Aktenzeichen:
8 O 28/23

Landgericht Freiburg im Breisgau

Abteilung für Zivilsachen

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

[redacted]

– Kläger –

Prozessbevollmächtigte:
Rechtsanwälte Wilde Beuger Solmecke, Kaiser-Wilhelm-Ring 27 - 29, 50672 Köln (Gz: [redacted])

gegen

Meta Platforms Ireland Limited, vertr.d.d. GF. Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland

– Beklagte –

Prozessbevollmächtigte:
Rechtsanwälte Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB, Bockenheimer Anlage 44, 60322 Frankfurt (Gz: [redacted])

wegen Persönlichkeitsrechtsverletzung, Verstöße gegen die Datenschutz-Grundverordnung

hat das Landgericht Freiburg im Breisgau – 8. Zivilkammer – durch den Richter am Landgericht [redacted] als Einzelrichter am 20.09.2023 aufgrund der mündlichen Verhandlung vom 26.07.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an die Klagepartei immateriellen Schadensersatz in Höhe von 200 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 3.2.2023 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klagepartei alle weiteren materiellen Schäden zu ersetzen, die dieser durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten im Jahr 2019 entstanden sind und/oder noch entstehen werden.

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 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, die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.

4. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 453,87 € zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 3.2.2023 zu zahlen.

5. Im Übrigen wird die Klage abgewiesen.

6. Von den Kosten des Rechtsstreits tragen die Klagepartei 55 Prozent und die Beklagte 45 Prozent.

7. Das Urteil ist vorläufig vollstreckbar, für die Klagepartei hinsichtlich des Tenors Ziffer 3 aber nur gegen Sicherheitsleistung in Höhe von 2000 €. Im Übrigen wird der Beklagten nachgelassen, die Vollstreckung durch die Klagepartei gegen Sicherheitsleistung in Höhe von 110 % des auf Grund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht die Klagepartei vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet. Der Klagepartei 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.

Beschluss

Der Streitwert wird auf 6000 € festgesetzt.

Klageantrag Ziffer 1 (1000 €).

Klageantrag Ziffer 2 (Feststellung) beziffert das Gericht mit 500 €, weil ein darüberhinausgehendes wirtschaftliches Interesse der Klagepartei nicht ausreichend dargelegt ist (OLG Karlsruhe, Beschluss vom 5. Juli 2023 – 10 W 5/23 –, Rn. 15, juris).

Klageantrag Ziffer 3 (Unterlassung) beziffert das Gericht mit insgesamt 4000 € für alle Unterlassungsanträge, weil die Klagepartei ein darüberhinausgehendes wirtschaftliches Interesse an der Unterlassung des beanstandenden Verhaltens nicht dargelegt hat (vgl. OLG Karlsruhe, aaO, Rn. 16).

Klageantrag Ziffer 4 (Auskunft) bewertet das Gericht mit 500 €, weil eine größere wirtschaftliche Bedeutung für die Klagepartei nicht erkennbar ist (vgl. OLG Karlsruhe, aaO, Rn. 17).

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.

Die Klagepartei 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.

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 - so die Klagepartei - oder nur "Freunde" - 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 hinterlegten 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.

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 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.

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 Internet. 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 dar. 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.

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 die Klagepartei mit Schreiben vom 22.4.2022 (K 1) die Beklagte zur Zahlung von 500 € Schadenersatz, Unterlassung der zukünftigen Zugänglichmachung der Klägerdaten an unbefugte Dritte sowie zur Auskunftserteilung auf. Mit Schreiben vom 16.5.2022 (B 16) 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. Die Entscheidung wurde von der Beklagten angefochten.

Die Klagepartei ist der Ansicht, die Beklagte habe Vorschriften der DSGVO verletzt.

Sie behauptet, ihre persönlichen Daten wie Telefonnummer, Name, Wohnort, Geschlecht, Land, Arbeitgeber seien durch "Scraping" abgegriffen worden (As. 209). 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 der Klagepartei, 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 diese Daten der Klagepartei zugänglich gemacht worden. Zum jetzigen Zeitpunkt könne noch nicht abgesehen werden, welche Dritten Zugriff auf die Daten der Klagepartei 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.

Die Klagepartei behauptet, die Veröffentlichung ihrer Daten habe weitreichende Folgen für sie. Sie habe einen erheblichen Kontrollverlust über ihre Daten erlitten, welcher großes Unwohlsein und große Sorge über einen möglichen Missbrauch der sie betreffenden Daten ausgelöst habe. Sie habe ein verstärktes Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen entwickelt und vermehrt dubiose Anrufe und SMS-Nachrichten erhalten.

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 die Klagepartei 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.

Die Klagepartei beantragt:

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

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

3. Die Beklagte wird verurteilt, es bei Meldung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, Facebook ID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat" noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.

4. Die Beklagte wird verurteilt der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.

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

Die Beklagte beantragt, 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 der Klagepartei 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. Bei der Klagepartei seien lediglich NutzerID, Vorname, Nachname, Land und Geschlecht und zudem die Telefonnummer 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.

Das Gericht hat die Klagepartei persönlich angehört; auf das Protokoll der mündlichen Verhandlung wird verwiesen.

