Aktenzeichen:
54 O 165/22

Landgericht Stuttgart

Im Namen des Volkes

Urteil

In dem Rechtsstreit

[redacted]
- Kläger -

Prozessbevollmächtigte:

gegen

[redacted]
Beklagte -

Prozessbevollmächtigte:
[redacted]

wegen Persönlichkeitsverletzung

hat das Landgericht Stuttgart - 54. Zivilkammer - durch den Richter am Landgericht Schellenberg als Einzelrichter aufgrund der mündlichen Verhandlung vom 14.03.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz i.H.v. 600 Euro nebst Zinsen i.H.v. 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 21.09.2022 zu zahlen.

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

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000 Euro, 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) personenbezogene Daten des Klägers, namentlich Telefonnummer, Facebook-ID, Familienname, Vorname, Geschlecht, Stadt und Beziehungsstatus, unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

   b) die Telefonnummer des Klägers auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Contact-Import-Tools 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 i.H.v. 627,13 € nebst Zinsen i.H.v. 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 21.09.2022 zu zahlen.

5. Im Übrigen wird die Klage abgewiesen.

6. Von den Kosten des Rechtsstreits hat der Kläger 13 %, die Beklagte 87 % zu tragen.

7. Das Urteil ist vorläufig vollstreckbar, für den Kläger hinsichtlich Ziff. 1, Ziff. 4 und wegen der Kosten nur gegen Sicherheitsleistung i.H.v. 110 Prozent des jeweils zu vollstreckenden Betrages, ansonsten hinsichtlich Ziff. 2 gegen Sicherheitsleistung i.H.v. 600 Euro und hin-

sichtlich Ziff. 3 gegen Sicherheitsleistung i.H.v. 6.000 Euro. Dem Kläger wird nachgelassen, die Vollstreckung durch die Beklagte gegen Sicherheitsleistung i.H.v. 110 Prozent des aufgrund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit i.H.v. 110 Prozent des jeweils zu vollstreckenden Betrages leistet.

Beschluss

Der Streitwert wird auf 6.500,00 € festgesetzt.

Tatbestand

Die Parteien streiten um Ansprüche auf Schadensersatz, Unterlassung und Auskunft im Zusammenhang mit einem sog. „*Scraping-Sachverhalt*“.

Die Klagepartei ist Nutzerin der Facebook-Plattform. Die Beklagte ist Anbieterin der Facebook-Plattform auf dem Gebiet der Europäischen Union.

Die Plattform ermöglicht nach einer Anmeldung die Kommunikation mit anderen Nutzern. Insbesondere können private Fotos und Informationen geteilt werden. 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 (“*immer öffentliche Nutzerinformationen*“). Eine Eingabe der Handynummer ist nicht zwingend erforderlich.

Die Beklagte stellt überdies Privatsphäre-Einstellungen zur Verfügung, damit Nutzer bestimmen können, inwieweit sie Informationen, die sie zur Verfügung stellen, öffentlich einsehbar machen möchten.

Bei der sogenannten "*Zielgruppenauswahl*" legt der Nutzer fest, wer einzelne Informationen auf

seinem 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.

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 es die Beklagte ihm, seine Kontakte mit den auf der Plattform hinterlegten Telefonnummern abzugleichen, um die hinter den Nummern stehenden Personen als Freunde hinzuzufügen. Dafür ist nicht erforderlich, dass der andere Nutzer seine Telefonnummer nach der "*Zielgruppenauswahl*" öffentlich gemacht hat. Demnach ist es möglich, Nutzer anhand einer Telefonnummer zu finden, solange ihre "*Suchbarkeits-Einstellung*" für Telefonnummern auf der Standard-Voreinstellung "*Alle*" eingestellt war. Daneben waren die Einstellungen nur "*Freunde von Freunden*" oder "*Freunde*" auswählbar. Ab Mai 2019 stand Nutzern auch die Option "*Nur ich*" zur Verfügung. Die Suchbarkeit der Klagepartei war seit dem 18. März 2010 bis mindestens zum Ende des relevanten Zeitraums September 2019 auf „*Everyone*“, d.h. „*Alle*“, eingestellt (Anl. B17).

Bei der Registrierung wird der Nutzer auf die Datenrichtlinie der Beklagten hingewiesen (Anl. B 9). Den Nutzern werden zudem im "*Hilfebereich*", der unmittelbar auf der Facebook-Homepage verlinkt ist, Informationen über die Privatsphäre-Einstellungen zur Verfügung gestellt. Auf diese Einstellungen kann unter der Überschrift "*Privatsphäre, Datenschutz und Sicherheit*" zugegriffen werden (Anlagen B1 bis B8).

Im Zeitraum von Januar 2018 bis September 2019 kam es zu einem sogenannten "*Datenscraping*", also dem massenhaften, automatisierten Sammeln der persönlichen Daten von bis zu 533 Millionen Facebook-Nutzern. "*Scraping*" ist eine Methode, um Daten, die typischerweise öffentlich einsehbar sind, von Internetseiten durch automatisierte Softwareprogramme abzurufen. Dieses Sammeln von Daten mittels automatisierter Tools und Methoden war und ist nach den Nutzungsbedingungen der Beklagten untersagt.

Die Telefonnummern wurden beim „*Scraping-Sachverhalt*“ von den Scrapern mit einem Prozess der sogenannten Telefonnummernaufzählung bereitgestellt. Nutzer konnten ihre Kontakte von ihren Mobilgeräten auf Facebook hochladen, um diese Kontakte auf der Facebook-Plattform zu finden und mit ihnen in Verbindung zu treten (Kontakt-Importer-Funktion). Zu diesem Zweck haben die Scraper mithilfe der Kontakt-Importer-Funktion Kontakte hochgeladen, welche mögliche Tele-

fonnummern von Nutzern enthielten, um so festzustellen, ob diese Telefonnummern mit einem Facebook-Konto verbunden sind. Soweit die Scraper feststellen konnten, dass eine Telefonnummer mit einem Facebook-Konto (in Übereinstimmung mit der jeweiligen Suchbarkeits-Einstellung des Nutzers) verknüpft war, haben sie die öffentlich einsehbaren Informationen (in Übereinstimmung mit der Zielgruppenauswahl des Nutzers) aus dem betreffenden Nutzerprofil kopiert und die Telefonnummer den abgerufenen, öffentlich einsehbaren Daten sodann hinzugefügt. Die weiteren Einzelheiten hinsichtlich des Ablaufs des "Scrapings" sind zwischen den Parteien streitig.

Die zuständige Datenschutzbehörde wurde von der Beklagte nicht über den Vorfall informiert. Die irische Datenschutzbehörde DPC verhängte gegen die Beklagte am 28.11.2022 eine Geldbuße in Höhe von 265 Mio. Euro (Entscheidung der DPC Anlage K3). Die DPC sah einen Verstoß der Beklagten insbesondere gegen Art. 25 Abs. 1 und 2 DS-GVO.

Mit einer E-Mail der Prozessbevollmächtigten des Klägers vom 27.01.2022 forderte dieser die Beklagte mit Fristsetzung bis 28.2.2022 zur Schadensersatzzahlung i.H.v. 500,00 EUR, zur Unterlassung zukünftiger Zugänglichmachung der Daten des Klägers an unbefugte Dritte und zur Auskunft darüber auf, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht worden waren (Anl. K1). Hierauf hat die Beklagte mit Anwaltschreiben vom 25.02.2022 (Anl. B16) erwidert.

Der Kläger behauptet im Wesentlichen,

seine persönlichen Daten wie Telefonnummer, Name, Wohnort und E-Mailadresse seien durch den "Scraping-Sachverhalt" abgegriffen worden. Ob noch mehr Daten entwendet worden seien, lasse sich mangels ausreichender Auskunft durch die Beklagte noch nicht angeben. Grundsätzlich seien von dem Vorfall Nutzerdaten wie Telefonnummer, Facebook-ID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus und weitere korrelierende Daten betroffen.

Die personenbezogenen Daten, wie auch diejenigen des Klägers, seien sodann im Internet auf Seiten, die illegale Aktivitäten wie Internetbetrug begünstigen sollen, so z.B. in bekannten "*Hacker-Foren*", veröffentlicht worden. Sie würden insbesondere für gezielte Phishing Attacken genutzt. Auf einer im sogenannten „*Darknet*“ für jedermann abrufbaren Datenbank seien Telefonnummer, die Facebook-ID, der Name, Geschlecht, Wohnort, Land, Beziehungsstatus und der Arbeitgeber der Klägerseite zugänglich gemacht worden (Bl. 196). Es könne noch nicht abgesehen werden, welche Dritte Zugriff auf die Daten des Klägers erhalten hätten und für welche konkreten strafbaren Handlungen die Daten missbraucht würden.

