtigung des Betroffenen nach den dort aufgeführten Voraussetzungen nicht erforderlich ist.

Als Verantwortlicher hat sie insbesondere keine geeigneten technischen und organisatorischen Sicherheitsvorkehrungen getroffen und diese Vorkehrungen auch nicht auf die von der Verletzung betroffenen personenbezogenen Daten angewandt. Insbesondere hat sie auch nicht solche Vorkehrungen getroffen, durch die die personenbezogenen Daten für alle Personen unzugänglich gemacht wurden, die nicht zum Zugang zu den personenbezogenen Daten berechtigt waren – etwa durch Verschlüsselung.

Auch wäre eine Benachrichtigung der Klägerseite nicht mit einem unverhältnismäßigen Aufwand für die Beklagte verbunden gewesen. In diesem Fall wäre es ihr bereits im Jahr 2019

möglich gewesen, stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme durchzuführen, durch welche auch die Klägerseite als betroffene Personen über die Verletzung des Schutzes von personenbezogenen Daten wirksam informiert worden wäre.

Im Gegenteil, die Klägerseite ist von der Beklagten nicht ab Kenntniserlangung von der Verletzung unterrichtet worden.

ee) Schlussendlich ist die Beklagte dem Auskunftsersuchen der Klägerseite über ihre personenbezogenen Daten nicht in ausreichendem Maße des Schutzes nachgekommen.

Der Anspruch auf Auskunftserteilung ergibt sich aus Art. 15 DSGVO. Danach hat ein Betroffener einen Anspruch gegen den Datenverarbeiter. Dieser beinhaltet insbesondere die Verarbeitungszwecke und die Empfänger bzw. Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt wurden (Art. 15 Abs. 1 a) und c) DSGVO).

ErwGr 63 S. 7 DSGVO spezifiziert weiter, dass bei einer großen Menge von verarbeiteten Daten, wie im Falle der Beklagten gegeben eine Konkretisierung im Auskunftsersuchen möglich ist. Eine solche Konkretisierung ist Seiten der Klägerseite erfolgt. Darin wurde die Beklagte aufgefordert, über den oben ereigneten Datenschutzvorfall Auskunft zu erteilen, insbesondere darüber, welchen Empfängern die Daten der Klägerseite durch Ausnutzung des Kontakt-Import Tools zugänglich gemacht wurden. Ein derartiges Verlangen ist von Art. 15 DSGVO gedeckt, der dies explizit zulässt.

Diesem Verlangen ist die Beklagte nicht in ausreichendem Maße nachgekommen. Sie hat lediglich allgemein angezeigt, welche Arten von Daten sie von der Klägerseite verarbeitet. Eine konkrete Auskunft zum in Rede stehenden Datenschutzvorfall hat sie jedoch nicht gemacht. Weder wurde darüber informiert, wer auf die Daten zugegriffen hat, noch wurde aufgeklärt welche Daten genau auf diesem Wege abgegriffen wurden. Konkret wurde keine Information darüber erteilt, welche Daten zum Zeitpunkt des Datenschutzvorfalls im Jahr 2019 für wen einsehbar waren.

b) Schaden

Nach Art. 82 Abs. 1 DSGVO hat die betroffene Person, die einen Schaden erlitten hat, gegen den verantwortlichen einen Schadensersatzanspruch.

Nach ErwGr. 146 S. 3 soll der Begriff des Schadens

„(...) im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt

werden, die den Zielen dieser Verordnung in vollem Umfang entspricht“.

Daraus kann abgeleitet werden, dass der nach Abs. 1 bereits weite Schadensbegriff im Zweifel weit ausgelegt wird (Gola/Piltz RDV 2015, 279 (284).

