Aktenzeichen:
7 O 10/22

Landgericht Heidelberg

Im Namen des Volkes

Urteil

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **Wilde Beuger Solmecke**, Kaiser-Wilhelm-Ring 27-29, 50672 Köln, Gz.:

gegen

Meta Platforms Ireland LimitedFacebook Ireland Ltd., vertreten durch d. Geschäftsführer (Director) Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland
- Beklagte -

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

wegen Persönlichkeitsrechtsverletzung

hat das Landgericht Heidelberg - 7. Zivilkammer - durch die Vorsitzende Richterin am Landgericht als Einzelrichterin am 31.03.2023 aufgrund der mündlichen Verhandlung vom 17.01.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von 250,00 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 07.07.2022 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle weiteren materiellen Schäden zu ersetzen, die diesem 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, dem Kläger Auskunft darüber zu erteilen, durch welche Empfänger personenbezogene Daten des Klägers bei der Beklagten durch den Scraping-Vorfall im Jahr 2019 erlangt wurden.

4. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 159,94 € zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 07.07.2022 zu zahlen.

5. Im Übrigen wird die Klage abgewiesen.

6. Von den Kosten des Rechtsstreits tragen der Kläger 85 Prozent und die Beklagte 15 Prozent.

7. Das Urteil ist vorläufig vollstreckbar, für den Kläger hinsichtlich des Tenors Ziffer 3 aber nur gegen Sicherheitsleistung in Höhe von 250,00 €. Im Übrigen wird der Beklagten nachgelassen, die Vollstreckung durch den Kläger gegen Sicherheitsleistung in Höhe von 110 % des auf Grund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht der Kläger vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet. Dem Kläger wird nachgelassen, die Vollstreckung durch die Beklagte gegen Sicherheitsleistung in Höhe von 110 % des auf Grund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet.

8. Der Streitwert wird auf 6.000,00 € festgesetzt.

Tatbestand

Die Parteien streiten über Ansprüche auf Schadensersatz, Unterlassung, Auskunft und Nebenforderungen aufgrund behaupteter Verstöße der Beklagten gegen die Datenschutzgrundverordnung (DS-GVO) im Zusammenhang mit einem sog. „Scraping-Vorfall“ bei der Beklagten.

Der Kläger nutzt das soziale Netzwerk Facebook, das auf dem Gebiet der Europäischen Union von der Beklagten betrieben wird und auf das sowohl über die Website www.facebook.com als auch über die gleichnamige App mittels Smartphone oder Tablet zugegriffen werden kann. Die Plattform ermöglicht es den Nutzern, persönliche Profile einschließlich privater Fotos und weiterer Informationen für sich zu erstellen und diese auf Facebook mit Freunden zu teilen. Der Kläger nutzt Facebook, um mit Freunden zu kommunizieren, zum Teilen privater Fotos und für Diskussionen mit anderen Nutzern.

Auf ihren persönlichen Profilen können die Nutzer Angaben zu ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können. Die Beklagte stellt dabei Tools und Informationen zur Verfügung, damit Nutzer ihre Privatsphäre auf der Facebook-Plattform verwalten können. Damit Nutzer leichter mit anderen Nutzern in Kontakt treten können, müssen sie bestimmte Informationen bei der Registrierung angeben, die als Teil des Nutzerprofils immer öffentlich einsehbar sind. Dazu gehören Name, Geschlecht und Nutzer-ID. Eine Eingabe der Handynummer ist nicht zwingend erforderlich. Hinsichtlich der weiteren Daten gibt es im Rahmen der Privatsphäre-Einstellungen Wahlmöglichkeiten für jeden Nutzer. Bei der sogenannten "Zielgruppenauswahl" legt der Nutzer fest, wer einzelne Informationen auf seinem Facebook-Profil, wie etwa Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse, einsehen kann. So kann der Nutzer anstelle der standardmäßigen Voreinstellung "öffentlich" auswählen, dass nur "Freunde" auf der Plattform, oder "Freunde von Freunden" die jeweiligen Informationen einsehen können. Lediglich die Telefonnummer des Nutzers wird insoweit gesondert behandelt, als dass diese standardmäßig nur der Nutzer selbst (AS 13) - so der Kläger - oder nur "Freunde" (AS 79) - so die Beklagte - einsehen kann.

Die "Suchbarkeits-Einstellungen" legen fest, wer das Profil eines Nutzers anhand einer Telefonnummer finden kann. Wenn also ein Nutzer in seinem Smartphone eine Telefonnummer als Kontakt eingespeichert hat, erlaubt ihm die Beklagte, seine Kontakte mit den bei Facebook hinterleg-

ten Telefonnummern abzugleichen, um die hinter den Nummern stehenden Personen als Freunde hinzuzufügen. Dafür war nicht erforderlich, dass der andere Nutzer seine Telefonnummer nach der "Zielgruppenauswahl" öffentlich gemacht hat. Demnach war es möglich, Nutzer anhand einer Telefonnummer zu finden, solange ihre "Suchbarkeits-Einstellung" für Telefonnummern auf der Standard-Voreinstellung "alle" eingestellt war. Daneben waren die Einstellungen nur "Freunde von Freunden" oder "Freunde" auswählbar. Ab Mai 2019 stand Nutzern auch die Option "Nur ich" zur Verfügung. Die "Suchbarkeits-Einstellung" war bei dem Kläger seit dem 13.11.2016 auf "Alle" eingestellt (Anl. B17).

Bei der Registrierung wird der Nutzer auf die Datenrichtlinie der Beklagten (Anl. B9) hingewiesen. Im auf der Homepage von Facebook verlinkten „Hilfebereich“, werden dem Nutzer Informationen über die Privatsphäre-Einstellungen zur Verfügung gestellt. Auf diese Einstellungen kann unter der Überschrift "Privatsphäre, Datenschutz und Sicherheit" zugegriffen werden. Wegen der relevanten Inhalte im Hilfebereich und in den Einstellungen wird auf die Abbildungen in der Klageschrift sowie die Anl. B1 bis B8 verwiesen.

Mit Geltungsbeginn der DSGVO am 25. Mai 2018 wies die Beklagte Nutzer der Facebook-Plattform in der EU nochmals explizit auf die im April 2018 aktualisierte Datenrichtlinie (Anl. B20) hin und forderte die Nutzer zur Überprüfung ihrer Privatsphäre-Einstellungen auf. Die Nutzer wurden zudem aufgefordert, den aktualisierten Nutzungsbedingungen zuzustimmen.

Außerdem ist es dem Nutzer überlassen, ob er als zusätzliche Sicherheitsmaßnahme im Sinne einer Zwei-Faktor-Authentifizierung seine Telefonnummer angibt. Wenn der Nutzer von anderen Gruppen von Nutzern nicht über diese Telefonnummer gefunden werden möchte, ist dies anhand einer separaten Privatsphäreeinstellung vorzunehmen, welche wiederum die Standardeinstellung „öffentlich“ aufweist.

Auf der daneben existierenden Facebook-Messenger-App bestand für die Nutzer die Möglichkeit, mithilfe eines „Contact-Import-Tools“ (im Folgenden: „CIT“) ihre auf dem Handy befindlichen Telefonkontakte auf Facebook hochzuladen, um diese automatisch auf der Facebook-Plattform zu finden und mit ihnen in Verbindung zu treten, ohne dass deren im Profil hinterlegte Nummer in der "Zielgruppenauswahl" öffentlich gemacht worden wäre.

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 im In-

ternet. Vorausgegangen war ein sog. „Datenscraping“ im Zeitraum von Januar 2018 bis September 2019. Scraping stellt eine weitverbreitete Methode zum massenhaften, automatisierten Sammeln von typischerweise öffentlich zugänglichen persönlichen Daten von Internetseiten durch automatisierte Softwareprogramme abzurufen. Dieses Sammeln von Daten mittels automatisierter Tools und Methoden war und ist nach den Nutzungsbedingungen der Beklagten untersagt. Im vorliegenden Fall wurden in großer Vielzahl mögliche Telefonnummern von Nutzern, die durch die Scraper mittels einer sog. "Telefonnummernaufzählung" bereitgestellt worden waren, über das „CIT“ auf Facebook hochgeladen, um festzustellen, ob diese Telefonnummern mit einem Facebook-Konto verbunden sind. Wenn dies der Fall war, kopierten sie die öffentlich einsehbaren Informationen aus dem betreffenden Nutzerprofil und fügten die Telefonnummer den abgerufenen, öffentlich einsehbaren Daten hinzu.

Nach Bekanntwerden des Vorfalls veröffentlichte die Beklagte im April und Mai 2021 verschiedene Artikel, in denen sie den Scraping-Vorfall, Scraping im Allgemeinen sowie diverse von ihr ergriffene Schutzmaßnahmen beschrieb und die Überprüfung der Einstellungen seitens der Nutzer empfahl (Anl. B10-B12).

Außerdem führte sie weitere Schutzmaßnahmen ein. Für den Kontakt-Import etablierte sie etwa eine Funktion, die darauf abzielte, einen übereinstimmenden Kontakt nur dann anzuzeigen, wenn die beiden Nutzer einander zu kennen schienen („Social Connection Check“), in dem der Abgleich vor einer Anzeige von Nutzerdaten nicht nur anhand der Telefonnummer, sondern auch des Namens erfolgte. In der Folge wandelte die Beklagte die Kontakt-Importer-Funktion in eine Liste mit Kontaktvorschlägen um (PYMK-Funktion).

Weder die zuständige irische Datenschutzbehörde noch jeder einzelne betroffene Nutzer wurde von der Beklagten über den Vorfall informiert.

Vorgerichtlich forderte der Kläger die Beklagte mit Email seiner Prozessbevollmächtigten vom 27.10.2021 zur Zahlung von 500,00 € Schadenersatz, Unterlassung der zukünftigen Zugänglichmachung der Klägerdaten an unbefugte Dritte sowie zur Auskunftserteilung auf (Anl. K1). Mit Schreiben vom 25.11.2021 (Anl. B16) wies die Beklagte die Schadenersatz- und Unterlassungsansprüche zurück und teilte mit, dass sich unter den abgegriffenen und veröffentlichten Daten auch jene des Klägers befunden hätten und wo der Kläger seine Daten finde.

Am 25.11.2022 verhängte die irische Datenschutzbehörde (Data Protection Commission) gegen

die Beklagte ein Bußgeld wegen Verstößen gegen die DS-GVO im Zusammenhang mit dem Scraping-Vorfall (Anl. K3). Die Entscheidung wurde von der Beklagten angefochten.

Der Kläger ist der Ansicht, die Beklagte habe Vorschriften der DSGVO verletzt.

Er behauptet, seine persönlichen Daten wie Telefonnummer, Name, Wohnort, Land, Arbeitgeber seien durch "Scraping" abgegriffen worden. Ob noch mehr Daten entwendet worden seien, lasse sich mangels ausreichender Auskunft durch die Beklagte noch nicht angeben. Grundsätzlich seien von dem Vorfall Nutzerdaten wie Telefonnummer Facebook-ID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus und weitere korrelierende Daten betroffen. Die entsprechenden personenbezogenen Daten, wie auch diejenigen des Klägers, seien sodann im Internet auf Seiten, die illegale Aktivitäten wie Internetbetrug begünstigen sollen, so z.B. in dem "Hacker-Forum" raid.com, veröffentlicht worden. Sie würden insbesondere für gezielte Phishing-Attacken genutzt. Auf einer im Darknet für jedermann abrufbaren Datenbank seien Telefonnummer, Facebook-ID, Name, Geschlecht, Wohnort, Land und Arbeitgeber des Klägers zugänglich gemacht worden. Zum jetzigen Zeitpunkt könne noch nicht abgesehen werden, welche Dritten Zugriff auf die Daten des Klägers erhalten hätten und für welche konkreten kriminellen Zwecke die Daten missbraucht würden.

Die Unbekannten hätten die Daten mittels des "CIT" aus zum Teil öffentlich zugänglichen Daten bei Facebook ausgelesen und persistiert. Die Telefonnummern der Nutzer hätten wegen einer Sicherheitslücke mit den restlichen Personendaten korreliert werden können, ohne dass die hinterlegten Telefonnummern öffentlich freigegeben gewesen seien. Den Scrapern sei es möglich gewesen, sämtliche Daten des Nutzers abzufragen und zu exportieren.