Der Kläger behauptet, die Unbekannten hätten die Daten aus dem Datenbestand von Facebook

mittels des Contact Importer Tool (“CIT“) aus zum Teil öffentlich zugänglichen Daten bei Facebook ausgelesen und persistiert. Die Telefonnummern der Benutzer hätten wegen einer Sicherheitslücke mit den restlichen Personendaten korreliert werden können. Durch die Eingabe einer Vielzahl von Kontakten in ein virtuelles Adressbuch sei es gelungen, die Telefonnummern konkreten Facebook-Profilen zuzuordnen, ohne dass die hinterlegten Telefonnummern öffentlich freigegeben waren. Um die Telefonnummer jeweils zu korrelieren, sei mit Hilfe des "CIT" jede fiktive Nummer geprüft und der zugehörige Facebook-Nutzer angezeigt worden. Ein Programm habe unzählige Kombinationen von Telefonnummern getestet, um festzustellen, ob diese mit einem Facebook-Nutzer übereinstimmen bzw. ob diese bei Facebook hinterlegt worden ist. Wenn dies der Fall gewesen sei, sei es dem Programm möglich gewesen, sämtliche Daten des Nutzers abzufragen und zu exportieren.

Der Kläger behauptet, dieses "Scraping" sei dadurch ermöglicht worden, dass die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten "CIT" zu verhindern. So seien keine Sicherheitscapchas (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. Ebenso wenig sei ein Mechanismus zur Überprüfung der Plausibilität der Anfragen bereitgehalten worden. Der massenhafte Zugriff auf die Facebook-Profile durch Dritte mit auffälligen Telefonnummerabfragen (z.B. 000001, 000002 usw.) wäre durch einfachste IP-Logs erkennbar und blockierbar gewesen. Es sei eine Kombination mehrerer Maßnahmen erforderlich, angemessen und üblich. Die Einführung einer Begrenzung der abgleichbaren Rufnummern oder Nutzung des "CIT" für Freunde von Freunden sei möglich gewesen. Mindestens aber ein expliziter Hinweis auf die "offenen" Standard-Einstellungen für die Suchbarkeit per Telefonnummer fehle, insbesondere bei erstmaliger Erhebung der Telefonnummer des Nutzers. Wären derartigen Sicherheitsmaßnahmen vorgenommen worden, wäre es mit an Sicherheit grenzender Wahrscheinlichkeit nicht möglich gewesen, mit einem automatisierten Verfahren Daten abzugreifen.

Der Kläger ist ferner der Ansicht, dass die Einstellungen zur Sicherheit der Telefonnummer auf Facebook so undurchsichtig und kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Die Beklagte handele 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 Telefon-

nummer von der Öffentlichkeit gefunden werden möchte, sei aufgrund der vielschichtigen Einstellungsmöglichkeit nicht zu erreichen, wenn lediglich nach den Einstellungsmöglichkeiten für die Telefonnummer gesucht werde.

Der Kläger habe einen erheblichen Kontrollverlust über seine Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über einen möglichen Missbrauch seiner Daten verblieben. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen. Darüber hinaus erhalte der Kläger seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese würden Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks enthalten. Das habe dazu geführt, dass der Kläger nur noch mit äußerster Vorsicht auf jegliche E-Mails und Nachrichten reagieren könne und jedes Mal einen Betrug fürchte und Unsicherheit verspüre.

Der Kläger behauptet, dass er seine Telefonnummer stets bewusst und zielgerichtet weiter gebe und er diese auf der Plattform nicht abgegeben hätte, wenn die Beklagte ausreichend und im angemessenen Umfang über die Folgen der Preisgabe der Telefonnummer informiert hätte.

Der Kläger beantragt:

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

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

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

   a) personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Bezie-

hungsstatus 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 trägt im Wesentlichen vor,

Daten seien weder durch Hacking noch infolge einer Schwachstelle, eines Fehlers oder eines Sicherheitsverstoßes in den Systemen der Beklagten erlangt worden. Vielmehr seien die durch Scraping abgerufenen Daten von Dritten im Wege eines groß angelegten Datenscrapings „*gescraped*“ worden, wobei dieser Begriff lediglich das automatisierte Sammeln von in diesem Fall öffentlich einsehbaren Daten von einer Website oder Anwendung („App“) beschreibe.

Soweit die durch Scraping abgerufenen Daten von der Facebook-Plattform stammen und Informationen über die Klagepartei enthalten, seien diese Daten entweder tatsächlich nicht durch Scraping abgerufen worden oder im Einklang mit den jeweiligen Privatsphäre-Einstellungen öffentlich auf der Facebook-Plattform einsehbar gewesen. Dritte hätten allein solche Daten gesam-

melt (d.h. „gescraped“), die ohnehin öffentlich einsehbar seien, und hätten diese öffentlich einsehbaren Daten auch anderweitig im Internet zugänglich gemacht. Dabei ermögliche das Contact-Import-Tool den Nutzern lediglich, ihre Kontakte von ihren Mobilgeräten auf Facebook hochzuladen, um diese Kontakte auf der Facebook-Plattform zu finden und mit ihnen in Verbindung zu treten, nicht dagegen einen Export von Nutzerdaten. Die Telefonnummern seien von den Scrapern bereitgestellt worden. Das Contact-Import-Tool habe es dann ermöglicht, den Kläger im Einklang mit seinen Suchbarkeits-Einstellungen anhand seiner Telefonnummer auf der Facebook-Plattform zu finden.

Es sei auch grundsätzlich nicht möglich, Scraping öffentlich einsehbarer Daten völlig zu verhindern, ohne den Zweck der Plattform durch Beseitigung der Funktionen zu unterlaufen. Es gebe allenfalls Mittel, um Scraping zu begrenzen. Da die Funktionen, welche Scraper ausnutzten, rechtmäßige, gewöhnliche Nutzerfunktionen darstellten, werde zur Begrenzung von Scraping regelmäßig nicht die gesamte zugrundeliegende Funktion beseitigt. Vielmehr würden in der Regel lediglich die Methoden beschränkt, mit denen auf die maßgeblichen Funktionen zugegriffen werden könne. Die Beklagte habe angemessene technische und organisatorische Maßnahmen ergriffen, das Risiko von Scraping zu unterbinden und Maßnahmen zur Bekämpfung von Scraping zu ergreifen.

Der Kläger sei sowohl über die Einstellungsmöglichkeiten als auch über mögliche Konsequenzen seiner Einstellungen informiert gewesen. Er habe sich entschieden, bestimmte Daten öffentlich einsehbar auf seinem Facebook-Profil zu teilen.

Wegen der weiteren Einzelheiten des Sach- und Streitstands wird Bezug genommen auf die gewechselten Schriftsätze nebst Anlagen sowie die Protokolle der mündlichen Verhandlung vom 21.02.2023 und vom 14.3.2023 samt informatorischer Anhörung des Klägers verwiesen.

Entscheidungsgründe

Die Klage ist zulässig und in dem aus dem Tenor ersichtlichen Umfang begründet; im Übrigen ist sie unbegründet.

A.

Das Landgericht Stuttgart ist international, örtlich und sachlich zuständig (vgl. bereits LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 34 - 39, juris).

I. Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 EuGVVO. Gemäß Art. 18 Abs. 1 Alt. 2 EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher – hier der Kläger – seinen Wohnsitz – hier: in der Bundesrepublik Deutschland – hat.

II. Die internationale Zuständigkeit deutscher Gerichte ergibt sich ferner aus Art. 79 Abs. 2 DS-GVO, deren zeitlicher, sachlicher und räumlicher Anwendungsbereich eröffnet ist.

III. Das Landgericht Stuttgart ist nach Art. 18 Abs. 1 Alt. 2 EuGVVO sowie Art. 79 Abs. 2 Satz 2 DS-GVO örtlich zuständig.

IV. Die sachliche Zuständigkeit ergibt sich aus §§ 23, 71 GVG, nachdem der Gegenstandswert mehr als 5.000 Euro beträgt (vgl. unten D.).

B.

Die Klage ist zulässig.

I. Der Klageantrag zu 1) ist zulässig und insbesondere hinreichend bestimmt.

Der Kläger stellt die Bemessung des Schmerzensgeldes, hinsichtlich dessen er eine Größenordnung seiner Vorstellungen angegeben hat, zulässigerweise in das Ermessen des Gerichts. Ferner hat die Klagepartei mitgeteilt, worauf sich ihr Begehren bezieht und dass sowohl einen Anteil des Schmerzensgeldes für das Verhalten der Beklagten vor dem Daten-Scraping-Vorfall als auch einen Anteil für das nachfolgende Verhalten begehrt wird, so dass eine alternative Klagebegründung nicht angenommen werden kann.

II. Auch der mit dem Klageantrag zu 2) geltend gemachte Feststellungsantrag ist zulässig.

1. Klageantrag zu 2) genügt insbesondere dem Bestimmtheitserfordernis des § 253 Abs. 2 Nr. 2 ZPO. Dem Antrag zu 2) lässt sich hinreichend bestimmt entnehmen, dass der Kläger festgestellt wissen will, dass die Beklagte verpflichtet ist, dem Kläger sämtliche künftige Schäden zu ersetzen, die dem Kläger aufgrund der missbräuchlichen Datenabgreifung entstanden sind bzw. noch entstehen werden.