Dass es sich um einen materiellen und einen immateriellen Schaden handeln kann, legt Abs. 1 bereits fest. In den ErwGr 75 und 85 werden einige mögliche Schäden aufgezählt, darunter Identitätsdiebstahl, finanzielle Verluste, Rufschädigung, aber auch der Verlust der Kontrolle über die eigenen Daten sowie die Erstellung unzulässiger Persönlichkeitsprofile. Zudem nennt Erwägungsgrund 75 auch die bloße Verarbeitung einer großen Menge personenbezogener Daten einer großen Anzahl von Personen. Der Schaden ist zwar weit zu verstehen, er muss jedoch auch wirklich „erlitten“ (ErwGr. 146 S. 6), das heißt „spürbar“, objektiv nachvollziehbar, von gewissem Gewicht sein (AG Diez v. 7. 11. 2018, Az. 8 C 130/18), um bloße Unannehmlichkeiten oder Bagatellschäden auszuschließen.

Mit wenigen Ausnahmen hatten bisher vor allem Untergerichte über geltend gemachte Schadensersatzansprüche nach Art. 82 DSGVO zu entscheiden. In knapp einem Dutzend veröffentlichten Urteilen wurde ein immaterieller Schadensersatz zugesprochen. Einige der Gerichte haben dabei ausdrücklich auf die notwendige Abschreckungswirkung Bezug genommen. (ArbG Neumünster ZD 2021, ZD Jahr 2021 171; ArbG Düsseldorf NZA-RR 2020, 409).

Die Gerichte taxierten die Ersatzpflicht für die verspätete Auskunft mit 500 Euro bis 1.000 Euro pro Monat (LG Lüneburg Urt. v. 14.7. 2020 – AZ 9 O 145/19, BeckRS 2020, 36932 ; AG Pforzheim ZD 2021, 50; ArbG Dresden ZD 2021, 54).

Der Schadensersatzanspruch nach Art. 82 DSGVO hat eine abschreckende Präventionsfunktion. Der Sinn und Zweck dieser Vorschrift würde ausgehöhlt werden, wenn man übermäßige Anforderungen an die Schwere und die Darlegung einer Beeinträchtigung stellen würde. Datenschutzrechtliche Fälle sind nämlich gerade durch ein hohes Maß an Ungewissheit geprägt, dass selbst bei drastischen Verstößen und substanziellen Risiken für die Betroffenen nicht zulässt, erhebliche, konkrete und „objektiv nachvollziehbare“ Schäden zu belegen. Anschaulich ist das Beispiel des Fahrzeugvermieters Buchbinder, von dessen massivem Datenleck 3,1 Mio. Kunden betroffen waren. Nur den wenigsten wird gelingen, einen konkreten Vermögensschaden, einen Identitätsdiebstahl oder eine Rufschädigung nachzuweisen, obschon nahezu sämtliche gespeicherten Informationen im Netz frei zugänglich waren, einschließlich detaillierter Unfallberichte, Führerschein-, Ausweis- und Zahlungsdaten. Wenn allerdings hohe Erheblichkeitsschwellen bestehen oder der bloße Kontrollverlust oder das Gefühl der Unsicherheit

nicht genügen sollen, wird Buchbinder trotz dieses gravierenden Datenschutzverstoßes wenig zu befürchten haben. Entstehen den Betroffenen keine materiellen Schäden, sollte im vorliegenden Fall zumindest auch durch den Verstoß gegen die DSGVO (s.o.), durch die öffentliche Zugänglichmachung der Daten, ein immaterieller Schaden angenommen werden können. Aus diesem Grund hat auch das LG München I im Falle eines Datenlecks ohne bisher erfolgten Identitätsdiebstahl auf Grund der bloßen Gefährdung einen Schadensersatz zugesprochen (LG München I, Urt. v. 9.12.2021, - 31 O 16606/20, BeckRs 2021, 41707 Rn. 42; LG München I, Urt. v. 20.01.2022 – 3 O 17493/20, BeckRS 2022, 612).

Der Klägerseite erlitt durch die unbefugte Veröffentlichung ihrer personenbezogenen Daten einen konkreten schadensersatzfähigen Schaden. Dieser besteht darin, dass die Klägerseite einen erheblichen Kontrollverlust über ihre Daten erlitten hat und in einem Zustand großen Unwohlseins und Sorge über möglichen Missbrauch ihrer Daten verbleibt. Dies manifestierte sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen, aber auch in der ständigen Sorge, dass die veröffentlichten Daten von kriminellen für unlautere Zwecke verwendet werden könnten.