Entscheidungsgründe

Die Klage ist hinsichtlich des Klageantrags 3a unzulässig. Hinsichtlich der übrigen Klageanträge hat sie nur teilweise Erfolg.

A. Zulässigkeit

Die Klage ist – mit Ausnahme des Antrags Ziffer 3 a) zulässig.

I. Zuständigkeit

Das Landgericht Freiburg ist für sämtliche Anträge international sowie örtlich und sachlich 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. Die Klagepartei hat ihren Wohnsitz in der Bundesrepublik Deutschland und im Bezirk des Landgerichts Freiburg.

2. Das Landgericht Freiburg ist gemäß §§ 23, 71 GVG auch sachlich zuständig, weil der Zuständigkeitsstreitwert 5.000,00 € überschreitet. Die örtliche Zuständigkeit folgt aus § 44 Abs. 1 S. 2 BDSG. Demnach können Klagen gegen einen Verantwortlichen an dem Ort erhoben werden, an dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat. Die Klagepartei hat ihren gewöhnlichen Aufenthaltsort durch ihren Wohnsitz im Bezirk des Landgerichts Freiburg, § 7 BGB.

II. 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 die Klagepartei nachgekommen, indem sie 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).

a) 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).

b) Vorliegend gründet Klageantrag Ziffer 1 auf einem einheitlichen Lebenssachverhalt, der dadurch gekennzeichnet ist, dass die Klagepartei 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. Miteinander verknüpft sind sämtliche Einzelaspekte dieses Vorgangs

durch die Daten, welche die Klagepartei bei der Registrierung hinterlegt hat. Eine Aufspaltung in mehrere Abschnitte stellte eine unnatürliche Trennung eines einheitlichen Sachverhaltes dar.

III. Klageantrag Ziffer 2 (Feststellung)

Der Feststellungsantrag ist in der vom Gericht vorgenommenen Auslegung 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 – VI 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 der Klagepartei, dass sich ihr Antrag ausschließlich auf materielle Schäden richtet, die ihr aus dem Scraping-Vorfall ohne ihr bisheriges Wissen entstanden sind oder die ihr 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 –VI ZR 133/06).

Dies ist hier nicht der Fall. Vielmehr sind die Daten der Klagepartei noch im Internet abrufbar; 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 der Klagepartei bereits ein Schaden zugefügt wurde, von dem er bislang nur noch keine Kenntnis hat.

IV. Klageanträge Ziffer 3 (Unterlassung)

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

1. Klageantrag Ziffer 3 a), mit dem die Klagepartei 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 nicht ausreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO und damit als unzulässig abzuweisen.

a) Nach § 253 Abs. 2 Nr. 2 ZPO darf ein Unterlassungsantrag – und nach § 313 Abs. 1 Nr. 4 ZPO eine darauf beruhende Verurteilung – nicht derart undeutlich gefasst sein, dass der Streitgegenstand und der Umfang der Prüfungs- und Entscheidungsbefugnis des Gerichts (§ 308 Abs. 1 ZPO) nicht erkennbar abgegrenzt sind, sich der Beklagte deshalb nicht erschöpfend verteidigen kann und die Entscheidung darüber, was dem Beklagte verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt. Eine hinreichende Bestimmtheit ist für gewöhnlich gegeben, wenn eine Bezugnahme auf die konkrete Verletzungshandlung erfolgt oder die konkret angegriffene Verletzungsform antragsgegenständlich ist und der Klageantrag zumindest unter Heranziehung des Klagevortrags unzweideutig erkennen lässt, in welchen Merkmalen des angegriffenen Verhaltens die Grundlage und der Anknüpfungspunkt für den Rechtsverstoß und damit das Unterlassungsgebot liegen soll (stRspr; vgl. nur BGH GRUR 2021, 746 Rn. 17 – Dr. Z, mwN). Demgegenüber sind Unterlassungsanträge, die lediglich den Wortlaut eines Gesetzes wiederholen, grundsätzlich als zu unbestimmt und damit als unzulässig anzusehen. Die Bejahung der Bestimmtheit und die Verwendung auslegungsbedürftiger Begriffe im Klageantrag ist in solchen Fällen nur dann zulässig, wenn über ihren Sinngehalt zwischen den Parteien kein Streit besteht und objektive Maßstäbe zur Abgrenzung vorliegen, oder wenn der Kläger den auslegungsbedürftigen Begriff hinreichend konkret umschreibt und gegebenenfalls mit Beispielen unterlegt oder sein Begehren an der konkreten Verletzungshandlung ausrichtet (BGH GRUR 2021, 1425 Rn. 12 – Vertragsdokumentengenerator, mwN; BGH, GRUR 2022, 1308 Rn. 26)

b) Dass mit der Unterlassungsverpflichtung begehrte Verbot ließe sich vorliegend insbesondere im späteren Vollstreckungsverfahren im tatsächlichen nicht im ausreichenden Maße durch Auslegung unter Heranziehung des Sachvortrags der Klagepartei entnehmen. Die Frage wer unbefugter Dritter ist, die tatsächliche Gestaltung der Sicherheitsmaßnahmen und die Frage, was Stand der Technik ist, steht vorliegend zwischen den Parteien gerade nicht außer Frage. Ihr Streit würde sich deshalb gerade nicht lediglich auf die rechtliche Qualifizierung der