Das „Scraping" sei dadurch ermöglicht worden, dass die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten "CIT" zu verhindern. So seien keine Sicherheitscaptchas (Abkürzung für "Completely Automated Public Turing Test to tell Computers and Humans Apart" - also ein vollständig automatisierter öffentlicher Turing-Test, um Computer von Menschen zu unterscheiden - verwendet worden, um sicherzustellen, dass es sich bei der Anfrage zur Synchronisierung um die Anfrage eines Menschen und nicht um eine automatisch generierte Anfrage handelt. Ein Mechanismus zur Überprüfung der Plausibilität der Anfragen sei nicht bereitgehalten worden. Der massenhafte Zugriff auf die Facebook-Profile durch Dritte mit auffälligen Telefonnummerabfragen (z.B. 000001, 000002 usw.) sei durch einfachste IP-Logs erkennbar und blockierbar gewesen. Es sei eine Kombination mehrerer Maßnahmen erforderlich,

angemessen und üblich. Die Beklagte hätte die maximale Anzahl mit dem CIT abgleichbarer Rufnummern begrenzen können. Die Suchbarkeit nach Rufnummer hätte per Default auf „Freunde-Freunde“ stehen müssen. Ein Monitoring- und Alarmierungssystem habe gefehlt, das bei Upload von sehr großen Adressbuchchargen eine Information zum Einleiten von Maßnahmen gegeben habe. Mindestens aber ein expliziter Hinweis auf die "offenen" Standard-Einstellungen für die Suchbarkeit per Telefonnummer habe gefehlt, insbesondere bei erstmaliger Erhebung der Telefonnummer des Nutzers.

Überdies seien die Einstellungen zur Sicherheit der Telefonnummer auf Facebook so undurchsichtig und kompliziert gestaltet, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne.

Die Beklagte handle aufgrund der datenschutzunfreundlichen Standard-Voreinstellungen entgegen des Prinzips der Datenminimierung und des "privacy by default"-Grundsatzes. Die versteckte Option, dass der Nutzer nicht anhand seiner Telefonnummer von der Öffentlichkeit gefunden werden möchte, sei aufgrund der vielschichtigen Einstellungsmöglichkeit nicht zu erreichen, wenn lediglich nach den Einstellungsmöglichkeiten für die Telefonnummer gesucht werde.

Die Einstellungen der Messenger-App seien unabhängig von denjenigen im sonstigen Facebook-Dienst. Eine Information über etwaige Risiken oder über die Verwendung der Telefonnummer erfolge nicht, obwohl ein Nutzer geradezu zur Verwendung des "CIT" gedrängt werde.

Die Beklagte habe ihre Nutzer nicht hinreichend über die ihr bekannten Gefahren informiert, insbesondere fehle der Hinweis, dass unberechtigte Dritte öffentlich zugängliche Daten leicht mit Hilfe von „Facebook-Tools“ anreichern, diese im Darknet veröffentlichen könnten und die Beklagte die betroffenen Personen nicht über solche Vorfälle informiere.

Der Kläger behauptet, die Veröffentlichung ihrer Daten habe weitreichende Folgen für ihn. Er habe einen erheblichen Kontrollverlust über seine Daten erlitten, welcher großes Unwohlsein und große Sorge über einen möglichen Missbrauch der sie betreffenden Daten ausgelöst habe. Er habe ein verstärktes Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen entwickelt und seit April 2021 vermehrt dubiose Nachrichten und E-Mails erhalten. Er könne nur noch mit äußerster Vorsicht auf E-Mails und Nachrichten reagieren.

Es könne zudem zum jetzigen Zeitpunkt noch nicht abgesehen werden, welche Dritte Zugriff auf

die Daten der klagenden Partei erhalten hätten und für welche konkreten kriminellen Zwecke die Daten missbraucht würden. Folgen von Datenschutzverletzungen würden sich ihrem Wesen nach erst spät zeigen und lange unerkannt bleiben. Es erscheine auf Grund der Veröffentlichung der Telefonnummern möglich, dass der Kläger durch eine Vielzahl betrügerischer Anrufe belästigt werde.

Die Beklagte habe ihre Auskunftsverpflichtung nicht erfüllt.

Ferner habe die Beklagte als Verantwortliche i.S.d. DSGVO die Klägerseite betreffende personenbezogene Daten ohne Rechtsgrundlage verarbeitet.

Die Beklagte habe weder die Klägerseite noch die Aufsichtsbehörde in ausreichendem Maße und rechtzeitig über die Verarbeitung sie betreffender personenbezogener Daten informiert bzw. aufgeklärt.

Die Beklagte trage die Darlegungs- und Beweislast, soweit die Einhaltung der DS-GVO in Streit stehe.

Der Kläger beantragt,

1. die Beklagte zu verurteilen, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 € nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

2. festzustellen, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.

3. die Beklagte zu verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 €, 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 zu verurteilen, der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.

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

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte ist der Ansicht, die Klage sei bereits aufgrund fehlender Bestimmtheit sowie nicht dargelegten Feststellungsinteresses weitgehend unzulässig.

Mit dem Scraping-Sachverhalt gehe seitens der Beklagten keine Verletzung der Rechte und Pflichten aus der DSGVO einher.

Die Beklagte behauptet, sie stelle ihren Nutzern alle in der DS-GVO festgelegten Informationen hinsichtlich der Datenverarbeitung zur Verfügung, daher sei ein Verstoß gegen Transparenzpflichten bereits im Grundsatz zu verneinen.

Zur Bekämpfung von „Scraping“ habe sie Übertragungsbegrenzungen /-beschränkungen und Bot-Erkennung eingerichtet, diese auch fortlaufend weiterentwickelt und ein Team von Datenwissenschaftlern, -analysten und Softwareingenieuren beschäftigt. Im April 2018 habe sie die Suche von Nutzern anhand der Telefonnummer in der Facebook-Suchfunktion deaktiviert. Zudem habe sie die Übertragungsbeschränkungen innerhalb der Kontakt-Importer-Funktion gesenkt, auch wenn sie zu diesem Zeitpunkt keine Scraping-Aktivität über diese Funktion festgestellt habe. Sie habe Captcha-Abfragen genutzt. Ferner gehe die Beklagte mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren gegen „Scraper“ und Hosting-Anbieter, also Unternehmen, auf deren Systemen die Daten zur Verfügung gestellt werden, vor.

Die im Internet erfolgte Veröffentlichung von Daten des Klägers habe sich nicht signifikant auf das ohnehin bestehende Risiko der Cyber-Kriminalität ausgewirkt. Es sei Teil des allgemeinen Lebensrisikos, Opfer von Internetkriminalität beziehungsweise Identitätsdiebstahl zu werden. Beim Kläger seien lediglich NutzerID, Vorname, Land und Geschlecht betroffen gewesen, wobei das Land wohl eher der Telefonnummer entnommen worden sei.

Hinsichtlich der Standardeinstellungen sei außerdem der Zweck der Facebook-Plattform maßgebend. Dieser liege gerade darin, Menschen zu ermöglichen, sich mit Freunden, Familie und Gemeinschaften zu verbinden. Daher seien die Funktionen gezielt so konzipiert, dass sie den Nutzern helfen, andere zu finden, sich mit ihnen zu verbinden und mit ihnen in Kontakt zu treten. Melde- oder Benachrichtigungspflichten hätten sie nicht getroffen, da es bereits an einer Verletzung der Sicherheit bzw. an einer unbefugten Offenlegung von Daten fehle, welche eine Verpflichtung auslösen würden.

Die Beklagte ist der Auffassung, Auskunft sei schon erteilt worden. Zur Beantwortung von Fragen betreffend die Verarbeitungstätigkeiten Dritter sei die Beklagte weder imstande noch nach Art. 15 DSGVO rechtlich verpflichtet.

Wegen der Einzelheiten des Parteivorbringens wird auf die vorbereitenden Schriftsätze nebst Anlagen sowie das Protokoll zur mündlichen Verhandlung Bezug genommen.

Die Kammer hat den Kläger persönlich angehört; auf das Protokoll der mündlichen Verhandlung vom 17.01.2023 wird verwiesen.

Entscheidungsgründe

Die Klage ist hinsichtlich des Klageantrages Ziffer 3 b) unzulässig; im Übrigen bestehen keine Bedenken gegen die Zulässigkeit (A.). Soweit die Klage zulässig ist, hat sie in der Sache nur teilweise Erfolg (B.).

A. Zulässigkeit

Die Klage ist – mit Ausnahme des Antrags Ziffer 3 b), dem das Rechtsschutzbedürfnis fehlt – zulässig.

I. Zuständigkeit

Das Landgericht Heidelberg ist für sämtliche Anträge international und örtlich (1.) sowie sachlich (2.) zuständig.

1. Die internationale und örtliche Zuständigkeit deutscher Gerichte folgt aus Art. 79 Abs. 2 S. 2 DS-GVO, der die Vorschriften der EuGVVO verdrängt (Albrecht/Jotzo, Das neue Datenschutzrecht der EU, Teil 8: Rechtsbehelfe, Haftung und Sanktionen Rn. 29, beck-online; Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 79 Rn. 33). Danach können Klagen gegen einen Verantwortlichen – von gewissen hier nicht relevanten Ausnahmen abgesehen – wahlweise auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat. Der Kläger hat seinen Wohnsitz in der Bundesrepublik Deutschland und im Bezirk des Landgerichts Heidelberg.

2. Das Landgericht Heidelberg ist gemäß §§ 23, 71 GVG auch sachlich zuständig, weil der Zuständigkeitsstreitwert 6.000,00 € beträgt und damit 5.000,00 € überschreitet.

Der Streitwert für den Klageantrag Ziffer 1 ergibt sich aus dem vom Kläger vorgestellten (Mindest-)Schadensersatzbetrag in Höhe von 1.000,00 €. Der auf Feststellung gerichtete Klageantrag Ziffer 2 ist ebenso wie der auf Auskunft gerichtete Klageantrag Ziffer 4 mit 500,00 € anzusetzen. Schließlich beträgt der Streitwert für die Unterlassungsanträge in Ziffer 3 jeweils 2.000,00 €, mithin insgesamt 4.000,00 €.

ll. Klageantrag Ziffer 1 (Schadenersatz)

Der Klageantrag Ziffer 1 ist hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO.

1. Die Bemessung des immateriellen Schadenersatzes stellt der Kläger zulässig in das Ermessen des Gerichts.

Der unbezifferte Klageantrag ist zulässig, wenn statt der Bezifferung mindestens die Größenordnung des Betrags, den der Kläger sich vorstellt, angegeben wird (h.M., vgl. MüKoZPO/Becker-Eberhard, 6. Aufl. 2020, ZPO § 253 Rn. 121). Dem ist der Kläger nachgekommen, indem er einen Mindestbetrag in Höhe von 1.000,00 € genannt hat.

2. Entgegen der Auffassung der Beklagten liegt auch keine alternative Klagehäufung vor. Eine solche ist gegeben, wenn der Kläger mehrere Streitgegenstände mit der Maßgabe geltend macht, dass das Gericht wahlweise einem dieser Begehren stattgeben soll und das jeweils andere Begehren dann nicht mehr beschieden werden muss, wobei die Prüfungsreihenfolge nicht vom Kläger vorgegeben wird, sondern im Ermessen des Gerichts liegen soll. Eine Antragstellung in dieser Form ist unbestimmt und daher unzulässig. Die Reihenfolge, in der über die einzelnen Streitgegenstände zu entscheiden ist, muss der Kläger festlegen (BeckOK ZPO/Bacher, 47. Ed. 1.12.2022, ZPO § 260 Rn. 12; MüKoZPO/Becker-Eberhard, 6. Aufl. 2020, ZPO § 260 Rn. 22).

Eine solche Konstellation liegt hier indessen nicht vor, denn der mit Klageantrag Ziffer 1 geltend gemachte Schadensersatzanspruch stellt einen einheitlichen Streitgegenstand dar. Der Streitgegenstand wird durch den Klageantrag, in dem sich die vom Kläger in Anspruch genommene Rechtsfolge konkretisiert, und den Lebenssachverhalt (Anspruchsgrund), aus dem der Kläger die begehrte Rechtsfolge herleitet, bestimmt (§ 253 Abs. 2 Nr. 2 ZPO). Zum Anspruchsgrund sind alle Tatsachen zu rechnen, die bei einer natürlichen, vom Standpunkt der Parteien ausgehenden und den Sachverhalt seinem Wesen nach erfassenden Betrachtung zu dem zur Entscheidung gestellten Tatsachenkomplex gehören, den der Kläger zur Stützung seines Rechtsschutzbegehrens dem Gericht vorträgt (vgl. BGH, Urteil vom 22. Oktober 2013 – XI ZR 42/12 –, BGHZ 198, 294-305, Rn. 15; Urteil vom 25. Juni 2020 – I ZR 96/19 –, Rn. 24, juris).

Vorliegend gründet Klageantrag Ziffer 1 auf einem einheitlichen Lebenssachverhalt, der dadurch gekennzeichnet ist, dass der Kläger zum Zeitpunkt des Scrapings auf der von der Beklagten betriebenen Facebook-Plattform angemeldet war, und die Fragen betrifft, ob die Beklagte zu diesem Zeitpunkt hinreichende Datenschutzvorkehrungen getroffen hatte, mit denen sie das Abgreifen der Daten hätte verhindern müssen, und wie sie im Nachhinein mit dem Vorfall umgegangen ist. Mit-

einander verknüpft sind sämtliche Einzelaspekte dieses Vorgangs durch die Daten, die der Kläger bei der Registrierung hinterlegt hat. Eine Aufspaltung in mehrere Abschnitte stellte eine unnatürliche Trennung eines einheitlichen Sachverhaltes dar.

lll. Klageantrag Ziffer 2 (Feststellung)

Der Feststellungsantrag ist zulässig.