Zudem beruht der Schaden auf einem Datenleck, von dem eine unüberschaubare Vielzahl von Personen betroffen ist. Verstöße dieser Art werden von ErwGr 75 aE DSGVO („wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft“) beispielhaft als ein Fall des erlittenen Schadens verstanden. Daraus ist zu schließen, dass unter der DSGVO die Folgen von Verstößen wie dem vorliegenden grundsätzlich als Schaden zu behandeln sind, um dem Zweck der DSGVO, ein möglichst hohes und umfassendes Schutzniveau der Betroffenen zu gewährleisten, gerecht zu werden. Es ist deswegen auch im Wege des effet utile-Grundsatzes geboten, in Fällen wie dem vorliegenden einen Schadensersatz zu gewähren, um die effektive Durchsetzung des Unionsrechts umfassend zu gewährleisten.

Seit April 2019 erhält die Klägerseite vermehrt dubiose Nachrichten und EMails der oben beschriebenen Art.

Die abgegriffenen und veröffentlichten Daten bedeuten für die Klägerseite ein hohes Risiko und Unsicherheit, wer nun ihre Daten zu welchen Zwecken unbefugt benutzt. Die negativen Folgen können vielfältig sein und schwere Nachteile mit sich bringen. Angefangen von vermehrter Belästigung durch Spam- und Werbemails bzw. Spam- und Werbenachrichten über Mobilfunknummer, über die Zusendung von Viren, einen möglichen Identitätsdiebstahl bis hin zu vermögenswirksamen Handlungen im Namen und zu Lasten der Klägerseite.

Doch all dies kann nach einer Vielzahl von Gerichten dahinstehen, weil bereits der Verstoß gegen die DSGVO und eine etwaig damit einhergehende rechtswidrige Verarbeitung von personenbezogener Daten – wie vorliegend – einen Schadensersatzanspruch der konkret betroffenen Person begründet.

So führt beispielsweise das Bundesarbeitsgericht (BAG, Beschluss 26.08.2021 - 8 AZR 253/20 (A)) aus:

„Insoweit geht der Senat in Kenntnis Vorabentscheidungsersuchens des Obersten des Gerichtshofs (Österreich) (- C-300/21 -) davon aus, dass Art. 82 Abs. 1 DSGVO ein Recht auf Schadenersatz nur für Personen vorsieht, die selbst wegen der Verletzung einer oder mehrerer Bestimmungen der DSGVO bei der Verarbeitung "ihrer" personenbezogenen Daten (vgl. 2. Erwägungsgrund der DSGVO) in ihren (subjektiven) Rechten verletzt worden sind, die also selbst Opfer eines Verstoßes bzw. mehrerer Verstöße gegen die DSGVO geworden sind. Ferner geht der Senat davon aus, dass der Rechtsanspruch auf immateriellen Schadenersatz nach Art. 82 Abs. 1 DSGVO über eine solche Verletzung der DSGVO hinaus nicht zusätzlich erfordert, dass die verletzte Person einen (weiteren) von ihr erlittenen immateriellen Schaden darlegt. Sie muss also aus Sicht des Senats keine "Konsequenz oder Folge der Rechtsverletzung von zumindest einigem Gewicht" (vgl. dazu jedoch die dritte Vorlagefrage des Vorabentscheidungsersuchens des Obersten Gerichtshofs (Österreich) - C-300/21 -) darlegen. Nach Auffassung des Senats führt demnach bereits die Verletzung der DSGVO selbst zu einem auszugleichenden immateriellen Schaden.“

Eben dieses ist auch vorliegend festzustellen.

c) Kausalität

Die oben dargelegten Verstöße sind zudem auch kausal für den entstandenen Schaden. Der Schaden ist „wegen“ der Verstöße gegen diese Verordnung eingetreten.

Die zivilrechtlichen Grundsätze zur Kausalität sind anwendbar. Ausreichend ist eine Mitursächlichkeit bei Entstehung des Schadens. Allerdings muss der eingetretene Schaden gerade durch den geltend gemachten Rechtsverstoß eingetreten sein.