angegriffenen Verhaltensweise beschränken lassen. Die Klagepartei hat ihren Unterlassungsantrag trotz entsprechenden Hinweises nicht auf die konkrete Verletzungshandlung beschränkt (vgl. dazu mwN: BGH, GRUR 2022, 1308 Rn. 26 - YouTube II; BGH GRUR 2021, 1425 Rn. 12 – Vertragsdokumentengenerator; Köhler/Feddersen in Köhler/Bornkamm/Feddersen, 41. Aufl. 2023, UWG § 12 Rn. 1.43 und 1.45).

c) Auch der Gesichtspunkt der Gewährleistung effektiven Rechtsschutzes erfordert vorliegend die Zulassung des Unterlassungsantrags nicht. Entgegen der Ansicht des Klägervertreters ergeben sich auch aus dem von der Klagepartei gehaltenen Sachvortrag keine hinreichend konkreten objektiven Maßstäbe zur Abgrenzung des zulässigen vom unzulässigen Verhalten, die unter diesen Voraussetzungen für die Annahme eines den Erfordernissen des § 253 Abs. 2 Nr. 2 ZPO entsprechenden Unterlassungsantrags unverzichtbar sind (vgl. BGH, GRUR 2013, 421 Rn. 45 - Pharmazeutische Beratung über Call-Center; BGH, GRUR 2011, 539 Rdnr. 13 – Rechtsberatung durch Lebensmittelchemiker, m. w. N.). Die Klagepartei kann aus Art. 82 Abs. 1 DSGVO nur das Unterlassen der Zugänglichmachung von Daten verlangen, wenn dadurch gegen die DSGVO verstoßen wird (vgl. Art. 82 Abs. 1 DSGVO). Es gibt nur Sachvortrag dazu, dass die Beklagte beim streitgegenständlichen Scrapingsachverhalt keine nach dem damaligen Stand der Technik ausreichenden Maßnahmen getroffen hat. Zwar kann eine auslegungsbedürftige Antragsformulierung hinzunehmen sein, wenn eine weitere Konkretisierung nicht möglich ist und die Antragsformulierung zur Gewährleistung effektiven Rechtsschutzes erforderlich erscheint. Dies ist hier aber nicht der Fall, weil die Klagepartei sich mit der Formulierung des Klageantrags an der konkreten Verletzungsform orientieren könnte, ohne dass für sie damit ein effektiver Rechtsschutz gefährdet wäre (vgl. BGH, GRUR 2012, 405 Rn. 15 - Kreditkontrolle). Etwas anderes ergibt sich auch nicht aus der vom Klägervertreter zitierten Entscheidung des BGH, weil die dortige Klägerin im Unterlassungsantrag auf die konkrete Verletzungsform Bezug genommen hat und dort der Sachverhalt des verbotenen Verhaltens unstreitig war und es nur um dessen rechtliche Einordnung ging (BGH, GRUR 2015, 1237 Rn. 14). Vorliegend ist aber gerade streitig, welche Maßnahmen die Beklagte zur Vermeidung solcher Scraping-Sachverhalte vorsehen muss. Sie behauptet ja sogar, dass sie beim streitgegenständlichen Vorfall die nach dem Maßstab der DSGVO erforderlichen Maßnahmen ergriffen habe.

2. Dem Klageantrag Ziffer 3 b) ist demgegenüber zulässig.

a) Zwar sind die Begriffe „unübersichtliche und unvollständige Informationen“ auslegungsbedürftig. Diese auslegungsbedürftigen Begriffe werden jedoch hinreichend konkret

umschrieben und mit Beispielen unterlegt bzw. das Begehren an der konkreten Verletzungshandlung ausgerichtet (BGH GRUR 2021, 1425 Rn. 12 – Vertragsdokumentengenerator, mwN; BGH, GRUR 2022, 1308 Rn. 26) durch den Zusatz „namentlich ohne eindeutige Informationen darüber, dass die Telefonnummern auch bei der Einstellung „privat“ noch durch die Verwendung des Kontaktimporttools verwendet werden kann…“.

b) Dem Antrag ist auch nicht mit der Begründung das Rechtsschutzinteresse zu versagen, dass die Klagepartei die Nummer in ihrem Facebookprofil löschen könnte. Denn solange die Beklagte die Möglichkeit zur Angabe der Telefonnummer eröffnet und diese dann verarbeitet, darf der Kunde dies auch wahrnehmen und hat dann einen Anspruch darauf, dass die Beklagte die Anforderungen der DSGVO – die vorliegend gerade streitgegenständlich sind – bei der Verarbeitung dieser Daten einhält.

B. Begründetheit

Die Klage ist – soweit sie zulässig ist – in der Sache nur teilweise erfolgreich. Die Klagepartei hat Anspruch gegen die Beklagte auf Ersatz immateriellen Schadens in Höhe von 200 € nebst Zinsen, Feststellung zukünftigen materiellen Schadens, einen Anspruch auf Unterlassung, sowie auf Zahlung außergerichtlicher Rechtsanwaltskosten nebst Zinsen. Hinsichtlich weitergehender Ansprüche ist die Klage abzuweisen.