1. Entgegen der Auffassung der Beklagten ist dieser Antrag hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO.

Wie bei einer Leistungsklage muss zur Individualisierung des Anspruchs der Anspruchsgrund bereits im Antrag so konkret benannt werden, dass der Umfang der Rechtshängigkeit und der Rechtskraft feststehen (BAG, NZA 2017, 342, beck-online; BeckOK ZPO/Bacher, 47. Ed. 1.12.2022, ZPO § 253 Rn. 72). Bei Ansprüchen auf Schadensersatz ist eine bestimmte Bezeichnung des zum Ersatz verpflichtenden Ereignisses erforderlich (BGH, NJW 1983, 2247, beck-online). Zur Ermittlung des Klagebegehrens ist jedoch nicht allein auf den Antrag selbst abzustellen, sondern auch die Klagebegründung heranzuziehen (BGH, Urteil vom 15. Juni 2021 – Vl ZR 576/19 –, Rn. 32, juris).

Zwar weist die Beklagte zutreffend darauf hin, dass die Formulierung des auf Feststellung der Ersatzpflicht für „*künftige (...) Schäden*“, die „*entstanden sind*“ gerichteten Klageantrages in sich widersprüchlich ist und keine Abgrenzung zu dem mit Ziffer 1 begehrten Ersatz des immateriellen Schadens erkennen lässt. Allerdings ergibt sich aus dem Vorbringen des Klägers, dass sich sein Antrag ausschließlich auf materielle Schäden richtet, die ihm aus dem Scraping-Vorfall ohne sein bisheriges Wissen entstanden sind oder die ihm noch entstehen werden. So verstanden, genügt der Antrag den Anforderungen an die Bestimmtheit.

2. Auch das für den Klageantrag Ziffer 2 erforderliche Feststellungsinteresse nach § 256 Abs. 1 ZPO liegt vor.

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 –Vl ZR 133/06).

Dies ist hier nicht der Fall. Vielmehr sind die Daten des Klägers noch im Darknet abzurufen; wer bereits in der Vergangenheit darauf zugegriffen hat und dies ggfs. in Zukunft noch in missbräuchlicher Weise tun wird, liegt völlig im Dunkeln. Dabei kann auch nicht ausgeschlossen werden, dass dem Kläger bereits ein Schaden zugefügt wurde, von dem er bislang nur noch keine Kenntnis hat.

lV. Klageanträge Ziffer 3 (Unterlassung)

Der Klageantrag Ziffer 3 a) ist zulässig, jener unter Ziffer 3 b) gestellte Antrag unzulässig.

1. Klageantrag Ziffer 3 a), mit dem der Kläger der Beklagten verbieten lassen möchte, bestimmte, im Einzelnen genannte personenbezogene Daten von ihm über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um eine Ausnutzung des Systems für andere Zwecke als die Kontaktaufnahme zu verhindern, ist – entgegen der Ansicht der Beklagten – ausreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO.

a) Nach § 253 Abs. 2 Nr. 2 ZPO darf ein Verbotsantrag nicht derart undeutlich gefasst sein, dass Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts (§ 308 Abs. 1 ZPO) nicht erkennbar abgegrenzt sind, sich die beklagte Partei nicht erschöpfend verteidigen kann, und letztlich die Entscheidung darüber, was ihr verboten ist, dem Vollstreckungsgericht überlassen bleibt (std. Rspr., vgl. BGH, Urteil vom 9. September 2021 – I ZR 90/20 –, BGHZ 231, 38-87, Rn. 19; Urteil vom 11. Februar 2021 – I ZR 227/19 –, Rn. 13, juris). Das bedeutet zwar nicht, dass die Verwendung auslegungsbedürftiger Begriffe im Antrag und in der Urteilsformel grundsätzlich und generell unzulässig wäre. Auch der Gebrauch solcher Begriffe kann hinnehmbar oder im Interesse einer sachgerechten Verurteilung zweckmäßig oder sogar geboten sein, wenn über den Sinngehalt der verwendeten Begriffe oder Bezeichnungen kein Zweifel besteht, so dass die Reichweite von Antrag und Urteil feststeht. Etwas anderes gilt aber dann, wenn im Einzelfall der Parteienstreit gerade darum geht, ob das angegriffene Verhalten unter einen bestimmten, auslegungsfähigen Begriff fällt (BGH, Urteil vom 5. Juni 1997 – I ZR 69/95 –, Rn. 39, juris).

b) Zwar erscheint auf den ersten Blick die allgemeine Fassung des Klageantrags - „*nach dem Stand der Technik möglichen Sicherheitsmaßnahmen*“ - mit dem Bestimmtheitsgebot des § 253 Abs. 2 Nr. 2 ZPO schwer zu vereinbaren und dazu angelegt, einen Teil der Entscheidung des Rechtsstreits in das Vollstreckungsverfahren zu verlagern, was im Allgemeinen nach dem oben Gesagten als nicht zulässig angesehen wird. Im Streitfall führt dies aber nicht zur Unzulässigkeit.

Denn die Frage, welche Sicherheitsmaßnahmen einzuleiten sind, kann von der Klägerseite bereits nicht näher bestimmt werden. Dies ist zum einen darauf zurückzuführen, dass die Beklagte als Verantwortliche selbst entscheiden kann, welche Maßnahmen sie wählt (Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 8), zum anderen auf die dynamische technische Entwicklung, die unter Umständen eine Anpassung der Schutzmechanismen erforderlich macht (Kühling/Buchner/Jandt, a.a.O., Rn. 9). Formulierte der Kläger also den Antrag als auf (eine) bestimmte Maßnahme(n) gerichtet, wäre dieser möglicherweise schon deshalb unbegründet, weil er gegen das Auswahlermessen der Beklagten verstieße. In – hinsichtlich der (auch hier zu verneinenden) Frage, ob der Kläger Anspruch auf die Einleitung konkreter Maßnahmen hat – vergleichbaren Fällen, nämlich den gegen rechtswidrige Immissionen wie Lärm oder Geruch gerichtete Unterlassungsbegehren hat der BGH es zugelassen, dass dieses allgemein auf Unterlassung von Störungen bestimmter Art oder auf „geeignete Maßnahmen“ gerichtet ist (vgl. Urteil vom 22. Oktober 1976 – V ZR 36/75 –, BGHZ 67, 252-254, Rn. 11; Urteil vom 17. Dezember 1982 – V ZR 55/82 –, Rn. 17, juris; NJW 1993, 1656, beck-online; s. auch Musielak/Voit/Foerste, 19. Aufl. 2022, ZPO § 253 Rn. 33). Auch im Hinblick auf die Dynamik der Entwicklung ist die Fallgruppe der gegen Immissionen gerichteten Unterlassungsanträge als dem hiesigen Begehren ähnlich zu bewerten. Denn würde der Kläger von der Beklagten bestimmte derzeit „aktuelle“ Sicherheitsmaßnahmen verlangen, könnten diese aufgrund fortschreitender technischer Entwicklungen bald wieder „veraltet“ sein, was eine erneute Klage erfordern würde. Insoweit hat der BGH es im Hinblick auf Lärmimmissionen als hinnehmbar erachtet, dass der Streit über die Wesentlichkeit von Immissionen gegebenenfalls im Vollstreckungsverfahren erneut entschieden werden müsse. Denn es sei vielfach unmöglich, mit Worten das Maß unzulässiger Einwirkungen so zu bestimmen, dass der Beeinträchtigte hinreichend geschützt wird und nicht schon eine geringfügige Änderung der Einwirkung trotz einer fortdauernden nicht zu duldenden Belästigung das Verbot hinfällig macht (BGH, NJW 1993, 1656, beck-online).

Nichts anderes kann hier gelten. Die teilweise Verlagerung der Prüfung, welche Sicherungsmaßnahmen anzuwenden wären, in das Vollstreckungsverfahren ist zur Gewährung effektiven Rechtsschutzes nach Art. 19 GG ausnahmsweise vertretbar (i.E. ebenso etwa LG Bielefeld, Urteil vom 19. Dezember 2022 – 8 O 182/22 –, Rn. 31, juris; LG Gießen, Urteil vom 3. November 2022 – 5 O 195/22 –, Rn. 24, juris).

Soweit der Kläger den Zweck der Sicherheitsmaßnahmen dahingehend umschreibt, dass die *„Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern“* erscheint dies strenggenommen als eine für die Beklagte unzumutbare und wohl auch unmögliche

Überprüfung der inneren Motivation Dritter. Die Formulierung lässt sich aber zwanglos und dem klägerischen Interesse entsprechend dahingehend auslegen, dass dem unbefugten massenhaften Zugriff auf die Daten des Netzwerkes vorgebeugt werden solle.

2. Dem Klageantrag Ziffer 3 b) fehlt das Rechtsschutzbedürfnis; er ist unzulässig.

a) Zwingende Prozessvoraussetzung für jede Klage ist ein allgemeines Rechtsschutzinteresse oder Rechtsschutzbedürfnis, das heißt ein schutzwürdiges Interesse an der gerichtlichen Geltendmachung des eingeklagten Rechts. Grundsätzlich hat jeder Rechtssuchende einen öffentlich-rechtlichen Anspruch darauf, dass die staatlichen Gerichte sein Anliegen sachlich prüfen und darüber entscheiden. Das Rechtsschutzbedürfnis kann aber fehlen, wenn das verfolgte Begehren auf einem einfacheren Weg zu erlangen ist oder wenn eine Klage objektiv schlechthin sinnlos ist, wenn also der Kläger unter keinen Umständen mit seinem prozessualen Begehren irgendeinen schutzwürdigen Vorteil erlangen kann (BeckOK ZPO/Bacher, a.a.O., Rn. 28, 30). Ein schnelleres und billigeres Mittel des Rechtsschutzes lässt das berechtigte Interesse für eine Klage nur entfallen, sofern es wenigstens vergleichbar sicher oder wirkungsvoll alle erforderlichen Rechtsschutzziele herbeiführen kann (BGH, NJW-RR 2009, 1148, beck-online).

b) Der Kläger fordert von der Beklagten, seine Telefonnummer nicht mehr auf der Grundlage einer unaufgeklärt erteilten Einwilligung zu verarbeiten. Dafür fehlt ihm das Rechtsschutzbedürfnis. Folge der vom Kläger behaupteten fehlerhaften Einwilligung ist, dass die Beklagte seine Telefonnummer nicht mehr oder nur nach Einholung einer neuen, wirksamen Einwilligung weiterverarbeiten darf.

Um zu erreichen, dass die Beklagte seine Telefonnummer nicht mehr verarbeitet, wäre es dem Kläger ohne weiteres möglich, seine im Facebook-Profil gespeicherte Telefonnummer zu entfernen. Dies bedeutete für ihn einen lediglich geringen Aufwand. Dass dieses Vorgehen einen weniger sicheren Weg darstellte, um das Ziel, die Verarbeitung seiner Telefonnummer seitens der Beklagten zu erreichen, ist nicht erkennbar. Die Behauptung des Klägervertreters in der mündlichen Verhandlung, dass nicht klar sei, ob die Beklagte die Telefonnummer etwa nach deren Löschung weiterverarbeiten würde, beruht auf reiner Spekulation. Diesbezügliche Anhaltspunkte sind nicht ansatzweise zu erkennen.

Soweit der Kläger an der weiteren Verarbeitung seiner Telefonnummer durch die Beklagte interessiert ist, diese also nicht aus seinem Profil löschen möchte, verlangt er von der Beklagten eine Aufklärung über die Art und Weise der Verarbeitung seiner Nummer, die er selbst in seinem Klageantrag formuliert. Mit dem Begehren, dass ihn die Beklagte nochmals über etwas informieren

sollte, das er ihr selbst vorgibt, vermag der Kläger keinerlei schutzwürdigen Vorteil zu erlangen. Ihm ist nämlich spätestens aus dem hiesigen Verfahren bekannt, wie seine Telefonnummer verarbeitet wird (so auch LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 169, juris, das mit dieser Argumentation allerdings zur Unbegründetheit gelangt). Damit verfügt er über eine hinreichende Grundlage, zu entscheiden, ob er mit deren Weiterverarbeitung durch die Beklagte einverstanden ist oder nicht. Eine Klage auf Unterlassung führt ihn nicht weiter.

B. Begründetheit

Die Klage ist – soweit sie zulässig ist – in der Sache nur teilweise erfolgreich. Der Kläger hat Anspruch gegen die Beklagte auf Ersatz immateriellen Schadens in Höhe von 250,00 € nebst Zinsen (I.), Feststellung zukünftigen materiellen Schadens (II.), Auskunft in beschränktem Umfang (IV.) sowie Zahlung außergerichtlicher Rechtsanwaltskosten nebst Zinsen (V.). Hinsichtlich weitergehender Ansprüche, insbesondere seines Unterlassungsbegehrens (III.) ist die Klage abzuweisen.