Hätte die Beklagte ausreichend und im angemessenen Umfang über die Folgen der Preisgabe der Telefonnummer informiert, so hätte die Klägerseite keine Einwilligung erteilt und ihre Telefonnummer nicht angegeben. Insbesondere, wenn klar darauf hingewiesen worden wäre, dass kein Schutz vor dem Abgreifen durch automatische Verfahren besteht, wäre eine Einwil-

ligung zur Verarbeitung nicht erteilt und die Telefonnummer nicht veröffentlicht worden.

Ebenso ist die Nichtvornahme entsprechender Schutzmaßnahmen gegen das automatische Abgreifen der Daten sowie gegen die Ausnutzung der Sicherheitslücke, die ein Abgreifen von nicht öffentlichen Daten ermöglichte, ursächlich für den Schaden der Klägerseite geworden. Wären derartigen Maßnahmen vorgenommen worden, wäre es mit an Sicherheit grenzender Wahrscheinlichkeit nicht möglich gewesen, mit einem automatisierten Verfahren Daten abzugreifen. Das Abgreifen hat durch die anschließende Veröffentlichung unmittelbar im Schaden der Klägerseite gemündet.

Auch die unterlassene Information der Klägerseite oder der Behörden hat zu einer Intensivierung des Schadens geführt. Durch einen auf mangelnder Unterrichtung beruhenden Zeitraum der Ungewissheit haben sich die Risiken, dass die Daten unbemerkt missbraucht werden, und damit das Unwohlsein und die Sorgen der Klägerseite, entschieden gesteigert. Wäre angemessen zügig eine Benachrichtigung erfolgt, so hätten zeitnah Schritte zur Risikominimierung und Absicherung eingeleitet werden können, um einen Schaden zu vermeiden.

d) Verschulden

Art. 82 Abs. 1 DSGVO begründet einen Anspruch zugunsten der Person, der wegen eines Verstoßes gegen die DSGVO ein Schaden entstanden ist. Damit kommt es zur Begründung des Anspruchs auf ein Verschulden nicht an. Der Exculpationsnachweis nach Abs. 3, nach welchem derjenige von einer Ersatzpflicht frei wird, der unter „keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“, hat die Beklagte nicht erbracht.

Das Bundesarbeitsgericht (BAG, Beschluss v. 26.08.2021 - 8 AZR 253/20 (A)) erklärt:

„Der Senat nimmt allerdings an, dass die Haftung des Verantwortlichen (bzw. Auftragsverarbeiters) nach Art. 82 Abs. 1 DSGVO verschuldensunabhängig ist, also diese Bestimmung die Haftung des Urhebers eines Verstoßes keineswegs vom Vorliegen oder dem Nachweis eines Verschuldens abhängig macht (vgl. zu anderen Bereichen des Unionsrechts etwa: EuGH 22. April 1997 - C180/95, EU:C:1997:208 - [Draehmpaehl] Rn. 17; 8. November 1990 C-177/88, EU:C:1990:383 - [Dekker] Rn. 22). Wie unter Rn. 33 ausgeführt, geht der Senat davon aus, dass bereits die Verletzung der DSGVO als solche für einen Anspruch nach Art. 82 Abs. 1 DSGVO ausreicht.“

Eben dieses ist auch vorliegend festzustellen.

e) Höhe des Anspruches

Ein Schadensersatz in Höhe von 1.000,- EUR ist vorliegend angemessen.