I. Klageantrag Ziffer 1 (immaterieller Schaden)

Die Klagepartei hat gegen die Beklagte gemäß Art. 82 Abs. 1 DS-GVO Anspruch auf immateriellen Schadenersatz in Höhe von 200 € 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). Die Beklagte hat personenbezogene Daten (Name, Telefonnummer etc. im Sinne des Art. 4 Abs. 1 Nr. 1 DS-GVO gemäß Art. 4 Abs. 1 Nr. 2 DS-GVO verarbeitet, weil sie diese bezogen auf die Person der Klagepartei im Rahmen der von ihr betriebenen Plattform Facebook gespeichert und sie die Verbindung der klagenden Partei mit ihrer Telefonnummer auch Dritten gegenüber durch die Schaffung dieser Abfragemöglichkeit offengelegt hat. Die Beklagte ist Verantwortliche im Sinne des Art. 4 Nr. 7 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 gegen mehrere Vorschriften der DS-GVO verstoßen. Sie hat sich nicht exkulpieren können. Der Klagepartei ist ein - kausal auf die Verstöße zurückzuführender – immaterieller Schaden entstanden, der auf 200 € beziffert wird.

a) 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). 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. Der EuGH hat aus der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO nunmehr dem Verantwortlichen ausdrücklich die Darlegungs- und Beweislast für die Rechtsmäßigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO auferlegt (EuGH, Urteil vom 04.05.2023 - C-60/22 Rn. 53 ff.).

b) Eine Eingrenzung folgt auch nicht aus des Wortlauts von Art. 82 Abs. 2-5 DSGVO dadurch, dass diese jeweils wörtlich auf die Verarbeitung abstellen. Diese Absätze des Art. 82 DSGVO

dienen lediglich der Abgrenzung der Haftung mehrerer Anspruchsgegner im Innenverhältnis, weil dort auf die die Auftragsverarbeiter betreffenden Pflichten abgestellt wird und nicht auf die durch sie getätigten Verarbeitungsschritte. Auch, dass die letztliche Haftung bei mehreren Anspruchsgegnern von der Verantwortlichkeit für den jeweils verletzten Umstand abhängt, Art. 82 Abs. 3 DSGVO, also erneut nicht auf eine konkrete Verarbeitungstätigkeit abgestellt wird, spricht gegen eine Eingrenzung des Art. 82 Abs. 1 DSGVO. Auch die englische und französische Sprachfassung verwenden entsprechende Formulierung in den jeweiligen Absätzen. Vor diesem Hintergrund sind die wörtlichen Bezüge „durch eine Verarbeitung“ in Abs. 2 sowie „aufgrund einer Verarbeitung“ so zu verstehen, dass diese lediglich auf einen Bezug zu einer Verarbeitung deuten. Das ist auch schon deswegen konsequent, weil die Anwendung der DSGVO selbst eine Verarbeitung voraussetzt, Art. 2 Abs. 1 DSGVO. Keine Vorschrift der DSGVO inkl. des Art. 82 Abs. 1 DSGVO ist überhaupt anwendbar, solange überhaupt gar keine Verarbeitung stattfindet. In diesem Verständnis ist es aber auch nur konsequent, dass diese vorhergehenden und nachfolgenden Pflichten der DSGVO in Bezug auf eine Verarbeitung die Schadensersatzpflicht ebenso auslösen. Diese Auslegung entspricht auch dem in Art. 1 Abs. 2 DSGVO postulierten Ziel, die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten zu schützen.

3. Verstoß gegen Art. 13 DS-GVO (Informationspflicht) und Art. 6 DS-GVO (Rechtmäßigkeit der Verarbeitung), indem sie entgegen Art. 5 Abs. 1 lit. a, Art. 6 Abs. 1 lit. a DSGVO die Zuordnung von Name zu Telefonnummer und FacebookID (Telefonnummernzuordnung) und weiterer Daten gegenüber Dritten offenlegt hat.

Die Beklagte hat gegen die gemäß Art. 13 Abs. 1 c) DS-GVO bestehende Informationspflicht bei Erhebung von personenbezogenen Daten verstoßen, indem sie die Klagepartei bei der Anmeldung auf der Facebook-Plattform nicht ausreichend über die Zwecke informiert hat, für die ihre Telefonnummer verwendet werden sollte. Nach Art. 5 Abs. 1 lit. a DSGVO müssen personenbezogene Daten auf rechtmäßige, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Nach Art. 6 Abs. 1 DSGVO ist die Verarbeitung nur rechtmäßig, wenn eine der aufgezählten Bedingungen erfüllt ist. Mangels hinreichender Information und Bedingungen im Sinne des Art. 6 DS-GVO erfolgte die Verarbeitung der Telefonnummer auch nicht rechtmäßig. Keine Verletzung der Informationspflicht ist – entgegen dem Verständnis der Klagepartei – hingegen in der mangelnden Aufklärung über die Möglichkeit missbräuchlichen Abgreifens von Daten.