I. Klageantrag Ziffer 1 (immaterieller Schaden)

Der Kläger hat gegen die Beklagte gemäß Art. 82 Abs. 1 DS-GVO Anspruch auf immateriellen Schadenersatz in Höhe von 250,00 € aufgrund der Verletzung von Vorschriften der DS-GVO.

1. Der zeitliche Anwendungsbereich der DS-GVO ist nach Art. 99 Abs. 2 DS-GVO eröffnet, weil sich nach dem unbestrittenen Vortrag der klagenden Partei der streitgegenständliche Vorfall im Jahre 2019 ereignete. Auch ist die DS-GVO räumlich (Art. 3 Abs. 1 DS-GVO) und sachlich anwendbar (Art. 2 Abs. 1 DS-GVO).

2. Gemäß Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen. Gemäß § 82 Abs. 3 DSGVO wird der Verantwortliche von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Die Beklagte hat als Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO gegen mehrere Vorschriften der DS-GVO verstoßen (a)). Sie hat sich nicht exkulpieren können (b)). Dem Kläger ist ein - kausal auf die Verstöße zurückzuführender – immaterieller Schaden entstanden (c)), der auf 250,00 € beziffert wird (d)).

a) Verstöße gegen die DS-GVO

Der Maßstab für Verstöße gegen die DS-GVO im Sinne des Art. 82 Abs. 1 DS-GVO ist weit zu fassen. Es kommen materielle wie formelle Verstöße in Betracht. Auch ist nicht allein auf die Datenverarbeitung abzustellen, sondern sämtliche Maßnahmen, so auch Vorbereitungsmaßnahmen, können einen entsprechenden Anspruch begründen (OLG Köln, Urteil vom 14. Juli 2022 – I-15 U 137/21 –, Rn. 24, juris; BeckOK DatenschutzR/Quaas, 43. Ed. 1.2.2023, DS-GVO Art. 82 Rn. 14; ähnl. auch Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Artikel 82 Haftung und Recht auf Schadenersatz, Rn. 5; Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 23; Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 8; EuArbRK/Franzen, 4. Aufl. 2022, VO (EU) 2016/679 Art. 82 Rn. 10; a.A. – für ein engeres Verständnis - Ehmann/Selmayr/Nemitz, 2. Aufl. 2018, DS-GVO Art. 82 Rn. 8; Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 82 Rn. 7). Dies ergibt sich aus dem Wortlaut des Art. 82 Abs. 1 DG-SVO selbst, der allgemein von „Verstoß gegen die DS-GVO“ spricht und damit jeglichen Verstoß einschließt. Etwas Anderes folgt nicht etwa aus Erwägungsgrund 146 S. 1. Soweit dort von Schäden, die einer Person aufgrund einer Verarbeitung (Hervorhebung hier) entstehen, die mit dieser Verordnung nicht im Einklang steht, die Rede ist, ist dies nicht etwa dahingehend aufzufassen, dass nur Verstöße bei der Verarbeitung von Daten im engeren Sinne gemeint sind. Dies widerspräche dem in Art. 1 Abs. 2 DS-GVO postulierten Ziel der Verordnung, die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten zu schützen. Vielmehr bezieht sich die gesamte DS-GVO auf die Verarbeitung von Daten und stellt Regeln auf, die bei der dem sachlichen Anwendungsbereich gemäß Art. 2 unterfallenden Datenverarbeitung einzuhalten sind.

Eine Begrenzung erfolgt im Rahmen der Kausalität (BeckOK, ebenda).

1) Art. 13 DS-GVO (Informationspflicht) und Art. 6 DS-GVO (Rechtmäßigkeit der Verarbeitung)

Die Beklagte hat gegen die gemäß Art. 13 Abs. 1 c) DS-GVO bestehende Informationspflicht bei Erhebung von personenbezogenen Daten verstoßen, indem sie den Kläger bei der Anmeldung auf der Facebook-Plattform nicht ausreichend über die Zwecke, für die seine Telefonnummer verwendet werden sollte, informiert hat (vgl. (a)). Mangels hinreichender Information erfolge die Verarbeitung der Telefonnummer auch nicht rechtmäßig (vgl. (b)). Keine Verletzung der Informationspflicht ist – entgegen dem Verständnis des Klägers – hingegen in der mangelnden Aufklärung über die Möglichkeit missbräuchlichen Abgreifens von Daten (vgl. (c)).

(a) Art. 13 Abs. 1 c) DSGVO verlangt bei der Erhebung personenbezogener Daten bei der betroffenen Person, dass der Verantwortliche der Person zum Zeitpunkt der Erhebung der Daten die Zwecke mitteilt, für die die personenbezogenen Daten verarbeitet werden sollen. Dabei sind alle Zwecke anzugeben, welche die verantwortliche Stelle im Zeitpunkt der Erhebung verfolgt (Gola/Heckmann/Franck, 3. Aufl. 2022, DS-GVO Art. 13 Rn. 12). Die Informationspflicht aus Art. 13 DS-GVO soll die betroffenen Personen von Beginn an in die Lage versetzen, bestimmen und einschätzen zu können, wer was wann über sie weiß (Sydow/Marsch DS-GVO/BDSG/Ingold, 3. Aufl. 2022, DS GVO Art. 13 Rn. 8). Nach ihrem Zweck müssen die Informationspflichten (ggf. unmittelbar) vor Beginn der Datenerhebung erfüllt werden. Denn die Informationen sollen der betroffenen Person auch ermöglichen, darüber zu entscheiden, ob sie in die Verarbeitung ihrer Daten einwilligt bzw. ob sie hiergegen Einwände erhebt. Dieser Zweck würde bei einer Information nach Beginn der Datenerhebung verfehlt oder zumindest beeinträchtigt. Ausreichend ist es beispielsweise, wenn die Daten mittels eines Formulars erhoben werden, auf dem sich auch die gebotenen Informationen finden (Kühling/Buchner/Bäcker, 3. Aufl. 2020, DS-GVO Art. 13 Rn. 56).

Dem ist die Beklagte nicht hinreichend nachgekommen. Zwar weist die Registrierungsseite von Facebook auf die – verlinkte – Datenrichtlinie hin. Dort wird der Kläger jedoch nicht darüber aufgeklärt, dass und wie seine Telefonnummer im Rahmen des Einsatzes des CIT verwendet wird. Insbesondere wird ihm nicht verdeutlicht, dass die Telefonnummer ohne Veränderungen der Einstellungen angesichts der Standardvoreinstellung für die Suchbarkeit über die Telefonnummer auf „für alle“ bereits mit deren Angabe genutzt werden kann, um den Kläger auf Facebook und insbesondere auch über das CIT zu finden. Dazu hätte dem Kläger erläutert müssen, dass die Verwendung des CIT der Messenger App es anderen Benutzern ermöglicht, mittels Abgleiches von in deren Smartphone gespeicherter Telefonkontakte mit der Mobilfunknummer des Klägers im Falle eines „Treffers“ dessen Benutzerprofil als „Freund“ hinzufügen und auf die entsprechenden Daten zuzugreifen.

Weder der mit der Anlage B9 überreichten und im Zeitraum bis 19.04.2018 geltenden Datenrichtlinie noch der Version vom 19.04.2018 (Anl. B20) lassen sich Hinweise auf die Verwendung der Mobilfunknummer für konkret diese Zwecke entnehmen.

Soweit die Beklagte hingegen meint, in der Datenrichtlinie vom 19.04.2018 hinreichend darüber informiert zu haben, dass öffentlich einsehbare Informationen von Dritten auch außerhalb der Facebook-Plattform veröffentlicht werden können, findet sich darin jedenfalls kein Hinweis auf die mögliche Verknüpfung von Telefonnummern mit dem Nutzerprofil über das CIT:

„Du solltest dir gut überlegen, mit wem du Inhalte teilst, da die Personen, die deine Aktivität auf unse-

ren Produkten sehen können, die Inhalte mit anderen auf und außerhalb von unseren Produkten teilen können, einschließlich Personen und Unternehmen, die nicht zu der Zielgruppe gehören, mit der du die Inhalte geteilt hast. Wenn du zum Beispiel einen Beitrag teilst oder eine Nachricht an bestimmte Freunde/Freundinnen oder Konten sendest, können sie diesen Inhalt herunterladen, einen Screenshot davon anfertigen oder ihn erneut mit anderen auf oder außerhalb von unseren Produkten, in persönlichen Erlebnissen oder solchen der virtuellen Realität wie Facebook Spaces teilen."

Auch der Hinweis auf S. 3

„Wir verwenden uns zur Verfügung stehende Informationen auch, um dir Verknüpfungen bereitzustellen und Vorschläge zu unterbreiten."

informiert allenfalls über den umgekehrten Fall, nämlich, dass dem Kläger Daten über andere vorgestellt werden, adressiert aber nicht die Möglichkeit, dass anderen mittels seiner eigenen Telefonnummer Verknüpfungen zu seinem Facebook-Profil vorgeschlagen werden.

Ohne Erfolg verweist die Beklagte auf die Hilfebereiche (Anl. B1-B8) sowie die Privatsphäretools. Abgesehen davon, dass sich auch dort keine entsprechenden Hinweise auf die Zugriffsmöglichkeit Anderer auf die Nutzerdaten über die Telefonnummer finden, ist nicht ersichtlich, dass diese Informationen unmittelbar zum Zeitpunkt der Datenerhebung zur Verfügung gestellt wurden.

(b) Da die vom Kläger gegebene Einwilligung in die Verarbeitung seiner Telefonnummer nicht ausreichend informiert erteilt wurde, weil insbesondere die Zwecke der Verarbeitung nicht transparent vermittelt wurden, verstieß diese gegen Art. 6 Abs. 1 DS-GVO (vgl. Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 7 Rn. 37). Denn keine der weiteren Voraussetzungen dieser Vorschrift für die rechtmäßige Verarbeitung ist einschlägig. Insbesondere ist die Telefonnummer nicht für die Erfüllung des Vertrages im Sinne des Art. 6 Abs. 1 b) DS-GVO erforderlich. Dies ergibt sich schon daraus, dass deren Angabe bei der Anmeldung bei Facebook nicht zwingend ist.

(c) Über die Möglichkeit des Missbrauchs der von der Beklagten bereitgestellten Tools hatte diese hingegen nicht aufzuklären. Art. 13 DS-GVO umfasst derartige Informationen nicht. Dies gilt insbesondere für Abs. 1 e). Auch wenn man unbefugte Dritte als Empfänger im Sinne dieser Vorschrift betrachtet, wofür gute Gründe sprechen (vgl. unten Ziffer IV. 1. b)), ist vom Verantwortlichen nicht zu verlangen, dass er diese zunächst nur abstrakte Möglichkeit nennt. Dies gilt zumal, als auf die ex ante Sicht des Verantwortlichen zum Zeitpunkt des Auskunftsbegehrens abzustellen ist, weshalb er nur dann zu informieren hat, wenn er zu diesem Zeitpunkt schon weiß, dass und wem gegenüber er Daten der betroffenen Person noch offenlegen wird (vgl. zu Art. 15 DS-GVO: BeckOK DatenschutzR/Schmidt-Wudy, 43. Ed. 1.2.2023, DS-GVO Art. 15 Rn. 61). Das Risiko des Missbrauchs, dem jeder ausgesetzt ist, der seine persönlichen Daten im Internet preisgibt, ist im Übrigen grundsätzlich hinreichend bekannt.

2) Artt. 24, 32, 5 Abs. 1 f) DS-GVO (Sicherheit der Verarbeitung)

Die Beklagte hat zudem gegen die Verpflichtung gemäß Artt. 24, 32, 5 Abs. 1 f) DS-GVO, die Sicherheit der Verarbeitung zu gewährleisten, verstoßen, indem sie keine ausreichend geeigneten technischen und organisatorischen Maßnahmen getroffen hat, um die personenbezogenen Daten des Klägers, namentlich seine Facebook-ID, seinen Vornamen und Namen, sein Geschlecht, seinen Geburts- und Wohnort sowie seinen Arbeitgeber, gegen unbefugten Zugriff zu schützen.

(a) Art. 32 Abs. 1 DS-GVO verlangt vom Verantwortlichen, 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. Gemäß Abs. 2 sind bei der Beurteilung des angemessenen Schutzniveaus insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. Das Gebot des Art. 32 DS-GVO soll insbesondere personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen davor schützen, dass Dritte diese unbefugt oder unrechtmäßig verarbeiten (Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 32 Rn. 2). Es tritt neben die Generalnorm des Art. 24 DS-GVO, der den Verantwortlichen allgemein dazu verpflichtet, die Einhaltung der Anforderungen des DS-GVO durch technische und organisatorische Maßnahmen sicherzustellen (Paal/Pauly/Martini, a.a.O., Rn. 7) und stellt eine Konkretisierung der in Art. 5 Abs. 1 f) DS-GVO normierten Datenschutzgrundsätze der Integrität und Vertraulichkeit dar (Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 1).