2. Daneben liegt auch das für den Klageantrag zu 2) erforderliche Feststellungsinter-

esse gemäß § 256 Abs. 1 ZPO vor. Der Kläger hat die Möglichkeit des Eintritts zukünftiger materieller Schäden hinreichend dargelegt. Das Feststellungsinteresse nach § 256 Abs. 1 ZPO liegt bei einer Verletzung eines absoluten Rechts oder eines vergleichbaren Rechtsguts bereits dann vor, wenn künftige Schadensfolgen möglich sind, auch wenn der Eintritt eines Schadens noch ungewiss ist. Dies wäre nur dann nicht der Fall, wenn aus Sicht des Klägers bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (BeckOK ZPO/Bacher, 46. Ed. 1.9.2022, ZPO § 256 Rn. 24, Rn. 34). Unter Berücksichtigung des Umstandes, dass die im Wege des "Scrapings" erlangten personenbezogenen Daten im Internet veröffentlicht worden sind, erscheint es bei lebensnaher Betrachtung möglich, dass es bei dem Kläger aufgrund der Veröffentlichung der Telefonnummer und weiterer persönlicher Daten wie der Name des Klägers im Internet zu künftigen materiellen Schäden, etwa durch betrügerische Anrufe, kommt.

3. Dem Feststellungsinteresse steht bezogen auf bereits entstandene, dem Kläger aber noch nicht bekannte materielle Schäden nicht der Vorrang der Leistungsklage entgegen. Aufgrund der Veröffentlichung der personenbezogenen Daten des Klägers im Internet ist nicht auszuschließen, dass dessen Daten bereits zu illegalen Zwecken verwendet worden sind, dies dem Kläger allerdings derzeit noch unbekannt geblieben ist. Eine abschließende Bezifferung etwaiger Schäden ist der Klagepartei mithin nicht möglich.

III. Auch die Klageanträge zu 3) a) und 3) b) sind zulässig.

1. Der Klageantrag zu 3) a) ist hinreichend bestimmt.

a) Soweit die Beklagte rügt, dass die Formulierung "*nach dem Stand der Technik möglichen Sicherheitsmaßnahmen*" im Klageantrag zu 3 a) zu unbestimmt sei, führt dieses nicht zur Unzulässigkeit des Antrags.

aa) Ein Verbotsantrag darf im Hinblick auf § 253 Abs. 2 Nr. 2 ZPO zwar nicht derart undeutlich gefasst sein, dass Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts (§ 308 ZPO) nicht erkennbar abgegrenzt sind, sich die Beklagte deshalb nicht erschöpfend verteidigen kann und letztlich die Entscheidung darüber, was der Beklagten verboten ist, dem Vollstreckungsgericht überlassen bleibt. Aus diesem Grund sind Unterlassungsanträge, die lediglich den Wortlaut eines

Gesetzes wiederholen, grundsätzlich als zu unbestimmt und damit unzulässig anzusehen. Etwas anderes kann dann gelten, wenn entweder bereits der gesetzliche Verbotstatbestand selbst entsprechend eindeutig und konkret gefasst oder der Anwendungsbereich einer Rechtsnorm durch eine gefestigte Auslegung geklärt ist oder wenn der Kläger hinreichend deutlich macht, dass er nicht ein Verbot im Umfang des Gesetzeswortlauts beansprucht, sondern sich mit seinem Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert. Die Bejahung der Bestimmtheit setzt in solchen Fällen allerdings grundsätzlich voraus, dass zwischen den Parteien kein Streit darüber besteht, dass das beanstandete Verhalten das fragliche Tatbestandsmerkmal erfüllt. Eine auslegungsbedürftige Antragsformulierung ist jedoch dann hinzunehmen, wenn eine weitergehende Konkretisierung nicht möglich und die gewählte Antragsformulierung zur Gewährung effektiven Rechtsschutzes erforderlich ist (vgl. BGH, Urt. v. 26.1.2017 - I ZR 207/14 = GRUR 2017, 422 m.w.N.). Unzulässigkeit liegt hingegen vor, wenn die Klägerseite seinen Antrag ohne weiteres konkreter fassen kann (vgl. BGH, Urteil vom 11.6.2015 - I ZR 226/13 = GRUR 2016, 88).

bb) Daran gemessen weist der Klageantrag zu 3) a.) eine ausreichende Bestimmtheit auf. Selbst bei einer Benennung derzeitiger möglicher Sicherheitsmaßnahmen würde dies in Anbetracht der technischen Weiterentwicklung alsbald dazu führen, dass die aktuellen Vorkehrungen veralten, sodass der Kläger erneut klagen müsste. Dies stünde einem effektiven Rechtsschutz entgegen. Zudem wird aus der Klagebegründung deutlich, dass der Kläger Sicherheitsstandards verlangt, die möglichen (weiteren) Scraping-Angriffen vorbeugen. Die gesetzlich vorgeschrieben Sicherheitsstandards einzurichten ist jedoch zuvorderst die Aufgabe der Beklagten. Insoweit kann diese nicht von ihren Nutzern die konkrete Benennung der Sicherheitsmaßnahmen verlangen.

2. Dass mit dem Klageantrag zu 3) b) begehrte Anspruchsziel ist ebenfalls hinreichend bestimmt. Das Anspruchsziel wird jedenfalls durch die Klagbegründung hin-

reichend konkretisiert.

C.

Die Klage ist überwiegend begründet.

I. Dem Kläger steht gegen die Beklagte einen Anspruch auf Schadensersatz i.H.v. 600,00 EUR aus Art. 82 Abs. 1 DS-GVO zu (vgl. bereits LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22, juris; LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22; **aA** LG Gießen, Urteil vom 3. November 2022 – 5 O 195/22; LG Bielefeld, Urteil vom 19. Dezember 2022 – 8 O 182/22; LG Essen, Urteil vom 10. November 2022 – 6 O 111/22).

Die Anspruchsvoraussetzungen des Art. 82 Abs. 1 DS-GVO sind im Streitfall gegeben.

Die Beklagte hat gegen Art. 25 Abs. 2 DS-GVO (dazu 2.), gegen Art. 13 Abs. 1 lit. c) DS-GVO (dazu 3.), gegen Art. 32, 24, 5 Abs. 1 lit. f) DS-GVO (dazu 4.), gegen Art. 33 DS-GVO (dazu 5.) und gegen Art. 34 Abs. 1 DS-GVO (dazu 6.) verstoßen. Hingegen liegt ein Verstoß gegen Art. 15 DS-GVO (dazu 7.) nicht vor. Der Klagepartei ist ein immaterieller Schaden entstanden (dazu 8.). Die Verstöße gegen die DS-GVO sind auch kausal für den bei dem Kläger entstandenen Schaden (dazu 9.). Die Beklagte handelte auch schuldhaft (dazu 10.). Die Klagepartei hat sich auch kein Mitverschulden nach § 254 Abs. 1 BGB anrechnen zu lassen (dazu 11.). Infolgedessen steht der Klagepartei ein immaterieller Schadensersatzanspruch i.H.v. 600 € zu (dazu 12.).

1. Nach Art. 82 DS-GVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Gemäß Art. 82 Abs. 1 DS-GVO haftet der Verantwortliche für Schäden wegen „*Verstößen gegen diese Verordnung*“. Grund und damit unabdingbare Voraussetzung der Haftung ist eine Pflichtverletzung, wenngleich es auf einen Schutznormcharakter der verletzten Vorschrift nicht ankommt, der Begriff der Pflichtverletzung also denkbar weit gefasst ist und letztlich jede Verletzung materieller oder formeller Bestimmungen der Verordnung einschließt (siehe Erwägungsgrund 146, wonach sogar die Verletzung delegierter Rechtsakte und nationalen, die Verordnung konkretisierenden Rechts genügt; OLG Stuttgart Urt. v. 31.3.2021 – 9 U 34/21, BeckRS 2021, 6282 Rn. 25, beck-online).