Art. 82 Abs. 1 DSGVO macht zwar bezüglich der Höhe des Schadensersatzanspruchs keine Vorgaben und auch in der Rechtsprechung bestehen bezüglich der Höhe Unsicherheiten. Bedenkt man jedoch das Ziel des Schadensersatzanspruches nach Art. 82 Abs. 1 DSGVO, Verstöße effektiv und vor allem abschreckend zu sanktionieren, ist ein Schadensersatzanspruch in der Höhe von mindestens 1.000,00 Euro für die vorliegenden Verstöße der Beklagten gerechtfertigt. Auch ErwGr 146 S. 6 fordert, dass die betroffene Person „einen vollständigen und wirksamen Schadensersatz“ für den erlittenen Schaden erhalten soll. In der bisherigen Rechtsprechung lagen zugesprochene Ersatzsummen im mittleren vierstelligen Bereich. Zu erwarten ist aber, dass Entschädigungszahlungen künftig deutlich höher ausfallen werden, da dem Schadensersatzanspruch nicht nur eine generell präventive, sondern zugleich auch sanktionierende Wirkung zukommt.

Die Höhe des Anspruchs ist bei immateriellen Schäden nicht willkürlich, sondern auf der Grundlage der inhaltlichen Schwere und Dauer der Rechtsverletzung zu beurteilen. Genugtuungs- und Vorbeugungsfunktion spielen bei der Bezifferung eine Rolle.

Ausgangspunkt für die Berechnung des immateriellen Schadensersatzes ist der weit auszulegende europarechtliche Schadensbegriff. Konkret bedeutet das, die Beträge hoch anzusetzen, um die geforderte wirksame und abschreckende Wirkung zu erzielen.

Bei den bisher zugesprochenen Schadensersatzansprüchen variieren die Beträge zwischen 300 Euro und 5.000 Euro (LG Darmstadt ZD 2020, 642: 1.000 Euro wegen Übermittlung von Bewerberdaten an Dritte; LG Lüneburg Urt. v. 14.7. 2020 - AZ 9 O 145/19, BeckRS 2020, 36932: 1.000 Euro wegen unzulässiger Meldung an Wirtschaftsauskunftei; ArbG Dresden ZD 2021, 54: 1.500 Euro wegen unbefugter Weitergabe von Gesundheitsdaten; ArbG Köln Urt. v. 12.3. 2020 – AZ 5 Ca 4806/19, BeckRS 2020, 31544: 300 Euro für PDF-Datei auf Homepage, nicht angegriffen vor LAG Köln ZD 2021, 168).

Bemerkenswert sind dabei Entscheidungen, die wegen der Verletzung von Auskunftsansprüchen 1.500 Euro bzw. 5.000 Euro zugesprochen haben, obwohl sie den entstandenen immateriellen Schaden als „nicht sehr groß“ und „nicht erheblich“ angesehen haben. Der Schaden liegt in der Ungewissheit über die Verarbeitung der eigenen Daten (ArbG Neumünster ZD 2021, 171 Rn 38; ArbG Düsseldorf NZA-RR 2020, 409 Rn. 85ff.). Die Gerichte taxierten die Er-

satzpflicht für die verspätete Auskunft mit 500 Euro bis 1.000 Euro pro Monat.

Im Vergleich zu den genannten Beispielen handelt es sich im vorliegenden Fall um einen Schaden mittlerer Intensität: Die entwendeten Daten sind zwar keine so höchstpersönlichen oder sensiblen, dass ein besonders intensiver Eingriff in die Privatsphäre der Klägerseite vorläge. Allerdings sind sie sehr umfangreich und ermöglichen in Verknüpfung mit dem Facebookprofil vielfältige Möglichkeiten für kriminelle Akteure, was der Klägerseite große Sorgen und gehöriges Unwohlsein bereitet.

Hinzu kommt die fehlerhafte Auskunftserteilung über die Empfänger der Daten.

Im Vergleich zu den oben bezifferten Schadensfällen liegt hier ein schwerer Verstoß vor als im Falle einer bloßen verspäteten Auskunftserteilung, die regelmäßig mit 500 Euro pro Monat angesetzt wird: Der befürchtete Kontrollverlust über die Daten ist hier tatsächlich eingetreten und birgt tatsächliche Risiken für die Klägerseite. Damit ist der ausgleichsbedürftige Schaden höher als derartige Auskunftsersuche anzusetzen, die hier dennoch erschwerend hinzukommen: Hier wirken sowohl Datenschutzverstoß als auch mangelhafte Erfüllung des Auskunftsbegehrens kumulativ zusammen. Ähnlich wiegt der Verstoß schwerer als etwa das bloße versehentliche Versenden einer E-Mail an einen einzelnen falschen Empfänger, welcher sogar mit einer Schadenshöhe von 1.000 Euro angesetzt wurde (so LG Darmstadt, ZD 2020, 642).