(b) Bei den hier in Rede stehenden persönlichen Angaben im Facebook-Profil handelt es sich zweifellos um personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO, die die Beklagte auch nach Art. 4 Nr. 2 DS-GVO verarbeitet, nämlich insbesondere erhoben, gespeichert, verknüpft und bereitgestellt, hat. Denn durch das von der Beklagten auf der Messenger-App zur Verfügung gestellte CIT ermöglichte sie Dritten, mittels den von diesen eingegebenen Telefonnummern Nutzerprofile mit deren öffentlich einsehbaren personenbezogenen Daten aufzufinden und diese mit der eingegebenen Telefonnummer zu verknüpfen. Dieses Tool konnte von jedem genutzt werden.

Die von der Beklagten zum Zeitpunkt des Scraping-Vorfalls implementierten Sicherheitsmaßnah-

men genügten nicht, um die vom Kläger zur Verfügung gestellten Daten hinreichend vor unbefugtem Zugriff zu schützen.

(1) Ziel von Art. 32 DS-GVO ist die Gewährleistung eines dem Risiko angemessenen Schutzniveaus. Es sind daher nicht alle möglichen Maßnahmen zur Gewährleistung von Datensicherheit zu ergreifen, sondern nur solche, die als verhältnismäßig anzusehen sind. Denn die DS-GVO verlangt keine Datensicherheit um jeden Preis, sondern es muss eine Abwägung zwischen Schutzzweck und Aufwand vorgenommen werden (OLG Stuttgart, Urteil vom 31. März 2021 – 9 U 34/21 –, Rn. 54, juris; Dr. Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Artikel 32 Sicherheit der Verarbeitung, Rn. 3; BeckOK DatenschutzR/Paulus, 42. Ed. 1.11.2021, DS-GVO Art. 32 Rn. 7). Dem Adressaten bleibt daher unter Berücksichtigung der in Abs. 1 vorgegebenen Abwägungskriterien ein Ermessensspielraum (Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 32 Rn. 10). Die Maßnahmen müssen umso wirksamer sein müssen, je höher die drohenden Schäden sind (Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 4).

(2) Dabei kann vorliegend dahinstehen, ob der Nutzer, hier also der Kläger, oder der Verantwortliche, hier also die Beklagte, die Darlegungs- und Beweislast für einen Verstoß gegen die genannten Vorschriften trägt (vgl. dazu OLG Stuttgart, Urteil vom 31. März 2021 – 9 U 34/21 –, Rn. 45, juris, EuArbRK/Franzen, 4. Aufl. 2022, EU (VO) 2016/679 Art. 82 Rn. 15, 16 und BeckOK DatenschutzR/Quaas, 42. Ed. 1.8.2022, DS-GVO Art. 82 Rn. 16: grds. Nutzer mit gewissen Erleichterungen; a.A. EuGH, Urteil vom 24. Februar 2022 – C-175/20 –, Rn. 77, 78, 81, juris und - diesem folgend - BVerwG, Urteil vom 2. März 2022 – 6 C 7/20 –, Rn. 47 ff., juris: Verantwortlicher unter Berufung auf Art. 5 Abs. 2 DS-GVO als Beweislastregel). Denn selbst im erstgenannten Fall obläge es der Beklagten, im Rahmen ihrer sekundären Darlegungslast vorzutragen, welche Maßnahmen sie ergriffen hat, um dem Risiko des Datenmissbrauchs entgegenzusteuern, da es sich insoweit um Sachverhalte handelt, auf die nur sie Zugriff hat (vgl. OLG Stuttgart, a.a.O. Rn. 45, juris).

(3) Vorliegend war das von der Beklagten behauptete Schutzniveau angesichts der Gefährdungslage, der Art der zu schützenden personenbezogenen Daten und der Schwere des Risikos bei einem unbefugten Zugriff auf die Daten nicht mehr von dem der Beklagten als Adressatin der nach Art. 32 Abs. 1 DS-GVO zustehenden Ermessensspielraum gedeckt.

Bei der Abwägung sind folgende Aspekte zu berücksichtigen:

Datenscraping stellte – auch in den Jahren 2018/19 – eine reale Gefahr dar. Dieses weitverbreite-

te Phänomen war damals auch der Beklagten bereits bekannt. Dies zeigt schon der Umstand, dass sie das Sammeln von Daten mit automatisierten Tools in den Nutzungsbedingungen von Facebook untersagte. In ihrer Mitteilung „Die Fakten zu Medienberichten über Facebook-Daten“ vom 06.04.2021 (Anl. B10) bezeichnet die Beklagte Scraping zudem etwa als „gängige Taktik“ und erklärt, über die zur Beschaffung des gescrapten Datensatzes verwendeten Methoden sei bereits im Jahr 2019 berichtet worden. Die Eintrittswahrscheinlichkeit war mithin hoch, zumal ein Soziales Netzwerk wie Facebook mit Milliarden Nutzern und einem entsprechenden Umfang an persönlichen Daten auch aus Sicht der Beklagten als besonders interessantes Angriffsziel für Scraper zu bewerten sein musste.

Die damalige Konzeption des CIT ermöglichte es Dritten, mittels einer eingegebenen Telefonnummer Zugang zum Facebook-Profil und damit zu den persönlichen Daten eines Nutzers zu erhalten. Es war damit möglich, durch Eingabe einer Telefonnummer, die ohne Bezug zu einer konkreten Person zunächst lediglich eine abstrakte Zifferfolge darstellte, eine dahinterstehende Person namentlich zu identifizieren und auf deren Nutzerprofil mit weiteren persönlichen Informationen Zugriff zu nehmen.

Bei diesen persönlichen Informationen, die es zu schützen galt, handelte es sich um sensible Daten, die insbesondere in ihrer Kombination – hier etwa: Namen, Geburts- und Wohnort, Arbeitgeber und schließlich Telefonnummer – geeignet sind, den Facebook-Nutzer, etwa durch einen Identitätsdiebstahl und Phishing-Attacken, in erhebliche Schwierigkeiten mit ggfs. daraus folgenden materiellen oder immateriellen Schäden zu bringen.

(4) Die Beklagte hat zunächst bis zuletzt nicht klar verdeutlicht, zu welchem Zeitpunkt welche konkreten Maßnahmen eingesetzt wurden. Denn trotz der Betonung, mit dem „relevanten Zeitraum“ werde der Zeitraum des Scrapings adressiert, bleibt angesichts der Behauptung, die Beklagte habe ihre Maßnahmen zur Verringerung von Scraping und als Reaktion auf sich verändernde Bedrohungen fortlaufend weiterentwickelt, offen, was damit genau gemeint sei soll. Insbesondere ihre Behauptung, auch Captcha-Abfragen verwendet zu haben, ist – trotz gerichtlichen Hinweises in der mündlichen Verhandlung, dass – dies unterstellt – unklar sei, wie derartige Abfragen von den Scrapern hätten umgangen werden können – mangels diesbezüglicher Erläuterung unplausibel geblieben. Dies gilt zumal, als auch in den von der Beklagten im Frühjahr 2021 veröffentlichten Nutzermitteilungen keine Rede von einer Scraping-Prävention durch Einsatz von Captchas war.

(5) Soweit sich dem Vortrag der Beklagten im Kern entnehmen lässt, dass sie Zeitraum 2018/19

Übertragungsbegrenzungen, Bot-Erkennung sowie ein EDM-Team eingesetzt haben will, genügt dies nicht. Denn damit ließ sich ein Abgreifen der Daten nicht hinreichend verhindern, wenn dies automatisiert und verteilt auf „zahlreiche simulierte Geräte“ geschah, „um ein Überschreiten von Raten- oder Datenlimits zu vermeiden und zu versuchen, sich in die normale Nutzeraktivität einzufügen“ und die „verschiedenen simulierten Geräte werden jeweils verwendet“ wurden, „um eine Kontaktliste (die jeweils ein Segment der Telefonnummern auf der Liste der Scraper enthält) in den Kontakt-Importer … hochzuladen“ (vgl. die Schilderung des Vorgangs durch die Beklagte selbst: Anl. B11). Dass diese Gefahr bestand, war von der Beklagten auch im Vorfeld des streitgegenständlichen Scraping-Vorfalls ohne Weiteres zu erkennen.

Daher wäre es für die Beklagte beispielsweise möglich gewesen, das CIT bereits damals derart – wie später geschehen – auszugestalten, dass eine Suche nach Nutzerprofilen nicht nur anhand von Telefonnummern erfolgen kann. Das Tool hätte beispielsweise weitere Variablen, wie den von dem Nutzer in seinem Adressbuch hinterlegten Vor- oder Nachname berücksichtigen können. Angesichts dessen, dass Nutzer die Telefonnummern häufig mit dem dazugehörigen Klarnamen ihres Kontakts abspeichern, wäre der Zweck des CIT, nämlich Verknüpfungen zwischen bekannten Kontakten und deren Facebook-Profil herzustellen, allenfalls unwesentlich, angesichts der oben geschilderten Gefährdungslage aber jedenfalls in einem hinzunehmendem Umfang beeinträchtigt worden. Dies gilt auch für Captcha-Abfragen, die zwar einen zusätzlichen Schritt für den seine Kontaktdaten abgleichenden Nutzer erfordert, aber auch einen effektiven Schutz gegen automatisch generierte Abfragen geboten hätten.

Dass die beispielhaft genannten Maßnahmen die Beklagte mit einem unangemessenen finanziellen oder organisatorischen Aufwand belastet hätten, ist nicht erkennbar. Die Beklagte berief sich vielmehr nur auf die Erschwerung der Funktionalität ihres sozialen Netzwerkes.

Etwaige Maßnahmen wie Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren, die erst in Reaktion auf einen konkreten Vorfall getroffen werden, vermögen diesen nicht mehr zu beseitigen und stellen keine nennenswerte präventive Maßnahme gegenüber zukünftigen Scrapern dar. Soweit die Suche von Nutzern anhand der Telefonnummer in der Facebook-Suchfunktion im April 2018 deaktiviert wurde, betraf dies nicht die Suche über das CIT.

Die Beklagte sorgte nach alledem nicht für ein angemessenes Schutzniveau.

3) Art. 25 Abs. 2 DS-GVO („*privacy by default*“)

Die Beklagte hat überdies gegen in Art. 25 Abs. 2 DS-GVO das Gebot, Datenschutz durch daten-

schutzfreundliche Voreinstellungen zu gewährleisten, verstoßen, indem sie standardmäßig die Suchbarkeit der Nutzer über deren Telefonnummer „für alle“ voreingestellt hat.

(a) Ein Verstoß gegen diese Vorschrift kann zu einem Schadenersatzanspruch im Sinne des Art. 82 DS-GVO führen. Das Gericht teilt – wie dem oben unter B. I. 2 a) Gesagten bereits erkennbar – nicht die gegenteilige Ansicht, der zufolge es sich in erster Linie um eine organisatorische Verpflichtung handelt (so Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DS-GVO Art. 25 Rn. 34). Vielmehr kann aus der Verletzung der sich aus Art. 25 DS-GVO ergebenden Pflichten eine Erhöhung der Gefahr eines Schadens resultieren (Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 25 Rn. 77).

(b) Art. 25 Abs. 2 DS-GVO verlangt vom Verantwortlichen geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden, und gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit (S. 1 u. 2). Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden (S. 3).

Gerade der letzte Satz zielt vor allem auf die Privatsphäre-Einstellungen der sozialen Netzwerke ab. Bei der Registrierung soll dem Betroffenen nämlich gewährleistet werden, dass er nur in eine solche Verarbeitung einwilligt, die die Veröffentlichung seiner Daten ohne sein Eingreifen kategorisch ausschließt (Spindler/Schuster/Spindler/Horváth, 4. Aufl. 2019, DS-GVO Art. 25 Rn. 12). Der Betreiber eines sozialen Netzwerks soll damit verpflichtet werden, die Default-Einstellungen so zu treffen, dass Inhalte der Nutzer nicht standardmäßig mit anderen Nutzern oder Dritten geteilt werden (Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DS-GVO Art. 25 Rn. 20). Als Voreinstellung ist daher der kleinstmögliche Empfängerkreis vorzusehen (Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DS-GVO Art. 25 Rn. 31).

(c) Gegen diese Anforderungen hat die Beklagte als Verantwortliche verstoßen. Die Suchbarkeit war im Zeitraum des vorgefallenen Scrapings standardmäßig so voreingestellt, dass der Facebook-Nutzer, der seine Telefonnummer angab, automatisch mitsamt seinem öffentlichen Nutzerprofil von jedermann über die Telefonnummer gefunden werden konnte. Dies galt auch für die Suche über das CIT. Eine andere, einschränkende Einstellung in seinem Privatsphärebereich erforderte ein Aktivwerden des Nutzers.