2. Die Beklagte hat gegen Art 25 Abs. 2 DS-GVO verstoßen (so bereits LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 54, juris).

a) Gem. Art. 25 Abs. 2 DS-GVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Durch die standardmäßige Konfiguration von Privatsphäre-Einstellungen ist zu gewährleisten, dass Nutzer ihre Daten nur den Personenkreisen und nur in dem Umfang zugänglich machen, die sie vorab selbst festgelegt haben. Das hat zur Folge, dass alle für die Nutzung nicht erforderlichen personenbezogenen Daten anderen Nutzern nicht zugänglich gemacht werden dürfen, es sei denn, die betroffene Person nimmt entsprechende Änderungen in den Voreinstellungen vor (vgl. Nolte/Werkmeister in Gola/Heckmann, DS-GVO – BDSG 3. Aufl. DS-GVO Art. 25 Rn. 28). Die von Nutzern veröffentlichten Informationen dürfen nicht ohne Einschränkungen der allgemeinen Öffentlichkeit zugänglich gemacht werden, sondern dies muss aktiv erst in den Privatsphäreeinstellungen durch den Nutzer eingerichtet werden (so Hartung in Kühling/Buchner, DS-GVO - BDSG 3. Aufl. DS-GVO Art. 25 Rn. 26). Erforderlich für den Verarbeitungszweck i.S.d Art. 25 Abs. 2 S. 1 sind Daten nur dann, wenn der Verarbeitungszweck sich ohne sie nicht erreichen lässt. Diese Daten darf der Verantwortliche auch durch Voreinstellung verarbeiten. Für solche Daten, die der Verantwortliche nicht notwendig verarbeiten muss, um die legitimen Zwecke der Verarbeitungserlaubnis (Art. 6 DS-GVO) erfüllen zu können, ist ihm der Weg der Voreinstellung demgegenüber verschlossen (Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 25 Rn. 45b).

b) Gemessen an diesen Grundsätzen liegt ein Verstoß der Beklagten gegen Art. 25 Abs. 2 DS-GVO vor (vgl. bereits LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22, juris; LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22; a.A. LG Essen, Urteil vom 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818).

aa) Bei der sogenannten "*Zielgruppenauswahl*" auf der Plattform der Beklagten legt der Nutzer fest, wer einzelne Informationen auf seinem Profil, wie etwa Telefonnummer, Wohnort, Stadt, Beziehungsstatus,

Geburtstag und E-Mail-Adresse, einsehen kann. Dabei ist standardmäßigen die Voreinstellung "*öffentlich*" ausgewählt. Die "*Suchbarkeits-Einstellungen*" der Beklagten legen überdies 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 es die Beklagte ihm, seine Kontakte mit den auf der Plattform hinterlegten Telefonnummern abzugleichen, um die hinter den Nummern stehenden Personen als Freunde hinzuzufügen. Dafür ist nicht erforderlich, dass der andere Nutzer seine Telefonnummer nach der "*Zielgruppenauswahl*" öffentlich gemacht hat. Demnach ist es möglich, Nutzer anhand einer Telefonnummer zu finden, solange ihre "*Suchbarkeits-Einstellung*" für Telefonnummern auf der Standard-Voreinstellung "*Alle*" eingestellt war.

bb) Diese durch die Voreinstellungen ermöglichte Datenerhebung ist nicht für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses erforderlich (Art. 6 Abs. 1 Satz 1 lit. b DS-GVO), ebenso wenig zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 Satz 1 lit. f DS-GVO). Sie mag im Einzelnen je nach Geschmack des Nutzers für die Nutzung der Facebook-Plattform nützlich und behilflich sein. Erforderlich für die Nutzung schlechthin ist sie aber nicht. Diesbezügliche Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten müssen sich auf das absolut Notwendige beschränken. Die Daten sind für eine Nutzung der Facebook-Plattform durch Dritte bzw. für den Betrieb derselben durch die Beklagte nicht unabdingbar (anders für ein Ärztebewertungsportal: BGH, Urteil vom 13.12.2022 – VI ZR 60/21 Rn. 21). Das zeigt sich auch daran, dass sämtliche Voreinstellungen, um die es hier geht, ohne weiteres abgewählt werden können, ohne dass dies ersichtlich der weiteren Vertragsdurchführung entgegensteht (so ausdrücklich KG, Urteil vom 20.12.2019 – 5 U 9/18, BeckRS 2019, 35233 Rn. 39).

cc) Daher kann sich die Beklagte nicht darauf zurückziehen, dass der Zweck der Facebook-Plattform gerade darin bestehe, es Menschen

zu ermöglichen, sich mit Freunden, Familie und Gemeinschaften zu verbinden und dass die Funktionen gezielt so konzipiert worden seien, dass sie den Nutzern helfen, andere zu finden, sich mit ihnen zu verbinden und mit ihnen in Kontakt zu treten. Gerade das widerspricht den Anforderungen der DS-GVO. Die Beklagte darf nicht durch die Definition ihres Leistungsangebots den Umfang der zulässigen Datenverarbeitung unter Hintanstellung der Nutzerinteressen allein an ihrem Interesse an der Vermarktung eines durch die Internetnutzung innerhalb und außerhalb von Facebook generierten Bestands personenbezogener Daten seiner Nutzer ausrichten und über das für die Benutzung des sozialen Netzwerkes erforderliche Maß ausweiten (so BGH, Beschluss vom 23.06.2020 – KVR 69/19 Rn. 110).

dd) Für die Durchführung des Schuldverhältnisses ist es z.B. für den jeweiligen Nutzer nicht erforderlich, dass Name, Profilbild und Titelbild anderen Nutzern helfen, andere zu finden, auch wenn das hilfreich und von vielen gewünscht sein mag. Die Angabe des Geschlechts ist nicht in irgendeiner Art und Weise erforderlich. Die Plattform muss nicht – worauf die Klageerwiderung abstellt – den Nutzer unter Beachtung seines Geschlechts „beschreiben“ (z.B. „*Füge sie als Freundin hinzu*“). Vor diesem Hintergrund ist es ebenso wenig ausreichend, wenn die Beklagte über die Möglichkeiten der Anpassung ihrer Suchbarkeits-Einstellungen und Zielgruppenauswahl informiert. Die Voreinstellung, die die Beklagten hinsichtlich einzelner Aspekte mit „*öffentlich*“ einräumt, läuft den Erfordernissen des Art. 25 Abs. 2 DS-GVO evident zuwider. Auch ist nicht erheblich, wie die Beklagten einen „*Hilfebereich*“ ausgestaltet, da diesen i.d.R. nur derjenige Nutzer anschauen wird, der die Notwendigkeit einer Änderung für sich wahrgenommen hat. Das ist bei einem Nutzer, der die Anmeldeprozedur mit vorgegebenen Einstellungen durchläuft, nicht notwendigerweise der Fall. Denn es kann ein Verhalten, das im Aufruf von Websites und Apps, der Eingabe von Daten in diese Websites und Apps sowie in der Betätigung von in diese eingebundenen Schaltflächen besteht, grundsätzlich auch nicht einem Verhalten gleichgestellt werden, das die sensiblen personenbezogenen Daten des Nutzers i.S. von Art. 9

Abs. 2 lit. e DS-GVO offensichtlich öffentlich macht (vgl. Schlussanträge des Generalanwaltes vom 20.09.2022 in der Rechtssache EuGH – C-252/21, BeckRS 2022, 24109 Rn. 44).

c) Ein Verstoß gegen Art. 25 Abs. 2 DS-GVO kann auch einen Ersatzanspruch auslösen (LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 57 - 65, juris; vgl. Mantz in Sydow/Marsch, DS-GVO | BDSG, 3. Aufl. DS-GVO Art. 25 Rn. 77; Martini in Paal/Pauly, DS-GVO – BDSG 3. Aufl. DS-GVO Art. 25 Rn. 6).

aa) Zwar wird vertreten, dass allein aus einem Verstoß gegen Art. 25 DS-GVO wegen seines organisatorischen Charakters ein Anspruch nach Art. 82 Abs. 1 DS-GVO nicht begründet werden könne (vgl. Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DS-GVO Art. 25 Rn. 3, 34; Kühling/Buchner/Hartung, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 31). Dies wird damit begründet, dass die Vorschrift bereits vor dem eigentlichen Beginn der Datenverarbeitung ihren Regelungscharakter entfalte. Zu diesem, einer tatsächlichen Datenverarbeitung vorgelagerten Zeitpunkt entfalte die DS-GVO jedoch nach Art. 2 Abs. 1 DS-GVO noch keine Wirkung. Die Anwendbarkeit der DS-GVO setze vielmehr eine tatsächliche Verarbeitung personenbezogener Daten voraus (vgl. Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DS-GVO Art. 25 Rn. 7). Ein Anspruch aus Art. 82 DS-GVO setze daher darüber hinaus voraus, dass weitere Verstöße gegen die DS-GVO vorliegen (vgl. Gola/Heckmann/Nolte/Werkmeister a.a.O.; LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 120, juris).

bb) Das Gericht schließt sich jedoch der Auffassung an, wonach auch ein Verstoß gegen Art. 25 Abs. 2 DS-GVO einen Ersatzanspruch auslösen kann (LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, juris; Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 25 Rn. 6; etwas einschränkend Mantz in Sydow/Marsch, DS-GVO | BDSG, 3. Aufl. DS-GVO Art. 25 Rn. 77).

(1) Haftungsbegründend kann eine Datenverarbeitung nämlich auch dann sein, wenn bei dem eigentlichen Verarbeitungsvor-

gang vor- oder nachgelagerte Pflichten verletzt werden. Auch solcherlei Pflichtverstöße können eine Schadensersatzpflicht begründen, wenn diese im Zusammenhang mit einer Datenverarbeitung stehen – und dies letztlich zu einem Schaden auf Seiten der betroffenen Person geführt hat (*Buchner/Wessels* in: ZD 2022, 251, beck-online)

(2) Das wird hier augenscheinlich dadurch, dass bei einer Voreinstellung, die mit Art. 25 Abs. 2 DS-GVO konform gewesen wäre, ein Abgreifen der Mobiltelefonnummer des Klägers so, wie letztlich geschehen, nicht ohne weiteres möglich gewesen wäre. Denn bei einer entsprechenden Voreinstellung der *Suchbarkeits-Einstellungen* die Nummer nicht öffentlich zugänglich gewesen wäre, sondern allenfalls aufgrund einer individuellen Auswahl des Klägers.