Auf Grund dessen ist ein Schadenersatzanspruch in Höhe von 1.000,00 EUR angemessen.

2. Feststellung zur Tragung zukünftiger Schäden

Aus der Verpflichtung der Beklagten zur Leistung von Schadensersatz aus dem dargestellten Schadensereignis folgt auch die Pflicht, zukünftige Schäden, die auf Grund der entwendeten Daten entstehen, zu tragen. So kann zum jetzigen Zeitpunkt noch nicht abgesehen werden, welche Dritten Zugriff auf die Daten des Klägers erhalten haben und für welche konkreten kriminellen Zwecke die Daten missbraucht werden. Um einen zukünftigen Prozess zu vermeiden, kann bereits jetzt mit Feststellungsinteresse i.S. d. § 256 ZPO festgestellt werden, dass die Beklagte für die aus dem Schadensereignis kausal entstehenden Schäden einzustehen hat (vgl. BGH, Urt. v. 20. 3. 2001 - VI ZR 325/99, NJW 2001, 3414). Ihrem Wesen nach zeigen sich die Folgen von Datenschutzverletzungen erst spät, oft bleiben sie lange unerkannt. Dies zeigt sich nicht zuletzt daran, dass auch das Datenleck bei Facebook, das schon seit Jahren bestand, erst vor Kurzem offenbar wurde. Es ist deshalb im Interesse des Klägers und der all-

gemeinen Rechtssicherheit, eine Haftung der Beklagten schon jetzt festzustellen, um später auf Grund des Zeitablaufs entstehende Unsicherheiten zu vermeiden.

3. Unterlassung

Dem Kläger steht auch nach §§ 1004 analog, 823 Abs 1 und aus Abs. 2 BGB i.V.m. Art. 6 Abs. 1 DSGVO sowie Art. 17 DSGVO gegen die Beklagte ein Anspruch auf Unterlassung, ihre personenbezogenen Daten in Zukunft unbefugt, d.h. konkret ohne vorherige ausreichende Belehrung, zu veröffentlichen und diese zukünftig unbefugten Dritten zugänglich zu machen, zu.

Die DSGVO ist ein Schutzgesetz i. S. d. § 823 Abs. 2 BGB, da sie Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten schützt. Grundsätzlich kann Verstößen gegen die DSGVO also im Wege eines Unterlassungsanspruchs entgegengetreten werden (Umfassend Leibold/Laoutoumai, ZD-Aktuell 2021, 05583 mwN.).

Die Beklagte hat gegen Art. 6 DSGVO verstoßen, indem sie unrechtmäßig personenbezogene Daten der Klägerseite verarbeitet hat.

Die in Frage kommende Rechtsgrundlage der Einwilligung (Art. 6 Abs. 1 a) DSGVO) erfordert, dass der Betroffene hinlänglich informiert wurde (Art. 7 Abs. 2 DSGVO). An einer solchen Information fehlt es in den Belehrungen der Beklagten, sodass die Einwilligung nicht freiwillig erteilt wurde.

Mangels Rechtsgrundlage erfolgte die Verarbeitung der Daten der Klägerseite deshalb in rechtswidriger Weise.

Die Beklagte hat zudem unbefugten Dritten personenbezogene Daten der Klägerseite zugänglich gemacht, indem sie eine ihnen bekannte Sicherheitslücke ihrer Netzwerke nicht unverzüglich geschlossen haben (vgl. obige Ausführungen). Das Zugänglichmachen personenbezogener Daten ist ohne Zweifel eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO.

Eine solche Verarbeitung personenbezogener Daten ist gem. Art. 6 DSGVO nur dann rechtmäßig, wenn eine der in Art. 6 Abs. 1 S. 1 lit. a - f DSGVO genannten Rechtsgrundlagen einschlägig ist. Im vorliegenden Fall erfolgte das Zugänglichmachen der personenbezogenen Daten der Klägerseite ohne eine der in Art. Art. 6 Abs. 1 S. 1 lit. a - f DSGVO aufgeführten Rechtsgrundlagen.