Der von der Beklagten genannte Zweck von Facebook, Menschen die Möglichkeit zu geben, Gemeinschaften zu bilden, und die Welt näher zusammenzubringen, erfordert die Standardeinstellung der Suchbarkeit mittels der Telefonnummer für alle nicht. Denn Personen, die bereits über die Telefonnummer eines anderen Nutzers verfügen, können mit diesem ohne Weiteres telefonisch in Kontakt treten, um sich ggfs. anschließend auf der Facebook-Plattform miteinander zu vernetzen. Die Beklagte bestätigt dies selbst teilweise, indem sie angibt, sie habe festgestellt, dass es für legitime Nutzer üblicher sei, die Suche anderer Nutzer anhand des Namens als anhand der Telefonnummer vorzunehmen, weshalb sie die Facebook-Suchfunktion im April 2018 deaktiviert habe. Gleichwohl ist nicht erkennbar, dass das Netzwerk nicht mehr oder nur noch eingeschränkt funktioniert hätte.

b) Keine Exkulpation gemäß Art. 82 Abs. 3 DS-GVO

Der Beklagten kann sich nicht gemäß Art. 82 Abs. 3 DS-GVO, der das Verschulden widerleglich vermutet, exkulpieren.

1) Soweit in der Vorschrift von der Verantwortlichkeit für den Schaden die Rede ist, ist dies im Sinne von Verschulden aufzufassen (wohl h.M.: vgl. OLG Stuttgart, Urteil vom 31. März 2021 – 9 U 34/21 –, Rn. 45, 51, juris; BeckOK DatenschutzR/Quaas, 42. Ed. 1.8.2022, DS-GVO Art. 82 Rn. 17.2; Ehmann/Selmayr/Nemitz, 2. Aufl. 2018, DS-GVO Art. 82 Rn. 14; Gola/Heckmann/Gola/Piltz, 3. Aufl. 2022, DS-GVO Art. 82 Rn. 24; Spindler/Schuster/Spindler/Horváth, 4. Aufl. 2019, DS-GVO Art. 82 Rn. 11; a.A. Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 82 Rn. 19: fehlendes Verschulden für Entlastung nicht ausreichend). Art. 82 Abs. 3 DS-GVO ordnet eine Beweislastumkehr hinsichtlich des Verschuldens an (Oberster Gerichtshof Wien, Urteil vom 27. November 2019 – 6 Ob 217/19h –, juris). Der Anspruchsverpflichtete kann sich daher nur entlasten, indem er beweist, dass er die am Maßstab des Stands der Technik und im Verkehr, d.h. am allgemeinen Schutzinteresse orientierte erforderliche Sorgfalt im Sinne von § 276 Abs. 2 BGB angewendet hat (BeckOK DatenschutzR/Quaas, 42. Ed. 1.8.2022, DS-GVO Art. 82 Rn. 18).

2) Die Beklagte hat keinerlei Umstände angeführt, die sie hinsichtlich der unzureichend erteilten Informationen in Bezug auf die Verarbeitung der Telefonnummer, die fehlenden Sicherheitsmaßnahmen zur Vermeidung des automatisierten Abgreifens von Daten über das CIT mittels Telefonnummern und die datenschutzunfreundliche Standardeinstellung bei der Suchbarkeit über die Telefonnummer entlasten könnte.

c) Schaden

Dem Kläger ist durch die Verstöße der Beklagten gegen die genannten Vorschriften DS-GVO ein immaterieller Schaden im Sinne des Art. 82 Abs. 1 DS-GVO entstanden.

1) Der Begriff des Schadens ist gemäß Erwägungsgrund 146 S. 3 DS-GVO weit auf eine Art und Weise auszulegen, die den Zielen dieser Verordnung in vollem Umfang entspricht.

Allerdings ist er nicht mit der zugrundeliegenden Rechtsgutsverletzung gleichzusetzen; der bloße Verstoß gegen Bestimmungen der DS-GVO reicht daher nicht aus (vgl. OLG Frankfurt a. M. Urt. v. 2.3.2022 – 13 U 206/20, GRUR-RS 2022, 4491 Rn. 62, beck-online; Schlussanträge des Generalanwalts vom 06.10.2022, C-300/21, Celex-Nr. 62021CC0300; BeckOK DatenschutzR/Quaas, 43. Ed. 1.2.2023, DS-GVO Art. 82 Rn. 23; Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Artikel 82 Haftung und Recht auf Schadenersatz, Rn. 5; so aber BAG, EuGH-Vorlage vom 26. August 2021 – 8 AZR 253/20 (A) –, Rn. 33, juris). Dies verbietet schon der Wortlaut des Art. 82 Abs. 1 DS-GVO sowie des Erwägungsgrundes 146 DS-GVO, wonach ein Schaden „entstanden“ bzw. „erlitten“ sein muss. Überdies wäre auch die Differenzierung zwischen materiellem und immateriellem Schaden im Verordnungstext völlig überflüssig, wenn die bloße Rechtsgutsverletzung hätte ausreichen sollen. Schließlich führte der Verzicht auf einen Schaden als Tatbestandsmerkmal zu einem Ausufern von Ersatzforderungen, weil Betroffene dann auch in Fällen völlig folgenloser Datenschutzverstöße Ersatz begehren könnten (vgl. OLG Frankfurt a. M., a.a.O., Rn. 64).

Allerdings können auch Bagatellschäden eine Ersatzpflicht hervorrufen. Denn eine Erheblichkeitsschwelle ist weder Art. 82 DS-GVO noch den Erwägungsgründen zu entnehmen. Erwägungsgrund 148 S. 2 sieht lediglich vor, dass (ausnahmsweise) bei geringfügigen Verstößen auf die Verhängung einer Geldbuße verzichtet werden kann (LAG BW, ZD 2021, 436 Rn. 82, beck-online; OLG Frankfurt a. M., a.a.O., Rn. 63; a.A. Hans-Jürgen Schaffland; Gabriele Holthaus, a.a.O., Rn. 13). Die Schwere eines Schadens wirkt sich nur im Rahmen der Festlegung der Schadenshöhe aus.

Deshalb kann ein Schaden auch bereits in einem unguten Gefühl, in der Angst und Besorgnis liegen, dass personenbezogene Daten Unbefugten bekannt geworden sind, wenn die Gefahr besteht, dass die Daten unbefugt weiterverwendet werden (vgl. Landesarbeitsgericht Baden-Württemberg, Urteil vom 25. Februar 2021 – 17 Sa 37/20 –, Rn. 96, juris). So führen die Erwägungsgründe 75 und 85 als möglichen Schaden unter anderem den Verlust, die personenbezogenen

Daten kontrollieren zu können, auf. Das Gericht schließt sich dabei dem Verständnis des Generalanwaltes im Verfahren UI gegen Österreichische Post AG der Bedeutung des erwähnten Kontrollverlustes an. Danach verursacht der Verlust über die Kontrolle der Daten nicht zwangsläufig einen Schaden. Vielmehr adressiert die Erwähnung des Kontrollverlustes in den Erwägungsgründen – in sprachlicher Unschärfe - die möglichen Folgen dieses Verlusts wie etwa Angst oder Besorgnis, was mit den Daten geschehen könnte (vgl. Schlussanträge des Generalanwalts vom 06.10.2022, C-300/21, Celex-Nr. 62021CC0300, Rn. 62 u. Fn. 43).

2) Im streitgegenständlichen Fall trat der immaterielle Schaden durch die aufgrund des Scrapings beim Kläger nachvollziehbar ausgelöste Besorgnis bezüglich des weiteren Schicksals seiner persönlichen Daten ein, die damit - als ein mit seiner Telefonnummer verknüpfter Datensatz - im Netz kursierten. Denn dadurch erlitt der Kläger einen Kontrollverlust über diese Daten, der vorliegend mit dem subjektiv besorgniserregenden Risiko einherging, dass diese Daten etwa durch Identitätsdiebstahl unbefugt und für den Kläger schadensträchtig genutzt werden.

Soweit die Beklagte meint, ein Schaden könne schon deshalb nicht entstanden sein, weil es keinen Schutz vor der (erneuten) Veröffentlichung bereits öffentlicher Daten gebe, verfängt dies nicht. Denn gerade die Verknüpfung der gescrapten Daten mit der Telefonnummer des Klägers in einem Datensatz, führt zu einer höheren Dimension des Kontrollverlustes des Klägers hinsichtlich seiner Daten. Dabei spielt es insbesondere keine Rolle, dass die Scraper überhaupt erst durch Eingabe einer Telefonnummer zu einem „Match“ mit einem Facebook-Profil kamen und daher diese demnach nicht originär dem Profil entnahmen.

Dabei ist die Kammer überzeugt davon, dass von den Tätern nicht nur die von Beklagtenseite eingeräumten Daten (NutzerID, Vorname, Land und Geschlecht) erlangt wurden, sondern auch Name, Geburts- und Wohnort sowie Arbeitgeber. Wie die Beklagte dazu kommt, dass nur der Vorname veröffentlicht worden sei, ist unklar, trägt sie doch selbst vor, dass zu den immer öffentlichen Daten auch der Name gehöre.

Der Kläger hat mittels Kopie in einem Schriftsatz einen Datenauszug (vgl. AS 172) vorgelegt, der diese Daten gemeinsam mit der Telefonnummer, der NutzerID und dem Vornamen des Klägers enthält, und von dem er behauptet, er sei aus einer Datenbank im Darknet abgerufen. Das Gericht zweifelt angesichts der Angaben des Klägers in seiner persönlichen Anhörung nicht daran, dass es sich um einen authentischen Auszug handelt und dieser aus dem Scraping-Vorfall stammt. Der Kläger hat in seiner persönlichen Anhörung angegeben, er habe bei der Anmeldung – neben dem zwangsläufig Erforderlichen – Geburtsort und Wohnort eingetragen und auch auf

„öffentlich“ gestellt, um über diese Angaben von etwaigen Namensvettern unterscheidbar zu sein. Hinsichtlich des Arbeitgebers, den er auch eingetragen habe, war er sich nicht mehr sicher, ob er diese Angabe auch auf „öffentlich“ gestellt habe. Zweifel an der Richtigkeit dieser Erklärung hegt das Gericht nicht, denn der Kläger vermittelte einen glaubwürdigen Eindruck, seine Angaben waren glaubhaft. Er äußerte sich offen und vermittelte nicht den Eindruck, dass seine Aussagen etwa prozesstaktisch motiviert wären. Unsicherheiten in seiner Erinnerung offenbarte er. Die vom Kläger angegebenen Daten korrelieren mit jenen im Datensatz. Anhaltspunkte dafür, dass der Kläger diesen selbst erstellt hätte, sind nicht ersichtlich. Dass dieser Datensatz aus dem streitgegenständlichen Scraping-Vorfall stammt, ergibt sich für das Gericht aus dem Umstand, dass die auf der von der Beklagten vorgelegten Anl. B17 befindliche NutzerID mit der nach der Telefonnummer befindlichen zweiten Nummer auf dem Datensatz übereinstimmt.

Die vom Kläger in seiner Anhörung geschilderte gewisse Zunahme von Spam- und Phishing-SMS sowie -WhatsApp-Nachrichten und Anrufe von unbekannten Nummern ist vorliegend nicht geeignet, den immateriellen Schaden zu begründen. Denn dass dies ein wirklich störendes Ausmaß angenommen hätte oder dem Kläger dadurch ein besonderer Aufwand entstanden wäre, um sich vor solchen Kontaktaufnahmeversuchen zu schützen, ist weder von ihm geschildert, noch sonst erkennbar. Es kommt daher nicht darauf an, dass den Angaben des Klägers auch eine zeitliche Korrelation mit dem Scraping-Vorfall nicht mit einer hinreichenden Sicherheit zu entnehmen ist.

d) Die erforderliche Kausalität zwischen den Verstößen der Beklagten gegen die DS-GVO und dem Schaden des Klägers liegt vor. Wäre der Kläger ohne Verstoß gegen die Informationspflichten nach Art. 13 Abs. 1 c) DS-GVO ordnungsgemäß darüber aufgeklärt worden, dass seine Telefonnummer, die er in der Zielgruppenauswahl als nicht öffentlich eingestellt hatte, im Rahmen des Einsatzes des CIT ohne Veränderungen der Einstellungen angesichts der Standardvoreinstellung für die Suchbarkeit über die Telefonnummer auf „für alle“ dazu verwendet wird, um ihn auf Facebook zu finden, hätte er seine Telefonnummer nicht eingetragen oder die Standardeinstellungen verändert. Denn aus seiner persönlichen Anhörung ergibt sich deutlich, dass er über seine Telefonnummer nicht gefunden werden wollte. Entsprechend hat auch die gegen Art. 25 Abs. 2 DS-GVO verstoßende datenschutzunfreundliche Standardvoreinstellung der Suchbarkeit über die Telefonnummer auf „für alle“ zur Schadensentstehung beigetragen. Schließlich ist der Schaden auch kausal auf den Verstoß der Beklagten gegen Artt. 24, 32, 5 Abs. 1 f) DS-GVO zurückzuführen, denn durch die unzureichenden Schutzmaßnahmen ermöglichte die Beklagte das missbräuchliche Abgreifen der Daten des Klägers.