3. Darüber hinaus ist die Beklagte der ihr nach Art. 13 Abs. 1 lit. c) DS-GVO auferlegten Informations- und Aufklärungspflicht nicht in vollständigem Umfang nachgekommen (LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 66, juris).

a) Art. 13 DS-GVO verpflichtet den Verantwortlichen, der betroffenen Person bestimmte Informationen über sie betreffende Datenverarbeitungen aktiv, also ohne besondere Aufforderung zur Verfügung zu stellen. Im Einzelnen ergeben sich Informationspflichten aus Art. 13 bei zwei Anlässen, die einander zeitlich nachgelagert sind: Gemäß Abs. 1 und Abs. 2 muss der Verantwortliche bestimmte Informationen zur Verfügung stellen, wenn er Daten bei der betroffenen Person erhebt. Gemäß Abs. 3 entstehen weitere Informationspflichten, wenn der Verantwortliche die erhobenen Daten zu einem anderen Zweck als dem Erhebungszweck weiterverarbeiten will. Nach Art. 13 Abs. 1 lit. c) DS-GVO hat der Verantwortliche der betroffenen Person die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung mitzuteilen. Die Angaben müssen vollständig und so detailliert sein, dass die betroffene Person sich ein Bild davon machen kann, mit welchen Datenverarbeitungen sie zu rechnen hat. Mit dieser Information legt der Verantwortliche den Verarbeitungszweck oder die Verarbeitungszwecke gegenüber der betroffenen Person verbindlich fest

(Kühling/Buchner/Bäcker, 3. Aufl. 2020, DS-GVO Art. 13 Rn. 25).

b) Hiergegen hat die Beklagte verstoßen. Sie hat die Klagepartei zum Zeitpunkt der Datenerhebung seiner Mobilfunknummer nicht ausreichend über die Zwecke der Verarbeitung dieser Nummer aufgeklärt. Nach Art. 13 Abs. 1 lit. c) DS-GVO sind indes die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, zum Zeitpunkt der Erhebung der Daten mitzuteilen. Dem hat die Beklagte zumindest hinsichtlich der Verwendung der Mobilfunknummer für das von ihr verwendete Contact-Import-Tool nicht genügt (LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, juris).

aa) Das Contact-Import-Tool ermöglicht einem Nutzer z.B. einen Abgleich der in seinem Smartphone gespeicherten Kontakte mit auf Facebook registrierten Nutzerprofilen, die ihr Profil mit einer Mobilfunknummer verknüpft haben. Durch die Eingabe einer beliebigen Mobilfunknummer wird dem Benutzer ermöglicht, das mit der Mobilfunknummer verknüpfte Benutzerprofil als "*Freunde*" hinzuzufügen.

bb) Aus den vorgelegten Unterlagen ist nicht ersichtlich, dass insoweit durch die Beklagte eine irgendwie geartete Aufklärung erfolgt wäre. Vielmehr wird durch die Information *„Möglicherweise verwenden wir deine Mobilnummer für diese Zwecke: … Um dir Personen, die du kennen könntest, vorzuschlagen, damit du dich mit ihnen auf Facebook verbinden kannst*“ (Bl. 102 und Anl. B6) gerade ein gegenteiliger Eindruck erweckt. Es wird nicht darüber informiert, dass andere den Kläger als Nutzer finden können, sondern darüber, dass dem Kläger seine Telefonnummer nützlich sein kann, andere Facebook-Nutzer zu finden. Das eine mag zwar mit dem anderen unmittelbar zusammenhängen, indes gestaltet sich die Information der Beklagten selektiv und damit unvollständig. Das wird auch nicht durch den anschließenden Hinweis, dass man kontrollieren könne, wer die eigene Telefonnummer sehen könne, geheilt, zumal auch in der vorgelegten „*Datenrichtlinie*“ der Anlage B 9 in der Rubrik „*Wie werden diese Informationen geteilt?*“ hierauf nicht hingewiesen wird.

cc) Angesichts des Vorstehenden kann hier auch nicht von einer wirksa-

men Einwilligung des Klägers i.S. von Art. 6 Abs. 1 lit. a DS-GVO ausgegangen werden, ebenso wenig ist das Auffinden über das Contact-Import-Tool für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich (Art. 6 Abs. 1 Satz 1 lit. d DS-GVO; LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, juris; LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, juris).

c) Ein Verstoß gegen Art. 13 Abs. 1 lit. c) DS-GVO kann einen Ersatzanspruch nach Art. 82 Abs. 1 DS-GVO auslösen (vgl. nur Schmidt-Wudy in BeckOK-Datenschutzrecht, Stand: 01.11.2022 DS-GVO Art. 13 Rn. 18; Franck in Gola/Heckmann, DS-GVO – BDSG, 3. Aufl. DS-GVO Art. 13 Rn. 64; LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 72, juris; a.A. LG Essen, Urteil vom 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818).

4. Die Beklagte als Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO verstieß aufgrund unzureichender Sicherheitsmaßnahmen bezüglich der Nutzung des Contact-Import-Tool auch gegen Art. 32, 24, 5 Abs. 1 lit. f) DS-GVO (LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –juris).

a) Gemäß Art. 32 Abs. 1 Hs. 1 DS-GVO haben der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

b) Art. 32 DS-GVO regelt die Pflicht des Verantwortlichen und des Auftragsverarbeiters, bestimmte technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Schutzniveau im Hinblick auf die verarbeiteten personenbezogenen Daten zu gewährleisten. Er konkretisiert die als Generalauftrag gestalteten Datensicherheitsmaßnahmen des Art. 24 DS-GVO und dient damit u.a. der Gewährleistung der Absicherung der Datenschutzgrundsätze der Vertraulichkeit und Integrität nach Art. 5 Abs. 1 f) DS-GVO.

Zielrichtung ist ein umfassender Schutz der für die Verarbeitung von personenbezogenen Daten genutzten Systeme, also im Kern die Datensicherheit (Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 1). Das Gebot soll insbesondere personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen davor schützen, dass Dritte diese unbefugt oder unrechtmäßig verarbeiten oder es unbeabsichtigt zu einem Verlust, einer Zerstörung oder Schädigung der Daten kommt (Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 32 Rn. 2; vgl auch Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 2). Bei der Implementierung von geeigneten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DS-GVO sind dabei der Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen als Faktoren zu berücksichtigen. Dies bedeutet allerdings nur, dass sie in die Verhältnismäßigkeitsprüfung einzustellen, jedoch nicht notwendigerweise absolut zu befolgen sind (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 14). Die DS-GVO legt zur Bemessung der Geeignetheit der Maßnahmen insbesondere weiter fest, dass diese ein dem Risiko der Verarbeitung angemessenes Schutzniveau bieten müssen. Dabei kommt es letztlich darauf an, wie groß die Risiken sind, die den Rechten und Freiheiten der betroffenen Person drohen und wie hoch die Wahrscheinlichkeit eines Schadenseintritts ist. Damit ergibt sich, dass die Maßnahmen umso wirksamer sein müssen, je höher die drohenden Schäden sind (Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 4; Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 4). Dies wird vor allem anhand der Sensibilität der Daten und der Wahrscheinlichkeit eines Schadeneintritts bestimmt (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 41). Art. 32 Abs. 1 DS-GVO verpflichtet den Verantwortlichen und Auftragsverarbeiter aber nicht zu einem absoluten Schutz(niveau) der Daten. Das Schutzniveau muss vielmehr, je nach Verarbeitungskontext, dem Risiko bezüglich der Rechte und Freiheiten der betroffenen Personen im Einzelfall angemessen sein. Dies bedeutet gleichzeitig, dass das Risiko nicht völlig ausgeschlossen werden kann und dies auch nicht Ziel der umzusetzenden Maßnahmen ist (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO

Art. 32 Rn. 11; vgl. auch Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 3). Zur Bestimmung des angemessenen Schutzniveaus sind gem. Art. 32 Abs. 2 DS-GVO 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. Diese sind zwingend in die Risikobetrachtung einzubeziehen (Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 5). Ausweislich des Erwägungsgrunds 76 zur DS-GVO sollten die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt (zum Ganzen LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 77 - 83, juris)

c) Diesen Anforderungen genügten die beklagtenseits behaupteten Schutzmaßnahmen nicht (LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 – juris).