Insbesondere hat die Klägerseite zum Zugänglichmachen ihrer personenbezogenen Daten für Unbefugte keine in informierter Art und Weise erteilte Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO erklärt. Die hierfür notwendige Belehrung hat die Beklagte – wie oben dargelegt - nicht ordnungsgemäß beigebracht. Diese Datenverarbeitung ist auch nicht für die Erfüllung eines Vertrages, deren Vertragspartei sie ist, erforderlich nach Art. 6 Abs. 1 S. 1 lit. b DSGVO. Weiterhin besteht auch kein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 S. 1 lit. f DSGVO am Zugänglichmachen der personenbezogenen Daten der Klägerseite für Unbefugte.

Dieser Verstoß gegen Art. 6 DSGVO ist rechtswidrig. Eine Rechtswidrigkeit entfällt auch nicht aufgrund § 1004 Abs. 2 BGB. Für die Klägerseite besteht hier insbesondere keine Duldungspflicht wegen einer möglichen eigenen Veröffentlichung ihrer personenbezogenen Daten. Zwar hat die Klägerseite ihre personenbezogenen Daten selbst bei Erstellung ihres Nutzerprofiles angegeben, hierdurch liegt allerdings keine Veröffentlichung dieser vor. Denn diese Angaben wurden ausschließlich der Beklagten gegenüber zum Zwecke der Registrierung gemacht.

Da die personenbezogenen Daten der Klägerseite unrechtmäßig Dritten zugänglich gemacht wurden, können diese Daten unbefugt verwendet werden. Hierdurch wird die Klägerseite insbesondere gegenwärtig in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt. Weitere Beeinträchtigungen durch eine unrechtmäßige Verwendung personenbezogenen Daten drohen.

Weiterhin besteht ein Unterlassungsanspruch gegen die Beklagte, die rechtswidrige Verarbeitung der personenbezogenen Daten der Klägerseite– hier eine Datenverarbeitung ohne Erfüllung der Informationspflichten - gemäß §§ 1004 analog, 823 Abs. 2 BGB i.V.m. Art. 13, 14 DSGVO zu unterlassen.

Wie oben dargelegt ist die DSGVO ein Schutzgesetz im Sinne des § 823 Abs. 2 BGB.

Indem die Beklagte die Klägerseite nicht – wie oben bereits dargelegt – ausreichend nach Art. 13, 14 DSGVO über die (weitere) Nutzung der mitgeteilten Mobilfunknummer informiert hat, hat sie rechtswidrig gegen Art. 13, 14 DSGVO verstoßen. Als Verantwortliche der Datenverarbeitung oblag es ihr jedoch, die von der Datenverarbeitung betroffene Person – hier die Klägerseite - über jegliche Verarbeitung zu informieren. Die Klägerseite hat den Verstoß gegen die Informationspflichten nach DSGVO weiterhin nicht zu dulden.

Indem die Beklagte der ihr obliegenden Informationspflichten nicht ausreichend nachgekommen sind, ist die Klägerseite in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt. Diese Beeinträchtigung besteht sowohl gegenwärtig als auch zukünftig. Datenschutz-

rechtliche Ansprüche können im Wege des Unterlassungsanspruches geltend gemacht werden. Solche Ansprüche sind nicht aufgrund von Art. 79 DSGVO gesperrt (vgl. BGH, Urt. v. 12.10.2021 VI ZR 488/19; LG Frankfurt a.M., Urt. v. 15. 10. 2020; LG Frankfurt a.M., Urt. v. 13.09. 2018 – 2-03 O 283/18).

4. Auskunft

Der Auskunftsanspruch ist entsprechend wie oben unter II. 1. aa) und ee) ausgeführt gemäß Art. 15 DSGVO im beantragten Umfang begründet.