(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).

Art. 6 Abs. 1 Buchstabe a DS-GVO setzt eine Einwilligung der betroffenen Person für die konkrete Verarbeitung zu bestimmten Zwecken voraus. Diese Einwilligung muss nach Art. 4 Nr. 11 DSGVO freiwillig und in informierter Weise und unmissverständlich für den bestimmten Fall als Erklärung oder durch eine sonst eindeutig bestätigende Handlung abgegeben werden. Nach Art. 7 Abs. 2 S. 1 DSGVO muss für eine schriftliche Erklärung über die Einwilligung, sofern sie auch noch andere Sachverhalte betrifft, das Ersuchen zu dieser Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Sofern dies nicht gegeben ist, ist die Einwilligungserklärung gemäß Art. 7 Abs. 2 S. 2 DSGVO nicht verbindlich.

Dem ist die Beklagte nicht hinreichend nachgekommen. Zwar wies die Registrierungsseite von Facebook auf die – verlinkte – Datenrichtlinie hin. Dort wurde der Nutzer jedoch nicht darüber aufgeklärt, dass und wie seine Telefonnummer im Rahmen des Einsatzes des CIT verwendet wird. Insbesondere wurde 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 ihn auf Facebook und insbesondere auch über das CIT zu finden. Dazu hätte dem Nutzer erläutert werden 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 Nutzers im Falle eines „Treffers“ dessen Benutzerprofil als „Freund“ hinzufügen und auf die entsprechenden Daten zuzugreifen.

Weder der im Zeitraum bis 19.04.2018 geltenden Datenrichtlinie noch der Version vom 19.04.2018 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 unseren 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 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). Danach ist eine Datenverarbeitung nur unter den dort abschließend aufgezählten Bedingungen rechtmäßig und von diesen ist hier keine erfüllt. Insbesondere ist die Telefonnummer nicht für die Erfüllung des Vertrages im Sinne des Art. 6 Abs. 1 b) DS-GVO erforderlich. Art. 6 Abs. 1 b) DS-GVO erlaubt alternativ die Verarbeitung, soweit sie zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist. Damit die Verarbeitung für den Zweck der Erfüllung eines solchen Vertrages erforderlich ist, muss sie objektiv unerlässlich sein, einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten

Vertragsleistung ist. Sind mehreren Leistungen in einem Vertrag zusammen vereinbart, die unabhängig voneinander erbracht werden könnten, ist in der Betrachtung jeweils nur auf die konkrete, einzelne Leistung abzustellen. Es reicht dabei nicht aus, dass eine solche Verarbeitung im Vertrag erwähnt wird oder für die Leistungserfüllung lediglich nützlich ist. Es dürfen vielmehr keine praktikablen und weniger einschneidenden Alternativen bestehen (EuGH, Urteil vom 4. Juli 2023, Az. C-252/21, ECLI:EU:C:2023:537, Rn 98 ff.). Die Erforderlichkeit ist eng zu verstehen, da sie jeweils eine Verarbeitung personenbezogener Daten auch ohne eine Einwilligung unter Berücksichtigung der hohen Maßstäbe erlauben, die an die Freiwilligkeit für diese anzulegen sind (EuGH, Urteil vom 4. Juli 2023, Az. C-252/21, ECLI:EU:C:2023:537, Rn 93). Die fehlende Erforderlichkeit der Auffindbarkeit über das CIT Tool ergibt sich hier schon daraus, dass die Angabe der Telefonnummer 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 Art 13 Abs. 1 e). Auch wenn man unbefugte Dritte als Empfänger im Sinne dieser Vorschrift betrachtet, 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.

4. Verstoß gegen 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 der Klagepartei, namentlich ihre Facebook-ID, ihren Vornamen und Namen, ihr Geschlecht, ihren Wohnort sowie 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 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 Sicherheitsmaßnahmen genügten nicht, um die von der Klagepartei zur Verfügung gestellten Daten hinreichend vor unbefugtem Zugriff zu schützen.

c) 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).

d) Der EuGH hat aus der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO nunmehr dem Verantwortlichen ausdrücklich die Darlegungs- und Beweislast für die Rechtsmäßigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO auferlegt. (EuGH, Urteil vom 04.05.2023 - C-60/22 Rn. 53 ff.). Die Beweislastregelung des Art. 5 Abs. 2 DS-GVO gilt gemäß Art. 5 Abs. 1 f DS-GVO auch hinsichtlich der Anforderungen des Art. 32 DS-GVO, weil dieser die Gewährleistung der angemessenen Sicherheit regelt. Hier hat die Beklagte noch nicht einmal hinreichend konkret genug die von ihr damals ergriffenen Maßnahmen zur Verminderung des Risikos des Datenmissbrauchs dargelegt.

e) 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 weitverbreitete 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 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.

f) 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 unplausibel geblieben, weil die Beklagte nicht erklärt hat, warum diese das Scraping nicht verhindert haben. 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.

g) Soweit sich dem Vortrag der Beklagten im Kern entnehmen lässt, dass sie im 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. 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 hinzunehmenden 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.