aa) Die von ihr behaupteten "*Anti-Scraping-Maßnahmen*" sind selbst, wenn der Beweis zum Vorliegen der Maßnahmen für den streitgegenständlichen Zeitraum geführt werden würde, für sich allein nicht geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das CIT ermöglicht einen unbefugten Zugang i.S.d. Art. 32 Abs. 2 DS-GVO. Beim Zugang zu Daten geht die entscheidende Aktivität vom Empfänger der Daten aus. Der Verantwortliche muss lediglich durch die Ausgestaltung der technischen Bedingungen die Daten grundsätzlich zum Abruf durch Dritte ermöglichen. Dieses Bereithalten der Daten zum Abruf kann z.B. durch das Einräumen von Zugriffsrechten im Rahmen von Netzwerken oder durch Einstellung in eine Datenbank, auf die auch Dritte zugreifen können, erfolgen (Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 34). So liegt der Fall hier, da das CIT zweckwidrig nicht zum Auffinden von persönlichen Kontakten auf

der Facebook-Plattform, sondern entgegen der Nutzungsbedingungen der Beklagten zu Missbrauchszwecken genutzt werden konnte und wurde. Es wird Dritten eine Zuordnung von Telefonnummer zum Nutzerprofil ermöglicht. Dementsprechend wird in Erfahrung gebracht, welche Person hinter der Telefonnummer steht. Hierbei können durch den Rückgriff auf das Nutzerprofil gleichzeitig weitere Informationen über die Person eingeholt werden. Dies birgt für die Nutzer das Risiko von gezielten Phishing-Attacken, Identitätsdiebstahl und weiteren Missbrauch der Daten und damit dem Eintritt von materiellen oder immateriellen Schäden.

bb) Dieses zwingend zu berücksichtigende Risiko bedingt bereits, dass der Maßstab für die Bestimmung der Angemessenheit des Schutzniveaus entsprechend hoch anzusetzen ist. Dies begründet sich unter anderem daraus, dass das CIT-Verfahren nicht eine reine Erhebung oder Speicherung von Daten durch die Beklagten darstellt. Auch handelt es sich bei den Daten nicht um ohnehin öffentlich einsehbare Daten. Vielmehr wird Dritten ein Zugang zu diesen, insbesondere der Telefonnummer des Nutzers, gewährt. Es erfolgt eine Verknüpfung der zuvor nicht öffentlich einsehbaren Telefonnummer zu den weiteren Daten des Nutzers auf der Plattform der Beklagten. Die Gefahr einer Veröffentlichung aller zusammengetragenen Daten, darunter insbesondere die Verknüpfung von Telefonnummer und Name, ist, wie der vorliegende Datenscraping-Fall aufzeigt, besonders hoch. Dies war auch der Beklagten bekannt. Für sie ist ausweislich ihres Artikels "*Die Fakten zu Medienberichten über Facebook-Daten*" vom 06.04.2021 (Anlage B10) Scraping "*eine gängige Taktik*". Die Beklagte musste sich daher darüber bewusst sein, dass Maßnahmen für ein angemessenes Schutzniveau für die personenbezogenen Daten hinsichtlich des Risikos von Scraping zu treffen waren.

cc) Soweit die Beklagte nun darauf abstellt, dass sie gegen Scraper mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren vorgehe, kommt diese Maßnahme bereits erst dann zu tragen, wenn ein Datenscraping tatsächlich eingetreten ist. Die Daten sind in

diesem Stadium bereits entwendet worden. Eine Veröffentlichung oder anderweitiger Missbrauch kann in diesem Stadium praktisch nicht mehr verhindert werden.

dd) Des Weiteren ist die behauptete teilweise Einschränkung des CIT auch nach dem Beklagtenvorbringen erst nach dem streitgegenständlichen Vorfall eingeführt worden. Auch die Beschäftigung eines Teams von Datenwissenschaftlern, -analysten und Softwareingenieuren zur Bekämpfung von Scraping, Übertragungsbeschränkungen sowie CAPTCHA-Abfragen genügen den Anforderungen des Art. 32 DS-GVO im vorliegenden Fall allein nicht. Die Beklagte legt diesbezüglich bereits nicht dar, wie es bei den - aus ihrer Sicht im hiesigen Verfahren ausreichenden - Sicherheitsmaßnahmen dennoch zum streitgegenständlichen Datenscraping kommen konnte. Aufgrund des hohen Risikopotenzials, das von einem Missbrauch des CIT ausgeht, waren jedoch weitergehende Maßnahmen für ein angemessenes Schutzniveau erforderlich. CAPTCHA-Abfragen werden z.B. bereits bei geringeren Risiken im Umgang mit personenbezogenen Daten eingesetzt. Die Arbeit des EDM-Teams entfaltet des Weiteren ausweislich des Vorbringens der Beklagten in der Regel erst während eines bereits begonnen Scraping-Prozesses ihre Wirkung, sodass Scraper in diesem Zeitpunkt bereits Datensätze erlangt haben. Außerdem ist es Scrapern möglich, Übertragungsbeschränkungen zu umgehen. Daher wären weitergehende Maßnahmen notwendig gewesen. Diese hätten beispielsweise so ausgestaltet werden können, dass weitergehende Informationen neben der Telefonnummer für die Nutzung des CIT anzugeben sind. Es kann ein Missbrauch des CIT in Form von Datenscraping dann zumindest erschwert werden, so z.B. durch die weitere Angabe eines Vornamens, der sich neben der Telefonnummer ebenfalls hochladen ließe. So würden weitere Variablen hinzutreten, die auf eine den Nutzungsbedingungen entsprechende Nutzung des CIT hindeuten. Datenscraper hingegen werden vor das Problem gestellt, das neben Variablen in Form von Zahlen auch Variablen in Form von Worten hinzutreten. Dies erschwert ein automatisiertes Verfahren. Zudem wäre ein höherer Datenverkehr erforderlich, der

ggf. den bereits behaupteten Maßnahmen der Übertragungsbeschränkungen und der Arbeit des EDM-Teams einen größeren Nutzen verleiht. Dies würde auch nicht dem von der Beklagten verfolgten Zweck zuwiderlaufen. Denn laut der Beklagten sei es Hauptzweck der Plattform, andere Nutzer zu finden und mit diesen in Kontakt zu treten. Das CIT ermöglicht dementsprechend Nutzer ihre Kontakte ihrer Mobilgeräte hochzuladen und anhand der Telefonnummern die Profile ihrer Kontakte zu finden. Weitergehende Angaben laufen diesen Absichten nicht zuwider, zumal diese ggf. ebenfalls über das CIT automatisch über die Kontaktliste des Mobilgeräts des Nutzers in Erfahrung gebracht werden könnte.

ee) Diese oder andere Schutzmaßnahmen, wie die klägerseits angeführten Begrenzungen der abgleichbaren Rufnummern oder Nutzung nur für Freunde von Freunden, implementierte die Beklagte jedoch vor oder während des streitgegenständlichen Datenscrapings nicht. Erst im Nachgang implementierte die Beklagte eine vergleichbare Sicherheitsmaßnahme, den sog. "*Social Connection Check*". Die Beklagte nahm damit vielmehr erst den Vorfall zum Anlass ihre Schutzmaßnahmen zu evaluieren und traf ausweislich ihres als Anlage B11 vorgelegten Artikel "*Scraping nach Zahlen*" vom 19.05.2021 "*eine Reihe von Verbesserungen*" im September 2019 (so insgesamt ausdrücklich und zutreffend LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 84 - 93, juris).

d) Ein Verstoß gegen Art. 32, 24, 5 Abs. 1 f) DS-GVO kann bei Vorliegen der übrigen Anspruchsvoraussetzungen einen Anspruch nach Art. 82 DS-GVO begründen (Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 40a; Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 31; LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 94, juris)

5. Die Beklagte hat zudem ihre Meldepflicht aus Art. 33 DS-GVO verletzt.

a) Nach Art. 33 Abs. 1 DS-GVO hat der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nachdem ihm die Verletzung bekannt wurde der gem. Art. 55

DS-GVO zuständigen Aufsichtsbehörde zu 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 DS-GVO festgelegt.

b) Dem ist die Beklagte vorliegend nicht nachgekommen.

aa) Unstreitig hat die Beklagte die zuständige Aufsichtsbehörde im Sinne des Art. 55 DS-GVO nicht über den "Scraping"-Vorfall informiert.

bb) Zudem liegt eine Verletzung des Schutzes personenbezogener Daten vor.

(1) Nach der Begriffsbestimmung in Art. 4 Nr. 12 DS-GVO fällt darunter eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Erfasst ist damit im weitesten Sinn jede objektive Schutzverletzung, unabhängig davon, ob diese beabsichtigt war oder nicht, wie etwa Datenpannen, -lecks, Hackerangriffe oder Datendiebstahl (Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DS-GVO Art. 33 Rn. 5; Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 33 Rn. 6 m.w.N.). Eine Verletzung liegt auch dann vor, wenn im Rahmen bestehender Zugriffsrechte Daten zweckentfremdet werden (Spindler/Schuster/Laue, DS-GVO Art. 33 Rn. 7). Nach der Stellungnahme 3/2014 der Artikel-29-Datenschutzgruppe erfolgt eine Kategorisierung in unterschiedliche Arten von Verletzungen der Sicherheit, namentlich der "*Verletzung der Vertraulichkeit*", bei der es zu einer unbefugten oder unbeabsichtigten Offenlegung von oder zu einem Zugriffs auf personenbezogene Daten kommt, der "*Verletzung der Verfügbarkeit*", bei der es zu einem unbeabsichtigten oder unbefugten Verlust von,

Zugriff auf, oder Vernichtung von personenbezogenen Daten kommt, sowie der "*Verletzung der Integrität*", bei der es zu einer unbefugten oder unbeabsichtigten Veränderung von personenbezogenen Daten kommt. Eine Verletzung der Vertraulichkeit von Daten liegt auch immer dann vor, wenn die Ebene, auf der die Daten zur Verfügung stehen, geändert wurde (Artikel-29-Datenschutzgruppe, Stellungnahme 3/2014 on Personal Data Breach Notification, WP 213, S. 18).