5. Rechtsanwaltskosten

Die vorgerichtlichen Rechtsanwaltskosten ergeben sich aus Anlage K1 und die Verzinsungspflicht aus §§ 288 Abs.1, 291 BGB.

C.

Die Kostenentscheidung beruht auf § 91 Abs. 1 ZPO. Der Ausspruch über die vorläufige Vollstreckbarkeit erfolgt gemäß § 708 Nr. 2 ZPO.

Rechtsbehelfsbelehrung:

Gegen dieses Urteil ist der **Einspruch** zulässig.

Der Einspruch ist binnen einer Notfrist von **2 Wochen** bei dem

Landgericht Zwickau
Platz der Deutschen Einheit 1
08056 Zwickau

einzulegen.

Die Frist beginnt mit der Zustellung des Urteils.

Vor dem Landgericht herrscht Anwaltszwang. Daher kann nur ein Rechtsanwalt/ eine Rechtsanwältin wirksam Einspruch einlegen, Anträge stellen und weitere Erklärungen abgeben. Handlungen, die die Partei selbst vornimmt, sind prozessrechtlich unwirksam.

Die Einspruchsschrift muss das Urteil, gegen das sich der Einspruch richtet, bezeichnen und die Erklärung enthalten, dass gegen dieses Urteil Einspruch eingelegt wird. Soll das Urteil nur zu einem Teil angefochten werden, ist der Umfang der Anfechtung zu bezeichnen.

Außerdem haben Sie innerhalb der Einspruchsfrist Ihre **Angriffs-** und **Verteidigungsmittel** (z.B. Einreden und Einwendungen gegen den gegnerischen **Anspruch**, Beweisangebote und Beweiseinreden) durch Ihren Rechtsanwalt/ Ihre Rechtsanwältin mitzuteilen. Sie werden ausdrücklich darauf hingewiesen, dass es äußerst wichtig ist, Ihre Angriffs- und Verteidigungsmit-

tel innerhalb der Einspruchsfrist vorzubringen. Versäumen Sie diese Frist, besteht die Gefahr, dass Ihnen jegliche Verteidigung abgeschnitten und der Prozess nur auf der Grundlage des gegnerischen Sachvortrages entschieden wird. Ein verspätetes Vorbringen wird vom Gericht nur zugelassen, wenn sich dadurch der Rechtsstreit nicht verzögert oder wenn Sie die Verspätung genügend entschuldigen. Verspätete verzichtbare Rügen, die die Zulässigkeit der Klage betreffen, können nur bei genügender Entschuldigung der Verspätung zugelassen werden.

Der Prozess kann also allein wegen der Versäumung der Frist zur Mitteilung der Angriffs- und Verteidigungsmittel verloren werden.

Erscheint die Frist für die Mitteilung von Angriffs- und Verteidigungsmitteln (nicht für den Einspruch selbst) als zu kurz, kann vor ihrem Ablauf um eine Verlängerung nachgesucht werden. Die Frist kann verlängert werden, wenn dadurch der Rechtsstreit nicht verzögert wird oder wenn Sie erhebliche Gründe darlegen.

Der Einspruch kann auch als elektronisches Dokument eingereicht werden. Das elektronische Dokument muss für die Bearbeitung durch das Gericht gemäß §§ 2 und 5 der Elektronischer-Rechtsverkehr-Verordnung (ERVV) geeignet sein.
Eine einfache E-Mail genügt den gesetzlichen Anforderungen nicht. Rechtsbehelfe, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument einzureichen. Das elektronische Dokument muss

1. mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein und gemäß § 4 ERVV übermittelt werden, wobei mehrere elektronische Dokumente nicht mit einer gemeinsamen qualifizierten elektronischen Signatur übermittelt werden dürfen, oder
2. von der verantwortenden Person signiert und auf einem der sicheren Übermittlungswege, die in § 130a Abs. 4 der Zivilprozessordnung abschließend aufgeführt sind, eingereicht werden.

Informationen hierzu können über das Internetportal https://justiz.de/laender-bund-europa/elektronische_kommunikation/index.php aufgerufen werden.

Schulte
Richter am Landgericht