5. Verstoß gegen 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 datenschutzfreundliche 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, weil aus der Verletzung der sich aus Art. 25 DS-GVO ergebenden Pflichten eine Erhöhung der Gefahr eines Schadenseintritts resultiert (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 verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist 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.

6. Verstoß gegen Artt. 33, 34 DS-GVO (Meldepflichten)

Gemäß Art. 33 Abs. 1 DSGVO muss der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der gem. Art. 55 DSGVO zuständigen Aufsichtsbehörde melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Der Mindestinhalt der Meldung ist in Art. 33 Abs. 3 DSGVO festgelegt. Dem ist die Beklagte vorliegend nicht nachgekommen (vgl. so auch: LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 88, beck-online). Ob auch ein Verstoß gegen Art. 34 Abs. 1 DSGVO liegt kann hier offenbleiben. Nach dieser Vorschrift benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten, wenn diese voraussichtlich ein hohes Risiko für seine persönlichen Rechte und

Freiheiten zur Folge hat (so LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 97, beck-online). Denn die Klagepartei hat nicht dargelegt, welche Schritte sie bei einer unverzüglichen Information ergriffen hätte und wie das den Schaden bzw. potenzielle Gefahren aus dem Scrapingsachverhalt beeinflusst hätte.

7. möglicher Verstoß gegen Auskunftspflicht des Art. 15 DS-GVO

Ob die Beklagte dem vorgerichtlichen Auskunftsersuchen der Klägerseite über ihre personenbezogenen Daten nicht in ausreichendem Maße nachgekommen ist und dadurch gegen Art. 15 DSGVO verstoßen hat kann dahinstehen. Denn die Ungewissheit über die Verarbeitung der eigenen Daten deckt sich mit dem Schaden durch den eigentlichen Verstoß. Ein eigenständiger Schadensersatzanspruch aufgrund einer Verletzung der Auskunftspflicht kommt nur in Betracht, wenn die fehlende Auskunft einen Schaden zumindest verschärft hat. Dies ist hier nicht zu erkennen, weil die Klagepartei nicht ansatzweise darlegt welche Schritte sie bei einer ausreichenden Auskunft vorgenommen hätte und wie das einen Schaden vermindert hätte.

8. Keine Exkulpation gemäß Art. 82 DS-GVO

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

a) 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).

b) 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.

9. Schaden

Der Klagepartei 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.

a) 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. Für einen Schadensersatzanspruch nach Art. 82 DSGVO reicht allerdings der bloße Verstoß gegen die Bestimmungen der DSGVO nicht aus. Es muss ein Schaden vorliegen (EuGH, Urteil vom 4. Mai 2023 – C-300/21 –, juris Rn 33 ff.). Der Ersatz eines immateriellen Schadens nach Art 82 DS-GVO ist aber nicht davon abhängig, dass der entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht (EuGH, aaO, Rn. 45), so dass auch Bagatellschäden einen Schadensersatzanspruch begründen.

b) 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 gegen die 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). Der EuGH hat in seiner hierzu ergangenen Entscheidung dieser Auffassung des Generalanwalts nicht widersprochen, sondern nur betont, dass über den auf dem DS-GVO beruhenden Datenverlust als solches ein immaterieller Schaden des Betroffenen festgestellt werden muss (EuGH, aaO, Rn. 50).

c) Im streitgegenständlichen Fall trat der immaterielle Schaden durch die aufgrund des Scrapings bei der Klagepartei 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 diese einen Kontrollverlust über ihre Daten, der vorliegend mit dem subjektiv besorgniserregenden Risiko einherging, dass diese Daten etwa durch Identitätsdiebstahl unbefugt und schadensträchtig genutzt werden. Diese Befürchtung hat sich dann im weiteren Verlauf nach der glaubhaften Schilderung des Klägers in 3-5 Spamanrufen in der Woche manifestiert. An Spam SMS konnte er sich hingegen nicht erinnern.

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 der Klagepartei in einem Datensatz, führt zu einer höheren Dimension des Kontrollverlustes des hinsichtlich ihrer 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.

Die Klagepartei hat mittels Kopie in einem Schriftsatz einen Datenauszug (vgl. As. 209/210) vorgelegt, der diese Daten gemeinsam mit der Telefonnummer, der NutzerID und dem Namen enthält, und von dem sie behauptet, er sei aus einer Datenbank im Darknet abgerufen. Das Gericht zweifelt angesichts der Angaben der Klagepartei in ihrer persönlichen Anhörung nicht daran, dass es sich um einen authentischen Auszug handelt und dieser aus dem Scraping-Vorfall stammt. 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 Anlage befindliche NutzerID mit der nach der Telefonnummer befindlichen zweiten Nummer auf dem Datensatz übereinstimmt.

d) Die erforderliche Kausalität zwischen den Verstößen der Beklagten gegen die DS-GVO und dem Schaden der Klagepartei liegt vor. Wäre die Klagepartei ohne Verstoß gegen die Informationspflichten nach Art. 13 Abs. 1 c) DS-GVO ordnungsgemäß darüber aufgeklärt worden, dass ihre 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 sie auf Facebook zu finden, hätte sie ihre Telefonnummer nicht eingetragen oder die Standardeinstellungen verändert. Denn aus ihrer persönlichen Anhörung ergibt sich deutlich, dass sie über ihre 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.