(2) Eine solche Verletzung der Vertraulichkeit liegt vor.

(a) Denn unabhängig davon, dass Name, Facebook-ID und Geschlecht des Klägers aufgrund seiner Privatsphäre-Einstellungen öffentlich waren und die Handynummer durch die frei zugängliche Nutzung des CIT-Tools mit diesen Daten verknüpft werden konnte, liegt vor dem Hintergrund des massenhaften "Scrapings" und der Veröffentlichung der Daten in "Darknet" eine Zweckentfremdung im Rahmen der grundsätzlich gewährten Zugriffsrechte vor. Der "Scraping"-Vorfall ist allein aufgrund seines Ausmaßes mit Datenpannen, -lecks, Hackerangriffe oder Datendiebstahl gleichzusetzen. Dies zeigt sich auch darin, dass ein solches Vorgehen nach den Nutzungsbedingungen untersagt ist und - so behauptet jedenfalls die Beklagte selbst - Sicherheitsmaßnahmen gegen derartige Vorfälle geschaffen wurden. Durch die Veröffentlichung der Daten im "Darknet" wurde zudem die Ebene, auf denen die Daten zur Verfügung stehen, geändert.

(b) Dass die Leitlinien des Europäischen Datenschutzausschusses das "Scraping" selbst nicht ausdrücklich als eines der Beispiele für eine Verletzung des Schutzes persönlicher Daten nennen ist unbeachtlich, da diese ausdrücklich nicht abschließend sind.

cc) Eine Einschränkung der Meldepflicht nach Art. 33 Abs. 1 DS-GVO ist nicht gegeben. Es ist nicht vorauszusehen, dass die Verletzung des Schutzes personenbezogener Daten nicht zu einem Risiko für die Rechte und Freiheiten des Klägers führt. Ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht gemäß des Erwägungsgrundes 85, wenn ihnen der Verlust der Kontrolle über ihre Daten, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile drohen. Dies ist der Fall (zum ganzen so ausdrücklich bereits LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 95 - 103, juris).

c) Ein Verstoß gegen die Meldepflicht nach Art. 33 DS-GVO kann ebenfalls - bei Vorliegen der übrigen Voraussetzungen - eine Schadensersatzpflicht gem. Art. 82 DS-GVO begründen (LG Essen ZD 2022, 50; Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 33 Rn. 27; Spindler/Schuster/Laue DS-GVO Art. 33 Rn. 24). Die Vorschrift dient sowohl dem Schutz des Betroffenen, als auch der Ermöglichung von Maßnahmen zur Eindämmung und Ahndung der Rechtsverletzung durch die Aufsichtsbehörde. Insofern genügt bereits ein solch formeller Verstoß gegen die DS-GVO zur Begründung eines Schadensersatzanspruchs dem Grunde nach (vgl. LG Essen ZD 2022, 50; BeckOK DatenschutzR/Quaas, 41. Edition Stand: 01.08.2022, DS-GVO Art. 82 Rn. 14; LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 104, juris).

6. Auch ein Verstoß gegen Art. 34 Abs. 1 DS-GVO liegt vor.

a) Hiernach hat 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, zu benachrichtigen. Die Benachrichtigung muss grundsätzlich gegenüber der betroffenen Person i.S.v. Art. 4 Nr. 1 DS-GVO erfolgen. Insofern bedarf es der Bestimmung der durch den Vorfall konkret betroffenen Personen. Der in Art. 34 Abs. 1 Hs. 2 DS-GVO gewählte Singular "Person" verdeut-

licht, dass in den Fällen des Art. 34 regelmäßig eine individuelle Information bezüglich des Datenschutzvorfalls erfolgen muss (Gola/Heckmann/Reif DS-GVO Art. 34 Rn. 4).

b) Eine solche individualisierte Information des Klägers ohne schuldhaftes Verzögern nach Offenbarung der Verletzung des Schutzes personenbezogener Daten im Jahr 2019 hat die Beklagte nicht vorgenommen.

c) Die hier vorliegende Verletzung des Schutzes personenbezogener Daten hat voraussichtlich auch ein hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen zur Folge. Ein solches Risiko besteht dann, wenn zu erwarten ist, dass bei ungehindertem Geschehensablauf mit hoher Wahrscheinlichkeit ein Schaden für die Rechte und Freiheiten des Betroffenen eintritt. In einem solchen Fall ist es nicht maßgeblich, ob die Datenschutzverletzung auch zu einen besonders hohen Schadensumfang führt (vgl. BeckOK DatenschutzR/Brink, DS-GVO Art. 34 Rn. 25.).

d) Die Benachrichtigungspflicht ist im hiesigen Fall auch nicht entbehrlich.

aa) Nach Art 34 Abs. 3 a) DS-GVO ist eine Benachrichtigung nicht erforderlich, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt hat, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung. Entsprechend der Ausführungen zu dem Verstoß gegen Art. 32 DS-GVO hat die Beklagte vorliegend keine geeigneten Sicherheitsvorkehrungen getroffen.

bb) Ferner ist eine Benachrichtigung nicht gem. Art. 34 Abs. 3 c) DS-GVO entbehrlich. Dafür müsste die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden sein. In diesem Fall hätte stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden. Zwar kann sich aus einer Vielzahl an betroffenen Personen ein unverhältnismäßiger Zeit- bzw. Kostenaufwand erge-

ben. Allerdings kann von einem unverhältnismäßigen Aufwand nicht ausgegangen werden, wenn die betroffenen Personen bekannt sind und deren E-Mailadressen vorliegen. Im Übrigen setzt die öffentliche Bekanntmachung voraus, dass die Betroffenen vergleichbar wirksam informiert werden. Ob eine Publikation des Vorfalls auf der eigenen Homepage ausreicht, hängt davon ab, inwiefern der Internetauftritt vom betroffenen Personenkreis regelmäßig besucht wird. Jedenfalls darf die Bekanntmachung des Vorfalls auf der Website nicht versteckt werden. Es bedarf eines an herausragender Stelle platzierten Banners bzw. einer entsprechend deutlichen Meldung. Gegebenenfalls muss die Information sowohl über digitale, als auch über analoger Kanäle erfolgen. Demnach ist die ausschließliche Benachrichtigung durch eine Pressemitteilung oder in einem Unternehmensblog kein wirksames Mittel, um die betroffenen Personen von einer Datenschutzverletzung in Kenntnis zu setzen (Gola/Heckmann/Reif DS-GVO Art. 34 Rn. 17 m.w.N.).

cc) Nach dem Vortrag der Beklagten genügen ihre Maßnahmen nicht den Anforderungen des Art. 34 DS-GVO. Zum einen sind die betroffenen Personen und ihre E-Mailadressen bekannt, sodass schon nicht von einem unverhältnismäßigen Aufwand in Bezug auf eine individuelle Benachrichtigung auszugehen ist. Im Übrigen hat die Beklagte lediglich darauf verwiesen, dass sie am 06.04.2021 in dem Artikel "Die Fakten zu Medienberichten über Facebook-Daten" erläutert habe, dass die Daten nicht durch einen Hack erlangt worden seien, sondern es sich um öffentlich einsehbare Informationen handele. Diese Mitteilung erfolgte weder rechtzeitig, noch auf einem probaten Weg, um den Anforderungen an eine öffentliche Bekanntmachung zu genügen. Die Informationen, die die Beklagte im Rahmen der Privatsphäre-Einstellungen zum Thema "Scraping" zur Verfügung stellte, stellen schon keinen Bezug zu dem konkreten Vorfall her und sind im Übrigen nicht an einer herausragender Stelle platziert. Vielmehr hätte die Bekanntmachung auf der Startseite eines jeden Nutzers erfolgen müssen (LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 105 - 112, juris).

e) Auch ein Verstoß gegen Art. 34 Abs. 1 DS-GVO ist geeignet, einen Schadensersatzanspruch zu begründen (OLG Frankfurt a.M. GRUR 2022, 1252; Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 34 Rn. 32; Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Auflage 2019, § 11 Rn. 4; LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 106, juris).