Dass die gescrapten Daten seitens des Klägers selbst in der Zielgruppeneinstellung als öffentlich

einsehbar seinen Profildaten hinzugefügt wurden, entlastet die Beklagte in keiner Weise. Denn der Zugang dazu durch unbekannte Dritte wurde erst mittels der Telefonnummer aufgrund des Zusammenwirkens von ungenügenden Sicherungsmaßnahmen, ungenügender Information und datenschutzunfreundlicher Voreinstellung ermöglicht.

e) Etwaige weitere Verstöße

Soweit sich der Kläger auf die Verletzung der Meldepflicht nach Art. 33 DS-GVO gegenüber der zuständigen Aufsichtsbehörde sowie der Pflicht zur Benachrichtigung der betroffenen Person nach Art. 34 DS-GVO beruft, sind zwar auch derartige Verstöße nach dem oben Gesagten (B. I. 2. a)) grundsätzlich geeignet, Schadenersatzansprüche auszulösen. Vorliegend kann die Verletzung der genannten Gebote indes dahinstehen, da ein daraus resultierender Schaden für den Kläger nicht erkennbar ist. Soweit der Kläger vortragen lässt, durch einen auf mangelnder Unterrichtung beruhenden Zeitraum der Ungewissheit hätten sich die Risiken, dass die Daten unbemerkt missbraucht würden, und damit das Unwohlsein und die Sorgen des Klägers entschieden gesteigert, und bei zügiger Benachrichtigung hätten zeitnah Schritte zur Risikominimierung und Absicherung eingeleitet werden können, um einen Schaden zu vermeiden, verrät diese floskelhafte Behauptung nicht, welche Schritte hätten eingeleitet werden sollen. Dies gilt zumal, da der Kläger in seiner persönlichen Anhörung angegeben hat, er habe nach Kenntnis vom Vorfall weder Suchbarkeitseinstellungen noch E-Mail-Adresse oder Telefonnummer geändert, da der Vorfall ja schon geschehen gewesen sei.

Nicht anderes gilt für einen etwaigen Verstoß gegen die Auskunftsverpflichtung.

f) Höhe des immateriellen Schadens

Der Kläger hat Anspruch auf Zahlung eines immateriellen Schadenersatzes in Höhe von lediglich 250,00 €.

1) Bei der Bestimmung des vom Kläger in das Ermessen des Gerichts gestellten Höhe des Schadenersatzes gemäß § 287 Abs. 1 S. 1 ZPO sind alle Umstände des Einzelfalls zu würdigen (vgl. BAG, Urteil vom 5. Mai 2022 – 2 AZR 363/21 –, Rn. 12 f., juris). Die Kriterien des Art. 83 Abs. 2 DS-GVO, die Anhaltspunkte für die Höhe der von der Aufsichtsbehörde zu verhängenden Geldbuße geben sollen, können auch für die Bemessung des immateriellen Schadenersatzes herangezogen werden (vgl. Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Artikel 82 Haftung und Recht auf Schadenersatz, Rn. 10; Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18d;

BeckOK DatenschutzR/Quaas, 43. Ed. 1.2.2023, DS-GVO Art. 82 Rn. 31). Danach sind unter anderem Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der Verarbeitung, der Grad des Verschuldens, Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens sowie die Kategorien der personenbezogenen Daten zu betrachten. Gemäß Erwägungsgrund 146 S. 6 DS-GVO sollen die betroffenen Personen einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten. Schadensersatzforderungen sollen abschrecken und weitere Verstöße unattraktiv machen (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 17; Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 10).

2) Im streitgegenständlichen Fall hält das Gericht unter Berücksichtigung der Ausgleichs- und Genugtuungsfunktion sowie der generalpräventiven Funktion des immateriellen Schadenersatzes einen Betrag in Höhe von 250,00 € erforderlich, aber auch ausreichend.

Dabei fließt anspruchserhöhend ein, dass der Beklagten mehrere schadensursächliche Verstöße gegen die DS-GVO zur Last zu legen sind, wobei die den Zweck von Facebook fördernde Art der Datenerhebung die Regeln der DS-GVO nicht nur im Einzelfall, sondern systematisch und über einen längeren Zeitraum missachtet hat. Anspruchsmindernd ist zu berücksichtigen, dass der Kläger durch das Ausspähen seiner Daten in seiner Lebensführung nur wenig beeinträchtigt wurde und sich seine Sorge ersichtlich derart in Grenzen gehalten hat, dass er im Rahmen seiner persönlichen Abwägung von Vor- und Nachteilen davon abgesehen hat, seinen Facebook-Account aufzulösen, die dortigen Einstellungen zu seinem Schutz abzuändern oder seine Telefonnummer zu wechseln. Bei den gescrapten Daten handelt es sich zudem nicht um besonders sensible Informationen wie Gesundheits- oder Kontodaten.

3. Der Zinsausspruch folgt aus §§ 288, 291, 187 Abs. 1 BGB. Zwar gelangte der Auslandsrückschein als Nachweis der Zustellung an die Beklagte nicht wieder zur Akte. Allerdings erfolgte die Zustellung der Klageschrift an die Beklagte spätestens am 06.07.2022. An diesem Tag verfasste der von der Beklagten mandatierte Prozessbevollmächtigte die Verteidigungsanzeige.

ll. Feststellungsanspruch

Der Feststellungsantrag ist begründet. Der Kläger hat gemäß Art. 82 DS-GVO auch Anspruch auf Feststellung der Ersatzpflicht der Beklagten für materielle Schäden, die aus dem von der Beklagten nach dem Gesagten mitzuverantwortenden Scraping-Vorfall gegebenenfalls entstanden sind oder noch entstehen werden.

1. Ein zulässiger Feststellungsantrag ist begründet, wenn die sachlichen und rechtlichen Voraussetzungen eines Schadensersatzanspruchs vorliegen, also ein haftungsrechtlich relevanter Eingriff gegeben ist, der zu möglichen künftigen Schäden führen kann. Eine darüber hinaus gehende gewisse Wahrscheinlichkeit des Schadenseintritts ist nach hier vertretener Auffassung nicht zu verlangen (so auch OLG Stuttgart, Urteil vom 21. Juni 2018 – 13 U 18/18 –, Rn. 46, juris an der Erforderlichkeit eines solchen zusätzlichen Begründungselementes zweifelnd: BGH, Urteil vom 16. Januar 2001 – VI ZR 381/99 –, Rn. 8, juris; Beschluss vom 9. Januar 2007 – VI ZR 133/06 –, Rn. 6, juris).

2. Dass der Scraping-Vorfall möglicherweise zu materiellen Schäden beim Kläger führen kann, steht angesichts dessen, dass nicht bekannt ist, wer Zugriff auf dessen Datensatz hat, für das Gericht außer Zweifel.

III. Unterlassung

Der mit Klageantrag Ziffer 3 a) verfolgte zulässige Unterlassungsanspruch ist unbegründet.

1. Zwar sind Unterlassungsansprüche auch unter Geltung der DS-GVO – anders als die Beklagte meint – nicht durch deren Vorrang ausgeschlossen. Soweit die DSGVO als solche keinen gesonderten Anspruch auf eine Unterlassung vorsieht, wird der Unterlassungsanspruch teilweise direkt auf Art. 17 Abs. 1 d) DSGVO (BGH, Urteil vom 13. Dezember 2022 – VI ZR 60/21 –, Rn. 10, juris; Urteil vom 27. Juli 2020 – VI ZR 405/18 –, BGHZ 226, 285-310, Rn. 20), teilweise auf § 823 Abs. 2 BGB, § 1004 BGB analog (OLG München, Urteil vom 19. Januar 2021 – 18 U 7243/19 –, Rn. 62, juris) gestützt. Eine Entscheidung kann hier dahinstehen, da – unabhängig von der Anspruchsgrundlage – zumindest Einigkeit über die Möglichkeit der Geltendmachung eines weitergehenden Unterlassungsanspruchs herrscht (vgl. Dr. Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Artikel 79 Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter, Rn. 1; Spindler/Schuster/Spindler/Dalby, 4. Aufl. 2019, DS-GVO Art. 79 Rn. 17; Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 79 Rn. 13).

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 (vgl. OLG Frankfurt, Urteil vom 14. April 2022 – 3 U 21/20 –, Rn. 29, juris).

2. Der Kläger kann allerdings von der Beklagten nicht verlangen, dass diese es unterlässt, die Daten des Klägers Dritten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen. Denn die Beklagte trifft als Verantwortliche keine Verpflichtung, die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen.

a) Zwar folgt aus Art. 32 Abs. 1 und 2 DS-GVO, dass der Verantwortliche ein dem Risiko eines unbefugten Zugangs zu personenbezogenen Daten angemessenes Schutzniveau zu gewährleisten hat. Dabei liegt es im Ermessen des Verantwortlichen, aus der Vielzahl möglicher Maßnahmen, die das Risiko der Datenverarbeitung reduzieren können, konkrete Maßnahmen auszuwählen, durch die nach seiner Einschätzung ein angemessenes Schutzniveau erreicht wird (Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 8).

Allerdings ist wesentlich, dass nicht alle möglichen Maßnahmen zur Gewährleistung von Datensicherheit zu ergreifen sind, sondern nur solche, die unter Abwägung zwischen Schutzzweck und Aufwand unter Berücksichtigung der Arten der Daten, dem Stand der Technik und den anfallenden Kosten als verhältnismäßig anzusehen sind (vgl. Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 32 Rn. 10). Denn die DS-GVO verlangt keine Datensicherheit um jeden Preis und verpflichtet den Verantwortlichen nicht zu einem absoluten Schutz der personenbezogenen Daten; vielmehr muss das Schutzniveau dem jeweiligen Einzelfall angemessen sein, wobei Risiken nicht gänzlich ausgeschlossen werden können (Gola/Heckmann/Piltz, DSGVO 3. Aufl., Art. 32 Rn. 11; Paal/Pauly/Martini, DSGVO 3. Aufl., Art. 32 Rn. 46; Dr. Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Artikel 32 Sicherheit der Verarbeitung, Rn. 3).

b) Der Kläger kann daher lediglich ein angemessenes Schutzniveau bzw. die Unterlassung einer Datenverarbeitung ohne dieses verlangen. Darauf, dass eines der Abwägungskriterien in den Vordergrund gestellt wird, hat der Kläger ebenso wenig Anspruch wie auf konkrete Maßnahmen (vgl. dazu auch BGH, Urteil vom 22. Oktober 1976 – V ZR 36/75 –, BGHZ 67, 252-254, Rn. 11; Urteil vom 17. Dezember 1982 – V ZR 55/82 –, Rn. 17, juris, jeweils zu Unterlassungsansprüchen gegen Immissionen).

Auf diesen Aspekt hat das Gericht den Kläger in der mündlichen Verhandlung hingewiesen, ohne dass der Antrag angepasst worden wäre.

lV. Auskunft

Der auf Auskunft gerichtete Antrag des Klägers ist nur zum Teil begründet. Der Kläger kann von

der Beklagten verlangen, ihm Auskunft darüber zu erteilen, durch welche Empfänger Daten des Klägers durch Scraping erlangt wurden (1.). Der weitergehende Antrag ist abzuweisen.

1. Auskunftsanspruch bzgl. Scraper

Der Kläger hat gegen die Beklagte – unter Berücksichtigung einer interessengerechten Auslegung (a)) des Antrages – Anspruch auf Mitteilung der Empfänger der durch Scraping erlangten Daten des Klägers (b)). Dieser Anspruch ist noch nicht erfüllt (c)).

a) Soweit der Kläger den Antrag dahingehend formuliert hat, dass die Daten „…*durch Scraping oder durch Anwendung des Kontaktimporttools…*“ erlangt werden konnten, ist damit ersichtlich der den Kläger betreffenden Scraping-Vorfall im Jahr 2019 adressiert. Die sachgerechte Auslegung des Antrags ergibt, dass der Kläger nicht etwa Auskunft über diejenigen Nutzer des Kontaktimporttools erlangen möchte, die sich im Rahmen der Nutzungsbedingungen der Beklagten gehalten haben.

b) Der Anspruch auf Mitteilung der Scraper resultiert aus Art. 15 Abs. 1 c) DS-GVO und Art. 33 Abs. 2 DS-GVO.

Gemäß Art. 15 Abs. 1 c) DS-GVO hat der Betroffene insbesondere das Recht auf Information zu den Empfängern, denen gegenüber personenbezogene Daten offengelegt wurden. Art. 34 Abs. 2 DS-GVO statuiert die Pflicht des Verantwortlichen nach einer Verletzung des Schutzes personenbezogener Daten mit einem voraussichtlich hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen, die betroffene Person über die „Art der Verletzung des Schutzes personenbezogener Daten“ zu informieren. Die Voraussetzungen dieser Vorschrift sind erfüllt. Insbesondere ist von einem hohen Risiko auszugehen. Dies ist etwa anzunehmen, wenn ein Kontrollverlust der betroffenen Person im Hinblick auf ihre personenbezogenen Daten eingetreten ist (vgl. Erwägungsgrund 85; so auch Gola/Heckmann/Reif, a.a.O., Art. 34 Rn. 8). Das ist hier – nach dem oben Gesagten – der Fall.