Dass die gescrapten Daten seitens der Klagepartei 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.

f) Höhe des immateriellen Schadens

Die Klagepartei hat Anspruch auf Zahlung eines immateriellen Schadenersatzes in Höhe von lediglich 200 €.

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). Bei der Festsetzung der Höhe des Schadensersatzes sind die mitgliedstaatlichen Vorschriften unter Berücksichtigung des unionsrechtlichen Effektivitätsgebots und Äquivalenzgebots anzuwenden. In Anbetracht der Ausgleichsfunktion des in Art. 82 DSGVO vorgesehenen Schadenersatzanspruchs ist eine auf diese Bestimmung gestützte finanzielle Entschädigung „vollständig und wirksam“, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen, ohne dass ein vollumfänglicher Ausgleich die Verhängung von Strafschadenersatz erfordert (EuGH, aaO, Rn. 58). Die DSGVO selbst enthält keine weiteren Bemessungsgrundsätze. Allerdings kann die Fluggastrechte-Verordnung als erster Anhaltspunkt dienen, die einen Ausgleichsanspruch i.H.v. 250 bis 600 Euro vorsieht. Die Fluggastrechte-Verordnung betrifft zwar einen gänzlich anders gelagerten Sachverhalt und gleicht auch nicht den Eingriff in das Recht zur informationellen Selbstbestimmung aus. Aber auch der Ausgleichsanspruch dient vorrangig dem Ausgleich eines immateriellen Schadens. (Wenn, jurisPR-ITR 5/2023 Anm. 3).

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 200 € 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 die Klagepartei 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. Zudem handelt es sich im Vergleich zu anderen Fällen um relativ wenige Anrufe, die inzwischen auch nachgelassen haben.

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

II. Feststellungsanspruch (Klageantrag Ziffer 2)

Der Feststellungsantrag ist begründet. Die Klagepartei 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 bei der Klagepartei führen kann, steht angesichts dessen, dass nicht bekannt ist, wer Zugriff auf dessen Datensatz hat, für das Gericht außer Zweifel. Dies ergibt sich schon aus der Möglichkeit des Missbrauchs der Telefonnummer.

III. Unterlassung (Klageantrag Ziffer 3)

1. Der mit Klageantrag Ziffer 3 a) verfolgte Unterlassungsanspruch ist nicht nur unzulässig (s.o.), sondern auch unbegründet.

Die Klagepartei kann von der Beklagten nicht verlangen, dass diese es unterlässt, die Daten der Klagepartei 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) Die Klagepartei 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 sie 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).

2. Der Unterlassungsanspruch 3b ist hingegen begründet, weil die Klagepartei zum einen bereits aus dem mit der Beklagten bestehenden Vertragsbeziehung die Einhaltung der Anforderungen der DS-GVO als vertragliche Nebenpflicht verlangen kann. Zudem folgt hier aus dem vergangenen Verstoß gegen Art. 13 Abs. 1c DS-GVO, insbesondere der unbefugten Offenlegung unter Verwendung unzureichender Standardeinstellungen als Verstöße gegen Art. 5 Abs. 1 lit. a DSGVO und Art. 25 Abs. 2 DSGVO ein legitimes Interesse der Klagepartei, der Beklagten für die Zukunft einen kerngleichen Verstoß gegen diese Vorschrift zu verbieten. Es besteht auch Wiederholungsgefahr, weil die Beklagte die Verstöße bestritten hat und weiterhin bestreitet.

Unterlassungsansprüche sind auch unter der Geltung der DS-GVO nicht durch deren Vorrang ausgeschlossen. Soweit die DS-GVO 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).

IV. Auskunft (Klageantrag Ziffer 4)

Der Klagepartei steht ferner der mit dem Klageantrag zu 4) verfolgte Auskunftsanspruch gegenüber der Beklagten nicht zu. Der Anspruch folgt insbesondere nicht aus Art. 15 DSGVO.

1) Nach dieser Vorschrift kann die betroffene Person Auskunft über personenbezogenen Daten verlangen, wenn der Verantwortliche sie betreffende personenbezogene Daten verarbeitet hat. Art. 15 Abs. 1 Hs. 1, 2 DSGVO enthält zunächst einen Anspruch der betroffenen Person gegen den Verantwortlichen, ihm zu bestätigen, ob ihn betreffende personenbezogene Daten verarbeitet werden. Verarbeitet der Verantwortliche personenbezogene Daten der betroffenen Person, so hat die betroffene Person gem. Art. 15 Abs. 1 Hs. 1, 2 DSGVO ein Recht auf Auskunft über diese personenbezogenen Daten (vgl. BGH, Urteil vom 15.06.2021 - VI ZR 576/19 = NJW 2021, 1381). Im Ausgangspunkt steht der Klagepartei nach dieser Vorschrift grundsätzlich ein Auskunftsanspruch über die bei der Beklagten als Verantwortlicher im Sinne des Art. 4 Nr. 7 Hs. 1 DSGVO verarbeiteten ihn betreffenden personenbezogenen Daten zu.

2) Der Anspruch ist jedoch durch Erfüllung untergegangen, § 362 Abs. 1 BGB.

a) Den Auskunftsanspruch erfüllt der Verantwortliche indem er die verlangten Informationen nach Maßgabe des Art. 15 erteilt. Außerdem muss der Verantwortliche eine Kopie der personenbezogenen Daten, die er verarbeitet, zur Verfügung stellen. 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 oder Unvollständigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen, was auch aus dem Wortlaut des § 259 Abs. 2 BGB folgt. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die - gegebenenfalls konkludente - Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (vgl. BGH, Urteil vom 03.09.2020 - III ZR 136/18 = GRUR 2021,110). Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll.

b) Dies ist hier der Fall. Mit Schreiben vom 16.05.2022 hat die Beklagte in angemessener Weise mitgeteilt, welche personenbezogenen Daten verarbeitet werden, indem sie der Klagepartei auf die Selbstbedienungstools verwiesen hat. Sie hat auch Auskunft darüber erteilt, welche Daten der Klagepartei nach ihrer Kenntnis vom Scraping betroffen sind. Diese Erfüllungshandlung war ausreichend um den Erfüllungserfolg zu gewährleisten.

c) Soweit die Klagepartei darüber hinaus Auskunft verlangt, „welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten“ besteht ein Anspruch nicht. Der Anspruch ist (ebenfalls) durch Erfüllung untergegangen, § 362 BGB. Die Beklagte hat mit der Klageerwiderung vorgetragen, über die Verarbeitungstätigkeiten Dritter (hier: „Scraper“), keine Angaben machen zu können. Unabhängig davon, ob die erteilte Auskunft unrichtig oder unvollständig ist, begründet die erteilte Auskunft jedenfalls keinen (weiteren) Auskunftsanspruch, da die Beklagte zum Ausdruck gebracht hat, das Auskunftsbegehren der Klagepartei vollständig erfüllt zu haben. (vgl. idS: LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 162-168, beck-online) Zwar hat die Auskunft über konkrete Empfänger Vorrang vor der Auskunft über Kategorien von Empfängern (vgl. EuGH, Urteil vom 12.01.2023, Az. C-154/21, ECLI:EU:C:2023:3 – Österreichische Post (Informations relatives aux destinataires de données personnelles), Rn. 43), allerdings führt dieser Vorrang nicht dazu, dass eine nicht vorhandene Information erteilt werden muss. Die Beklagte war gemäß Art. 11 Abs. 1 DSGVO auch nicht verpflichtet, diese Information zu erheben, nur um Sie für den Fall der Geltendmachung eines Auskunftsanspruchs erteilen zu können.

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 (200 € immaterieller Schadenersatz + 500 € Feststellung + 4000 € Unterlassung +500 Auskunft) zum Zeitpunkt der außergerichtlichen Tätigkeit führt dies zu berechtigten außergerichtlichen Kosten in Höhe von 453,87 € (1,3-fache Geschäftsgebühr nebst Pauschale nach Nr. 7002 VV RVG zzgl. 19% MwSt.). Der Zinsanspruch folgt aus §§ 288, 291, 187 Abs. 1 BGB.

C. Nebenentscheidungen

1. Die Entscheidung über die Kosten beruht auf § 92 Abs. 1 ZPO.

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

Rechtsbehelfsbelehrung

Gegen die Festsetzung des Streitwerts kann Beschwerde eingelegt werden, wenn der Wert des Beschwerdegegenstands 200 EUR übersteigt oder das Gericht die Beschwerde zugelassen hat.

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

Landgericht Freiburg im Breisgau
Salzstraße 17
79098 Freiburg im Breisgau

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 dieser Frist festgesetzt worden, kann die Beschwerde noch innerhalb eines Monats nach Zustellung oder formloser Mitteilung des Festsetzungsbeschlusses eingelegt werden.

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 eingereicht werden. **Eine einfache E-Mail genügt den gesetzlichen Anforderungen nicht.**

Rechtsbehelfe, die durch eine Rechtsanwältin, einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als **elektronisches Dokument** einzureichen, es sei denn, dass dies aus technischen Gründen vorübergehend nicht möglich ist. In diesem Fall bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig, wobei die vorübergehende Unmöglichkeit bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen ist. Auf Anforderung ist das elektronische Dokument nachzureichen.

Das elektronische Dokument muss

- mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder
- von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.

Ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen ist, darf wie folgt übermittelt werden:

- auf einem sicheren Übermittlungsweg oder
- an das für den Empfang elektronischer Dokumente eingerichtete Elektronische Gerichts- und Verwaltungspostfach (EGVP) des Gerichts.

Wegen der sicheren Übermittlungswege wird auf § 130a Absatz 4 ZPO verwiesen. Hinsichtlich der weiteren Voraussetzungen zur elektronischen Kommunikation mit den Gerichten wird auf die Verordnung

über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung – ERVV) in der jeweils geltenden Fassung sowie auf die Internetseite www.justiz.de verwiesen.

[redacted]