Beide Vorschriften sind so zu verstehen, dass dem von einem unbefugten Zugriff auf seine Daten Betroffenen vom Verantwortlichen, soweit diesem bekannt, auch die Identität des unbefugt Zugreifenden mitzuteilen ist.

Der Wortlaut der Regelungen lässt dies zu. Als Empfänger im Sinne des Art. 15 Abs. 1 c) DS-GVO, dem gegenüber Daten offengelegt wurden, kann zwanglos auch noch derjenige verstanden werden, der diese unbefugt erhalten hat. Auch der Begriff „Offenlegen“ umfasst die unbe-

absichtigte Preisgabe (vgl. auch die engl. Fassung: „…*the recipients or categories of recipient to whom the personal data have been or will be disclosed.*", wobei „*disclosed*" ebenfalls das unbeabsichtigte Enthüllen einschließt). Auch die in Art. 34 Abs. 2 DS-GVO bezeichnete „Art der Verletzung des Schutzes personenbezogener Daten" schließt, wenn bekannt, die Auskunft darüber ein, wer sich nun – unbefugt – im Besitz dieser Daten befindet.

Sinn und Zweck der Auskunfts- und Informationsrechte legen eine weite Auslegung nahe. Gerade unter dem Gesichtspunkt der in der DS-GVO mehrfach betonten Transparenz sowie der Kontrolle der Betroffenen über ihre eigenen Daten wäre es widersinnig, einen solchen Anspruch zu verneinen. Denn erst mit der Kenntnis der unbefugten Dritten wird der Betroffene in die Lage versetzt, diesen gegenüber Ansprüche, wie etwa das Recht auf Löschung gemäß Art. 17 DS-GVO, effektiv geltend zu machen, und die Möglichkeit zu haben, die Kontrolle über seine Daten wiederzuerlangen (vgl. dazu auch die Schlussanträge des Generalanwalts vom 15.12.2022, C-579/21, Celex-Nr. 62021CC0579, Rn. 79 zum Interesse des Betroffenen im Falle eines unrechtmäßigen „Mitarbeiterexzesses" an der Mitteilung dessen Identität). Dementsprechend kommt es für die Beauskunftung der Empfänger nicht darauf an, ob die Offenlegung rechtmäßig erfolgte (Gola/Heckmann/Franck, 3. Aufl. 2022, DS-GVO Art. 15 Rn. 11).

Vielmehr hat der Kläger Anspruch darauf, von der Beklagten zu erfahren, wer die ihn betreffenden Daten unbefugt erlangt hat.

c) Der Anspruch ist nicht durch Erfüllung untergegangen. Dafür genügt nicht etwa der Hinweis der Beklagten in der Klageerwiderung, über die Verarbeitungstätigkeiten Dritter (hier: „Scraper"), keine Angaben machen zu können. Denn damit ist nur gesagt, dass sie nicht mitteilen kann, wie die Dritten mit den abgegriffenen Daten vorgegangen sind, ob und wo sie diese etwa gespeichert, weiterverbreitet oder verknüpft haben (vgl. Art. 4 Nr. 2 DS-GVO). Darauf richtet sich aber das Auskunftsbegehren des Klägers gar nicht. Die Beklagte hat auch nicht dahingehend Auskunft erteilt, zur Identität der Scraper keine Angaben machen zu können, womit sie den Auskunftsanspruch erfüllt hätte. Vielmehr hat sie sich trotz Hinweises des Gerichts in der mündlichen Verhandlung nicht dazu geäußert, sondern ein antragsgemäß gewährtes Schriftsatzrecht begehrt, sich zu dieser Frage jedoch nicht geäußert.

2. Auskunftsanspruch bezüglich der verarbeiteten Daten sowie des Zeitpunktes des Scrapings

Soweit der Kläger weiter „*Auskunft über die ihn betreffenden personenbezogene Daten, welche die Beklagte verarbeitet, … namentlich welche Daten zu welchem Zeitpunkt durch Scraping … erlangt werden konnten*", begehrt, ist solch ein Anspruch (a)) jedenfalls aufgrund

des Auskunftsschreibens der Prozessbevollmächtigten der Beklagten vom 25.11.2021 (Anl. B16) durch Erfüllung erloschen (b)).

a) Gemäß Art. 15 Abs. 1 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten, insbesondere die Kategorien personenbezogener Daten (Art. 15 Abs. 1 b) DS-GVO), die verarbeitet werden. Nach Maßgabe dessen konnte der Kläger von der Beklagten Auskunft über die von ihr verarbeiteten Daten verlangen.

Der Anspruch auf Mitteilung, welche Daten durch Scraping erlangt werden konnten, ergibt sich zwar nicht aus Art. 15 Abs. 1 DS-GVO, denn diese Vorschrift sieht eine entsprechende Information nicht vor. Allerdings ist Art. 34 Abs. 2 DS-GVO funktional dahingehend auszulegen, dass, soweit möglich, auch Angaben zu den von der Verletzung des Schutzes konkret betroffenen Daten bzw. Datenkategorien zu machen sind (Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 34 Rn. 22). Denn geeignete Schutzmaßnahmen der betroffenen Person dürften ohne diese Kenntnis gegebenenfalls nicht möglich sein (ebenda). Wie bereits ausgeführt (vgl. oben B. IV. 1. b)), sind die Voraussetzungen dieser Vorschrift erfüllt.

Ob Art. 34 Abs. 2 DS-GVO auch einen Anspruch auf Mitteilung des Zeitpunktes der Verletzung des Schutzes der Daten beinhaltet, kann dahinstehen.

b) Denn sämtliche der genannten Ansprüche sind jedenfalls gemäß § 362 Abs. 1 BGB durch Erfüllung erloschen.

1) Erfüllt im Sinne des § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die - gegebenenfalls konkludente - Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (BGH, Urteil vom 15. Juni 2021 – VI ZR 576/19 –, Rn. 19, juris).

2) Gemessen daran, ist der Anspruch hier sowohl im Hinblick auf die verarbeiteten personenbezogenen als auch die gescrapten Daten sowie den Zeitpunkt erfüllt.

Die Beklagte hat dem Kläger mit Schreiben vom 25.11.2021 (Anl. B16), S. 7, genau beschrieben, wie er die von ihm gespeicherten Daten auf Facebook herunterladen kann. Damit ist sie ihrer Auskunftsverpflichtung gemäß Art. 15 Abs. 1 b) DS-GVO nachgekommen. Insbesondere genügt vorliegend auch der Verweis auf die Selbstbedienungstools „*Access Your Information*“ und „*Deine Informationen herunterladen*“, mit dem sich der Kläger – passwortgeschützt – eine Kopie seiner Daten herunterladen kann. Eine weitergehende schriftliche Auskunft kann der Kläger nicht verlangen. Denn Art. 15 Abs. 3 S. 3 DS-GVO gestattet ein rein elektronisches Format. Entsprechend Erwägungsgrund 63 S. 4 sollte der Verantwortliche insoweit - je nach Möglichkeit - einen Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten gewährt. Der Fernzugang tritt gegebenenfalls alternativ neben den Anspruch auf Kopie. Ein Beharren auf Kopie-Abzug kann rechtsmissbräuchlich wirken, wenn sich die betroffene Person die Daten einfach(er) selbst besorgen kann (Gola/Heckmann/Franck, 3. Aufl. 2022, DS-GVO Art. 15 Rn. 40; Hessisches Landesarbeitsgericht, Urteil vom 29. Januar 2013 – 13 Sa 263/12 –, Rn. 107, juris). Art. 12 Abs. 1 DS-GVO stellt insoweit keine höheren Anforderungen an die Form der Auskunft: Danach trifft der Verantwortliche geeignete Maßnahmen, um der betroffenen Person unter anderem alle Mitteilungen gemäß Artikel 15 DS-GVO, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Auch dies ist mit dem Verweis auf die Möglichkeit, sich die Daten selbst herunterzuladen, erfüllt.

In dem genannten Schriftsatz hat die Beklagte dem Kläger zudem auch mitteilen lassen, über eine Kopie der gescrapten Rohdaten zwar nicht zu verfügen, aber auf der Grundlage der bisherigen Analysen von im Einzelnen genannten durch Scraping abgerufenen Datenkategorien auszugehen. Damit hat die Beklagte zu erkennen gegeben, insoweit keine weiteren Auskünfte erteilen zu können. Ungeachtet einer etwaigen Unrichtigkeit der genannten Informationen ist dem Auskunftsanspruch des Klägers damit Genüge getan.

Auch der Zeitpunkt des Scraping-Vorfalls wurde dem Kläger von der Beklagten genannt. Dass er insoweit informiert wurde, lässt er etwa in der Formulierung des Antrages Ziffer 2 („…*der nach Aussage der Beklagten im Jahr 2019 erfolgte …*“) erkennen.

V. Vorgerichtliche Rechtsanwaltskosten

Die vorgerichtlichen Rechtsanwaltskosten sind als Teil des zu ersetzenden Schadens gemäß Art. 82 Abs. 1 DS-GVO zu erstatten. Aufgrund der Schwierigkeit der Sach- und Rechtslage war die Hinzuziehung eines Rechtsanwalts zur effektiven Durchsetzung der klägerischen Ansprüche

erforderlich und notwendig. Unter Zugrundelegung des Wertes des berechtigten Verlangens des Klägers von 750,00 € (250,00 € immaterieller Schadenersatz + 500,00 € Auskunft) zum Zeitpunkt der außergerichtlichen Tätigkeit führt dies zu berechtigten außergerichtlichen Kosten in Höhe von 159,94 € (1,3-fache Geschäftsgebühr nebst Pauschale nach Nr. 7002 VV RVG zzgl. 19% MwSt.).

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

VI. Die nach dem Schluss der mündlichen Verhandlung eingegangenen Schriftsätze geben mangels neuen Tatsachenvortrages keinen Anlass zur Wiedereröffnung der mündlichen Verhandlung nach § 156 ZPO.

C. Nebenentscheidungen

1. Die Entscheidung über die Kosten beruht auf § 92 Abs. 1 ZPO. Der Kläger hat in Höhe eines Anteils von 900,00 € (250,00 € immaterieller Schaden + 500,00 € Feststellungsbegehren + mit 150,00 € zu bemessender Anteil des Auskunftsanspruchs) am Streitwert obsiegt.

2. Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt aus §§ 708 Nr. 11, § 711 S. 1 und 2 und § 709 S. 1 und 2 ZPO.

Vermögensrechtlich im Sinne des § 708 Nr. 11 ZPO ist eine Streitigkeit, unabhängig von der Natur des zugrundeliegenden Rechtsverhältnisses, wenn der prozessuale Anspruch – wie bei Klageantrag Ziffer 1 – auf Geld (Sachen oder Rechte) gerichtet ist (OLG Köln Urt. v. 26.11.2020 – 15 U 39/20, GRUR-RS 2020, 38050; BeckOK ZPO/Ulrici, 47. Ed. 1.7.2022, ZPO § 708 Rn. 23.1).

3. Zur Begründung der Streitwertentscheidung, die auf § 48 GKG i.V.m. §§ 3, 4, 5 ZPO beruht, wird auf die Ausführungen zur sachlichen Zuständigkeit (oben A. I. 2.) verwiesen.

Rechtsbehelfsbelehrung:

Gegen die Entscheidung, mit der der Streitwert festgesetzt worden ist, kann Beschwerde eingelegt werden, wenn der Wert des Beschwerdegegenstands 200 Euro übersteigt oder das Gericht die Beschwerde zugelassen hat.

Die Beschwerde ist binnen **sechs Monaten** bei dem

Landgericht Heidelberg
Kurfürsten-Anlage 15
69115 Heidelberg

einzulegen.

Die Frist beginnt mit Eintreten der Rechtskraft der Entscheidung in der Hauptsache oder der anderweitigen Erledigung des Verfahrens. Ist der Streitwert später als einen Monat vor Ablauf der sechsmonatigen Frist festgesetzt worden, kann die Beschwerde noch innerhalb eines Monats nach Zustellung oder formloser Mitteilung des Festsetzungsbeschlusses eingelegt werden. Im Fall der formlosen Mitteilung gilt der Beschluss mit dem dritten Tage nach Aufgabe zur Post als bekannt gemacht.

Die Beschwerde ist schriftlich einzulegen oder durch Erklärung zu Protokoll der Geschäftsstelle des genannten Gerichts. Sie kann auch vor der Geschäftsstelle jedes Amtsgerichts zu Protokoll erklärt werden; die Frist ist jedoch nur gewahrt, wenn das Protokoll rechtzeitig bei dem oben genannten Gericht eingeht. Eine anwaltliche Mitwirkung ist nicht vorgeschrieben.

Rechtsbehelfe können auch als elektronisches Dokument eingelegt werden. Eine Einlegung per E-Mail ist nicht zulässig. Wie Sie bei Gericht elektronisch einreichen können, wird auf www.ejustice-bw.de beschrieben.

Schriftlich einzureichende Anträge und Erklärungen, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zu Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument zu übermitteln. Ist dies aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig. Die vorübergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen.

Dr. Stein
Vorsitzende Richterin am Landgericht