7. Ein Verstoß gegen Art. 15 Abs. 1 DS-GVO liegt hingegen nicht vor.

a) Offen bleiben kann insoweit, ob eine bloße Verletzung einer Auskunftspflicht nach Art. 15 DS-GVO überhaupt einen Schadensersatzanspruch begründen kann (vgl. Bejahend OLG Köln, Urteil vom 14.07.2022 – 15 U 137/21, GRUR-RS 2022, 17897 Rn. 15; Franck, ZD 2021, 680; verneinend LG Bonn, Urteil vom 01.07.2021 – 15 O 372/20, BeckRS 2021, 18275; Kreße in Sydow/Marsch, DS-GVO | BDSG, 3. Aufl. DS-GVO Art. 82 Rn. 13). Für die Möglichkeit eines Schadensersatzanspruches spricht unter anderem, dass Art. 82 Abs. 1 DS-GVO dem Wortlaut nach weit gefasst ist. Dagegen wird eingewandt, dass die Vorschrift unter Berücksichtigung des Art. 82 Abs. 2 DS-GVO und deren Erwägungsgrunds 146 dahingehend auszulegen ist, dass von der Schadensersatzpflicht lediglich solche Schäden umfasst sind, die auf Grund einer Verarbeitung entstehen. Denn gem. Art. 82 Abs. 2 DS-GVO hafte jeder an einer Verarbeitung beteiligte Verantwortliche für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Dies stehe im Einklang mit Erwägungsgrund 146, in dem es lautet „*Der Verantwortliche oder der Auftragsverarbeiter sollte Schäden, die einer Person auf Grund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen*“ (so auch Ehmann/Selmayr/Nemitz, 2. Aufl. 2018, DS-GVO Art. 82 Rn. 8; LG Bonn BeckRS 2021, 18275). Die verzögerliche Reaktion auf ein Auskunftsverlangen dürfte nach dieser Auffassung jedoch keine Verarbeitung personenbezogener Daten i.S.d. DS-GVO darstellen. Datenverarbeitung bezeichnet gem. Art. 4 Nr. 2 DS-GVO nur jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das

Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (LG Düsseldorf, Urteil vom 28.10.2021 – 16 O 128/20; LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 122, juris).

b) Letztendlich kann dies dahinstehen, da die Beklagte einen etwaigen Anspruch nach Art. 15 DS-GVO jedenfalls rechtzeitig erfüllt hat.

aa) Der Kläger hat sich am 27.01.2022 an die Beklagte „*wegen der im April 2021 bekannt gewordenen Onlineveröffentlichung eines Datensatzes mit Facebook-Profilen von Nutzern*“ gewandt und konkrete Fragen formuliert, hinsichtlich derer er eine Erklärung der Beklagten wünsche (S. 11, Anl. K 1). Diese betreffen ausschließlich die abhanden gekommenen – gescrapten – personenbezogenen Daten und nicht die Frage, über welche personenbezogenen Daten die Beklagte überhaupt verfügt.

bb) Dieses Auskunftsverlangen, das sich aus Art. 15 DS-GVO ableiten lässt, hat die Beklagte mit dem (Anwlats-)Schreiben vom 25.02.2022 (Anl. B16) erfüllt.

(1) Eine Erfüllung ist dann anzunehmen, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen (vgl. nur BGH, Urteil vom 03.09.2020 – III ZR 136/18 Rn. 43).

(2) Die Beklagte hat mitgeteilt, dass sie eine Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten enthielten, nicht habe. Auf Grundlage der bislang vorgenommenen Analysen sei es ihr jedoch gelungen, der Nutzer-ID des Klägers die folgenden Datenkategorien zuzuordnen, die nach ihrem Verständnis in den durch Scraping abgerufenen Daten erschienen und mit den auf dem Facebook-Profil des Klägers verfügbaren Informationen übereinstimmten: Nutzer-ID, Vorname, Nachname,

Land, Geschlecht. Daneben sei auch die Telefonnummer „*nach unserem Verständnis in den durch Scraping abgerufenen Daten enthalten*“. Zudem hat die Beklagte erläutert, wie das Daten-Scraping erfolgte. Damit hat die Beklagte zum Ausdruck gebracht, dass sie die von ihr geschuldeten Angaben mitgeteilt hat (LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 81 - 86, juris).

8. Der Klagepartei ist ein immaterieller Schaden entstanden.

a) Der Begriff des Schadens ist nach Erwägungsgrund (EG) 146 S. 3 weit und unter Berücksichtigung der Ziele der DS-GVO auszulegen. Der Anspruch soll nach EG 146 S. 6 einen vollständigen und wirksamen Ersatz des erlittenen Schadens sicherstellen, was das Erfordernis einer weiten Auslegung des Schadenbegriffs unterstreicht. Der Begriff des Schadens in Art. 82 DS-GVO ist autonom auszulegen. Daher kommt es nicht darauf an, ob bestimmte Schadenspositionen im nationalen Recht nicht als Schaden angesehen werden. Entsprechend sind sowohl materielle als auch immaterielle Schäden zu ersetzen.

b) Die bisherige deutsche Rechtsprechung, die immateriellen Schadensersatz überhaupt nur bei schwerwiegenden Persönlichkeitsrechtsverletzungen zugesprochen hat, ist insoweit nicht anwendbar. Da der Begriff des Schadens in Art. 82 ein europarechtlicher ist, darf nicht auf nationale Erheblichkeitsschwellen oder andere Einschränkungen abgestellt werden. Einen Ausschluss vermeintlicher Bagatellschäden sieht das Gesetz nicht vor. Es fehlt gerade bei den Erwägungsgründen zum Schadensersatz der in EG 148 S. 2 zu findende Hinweis auf geringfügige Verstöße, bei denen ausnahmsweise auf die Verhängung einer Geldbuße verzichtet werden kann. Es ist zwar richtig, dass nicht jeder Verstoß gegen die DS-GVO allein aus generalpräventiven Gründen zu einem Schadensersatzanspruch führt. Doch soweit es nicht um reine Formfehler wie Verstöße gegen Dokumentationspflichten geht, geht mit der Verletzung datenschutzrechtlicher Normen letztlich immer ein immaterieller Schaden einher. Einen Schaden erst dann anzunehmen, wenn es etwa zu einer mit einer unrechtmäßigen Zugänglichmachung von Daten liegenden (öffentlichen) „*Bloßstellung*“, einem Identitätsdiebstahl, einer Weiter-

gabe intimer Informationen oder einer anderen „*ernsthaften Beeinträchtigung für das Selbstbild oder Ansehen einer Person*“ kommt, und ein „*besonderes immaterielles Interesse*“ zu verlangen, das über den allein durch die Verletzung an sich hervorgerufenen Ärger oder sonstige Gefühlsschäden hinausgeht, verkennt den autonom und nach EG 146 ausdrücklich weit auszulegenden Begriff des Schadens. Erst recht geht es nicht an, bei kleineren fahrlässigen Verstößen einen immateriellen Schaden komplett abzulehnen, nur weil ein Unternehmen gute Datenschutz-Managementstrukturen hat (zu Vorstehenden insgesamt Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 17-18d mwN).

c) Der Schaden kann auch bereits etwa in dem unguten Gefühl liegen, dass personenbezogene Daten Unbefugten bekannt geworden sind (vgl. Dickmann r+s 2018, 345 (348); Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82), insbesondere wenn nicht ausgeschlossen ist, dass die Daten unbefugt weiterverwendet werden – ja bereits in der Ungewissheit, ob personenbezogene Daten an Unbefugte gelangt sind. Unbefugte Datenverarbeitungen können zu einem Gefühl des Beobachtetwerdens und der Hilfslosigkeit führen, was die betroffenen Personen letztlich zu einem reinen Objekt der Datenverarbeitung degradiert. Den Kontrollverlust nennt EG 75 ausdrücklich als „insbesondere“ zu erwartenden Schaden; denknotwendig kann es sich dabei regelmäßig nur um einen immateriellen Schaden handeln. Spezifische Angaben, wie konkret sich der Kontrollverlust auf die Persönlichkeit und auf das Leben der betroffenen Person ausgewirkt hat, sind nicht erforderlich. Als mögliche Schäden kommen darüber hinaus beispielsweise auch Ängste, Stress sowie Komfort- und Zeiteinbußen in Betracht, die sich vor allem nach den im konkreten Fall erforderlichen Abhilfemaßnahmen richten (zu Vorstehenden insgesamt Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 17-18d).

d) Immaterielle Schäden können ferner aus den verschiedensten für sich genommen rechtswidrigen Verarbeitungen personenbezogener Daten resultieren: etwa die unrechtmäßige Videoüberwachung, die unzulässige Observierung durch eine Detektei, die unzulässige Einbindung von Dritt-Inhalten auf Websites und die damit verbundene Offenlegung der Nutzung an den

Dritt-Anbieter – verstärkt, wenn dadurch die Erstellung von websiteübergreifenden Nutzungsprofilen (Tracking) ermöglicht wird – oder auch das unzulässige interne Verarbeiten von Negativangaben durch eine Auskunftei ohne Weitergabe an Dritte. Aber auch das Unterlassen der Information nach den Art. 13, 14 (vgl. Wirthensohn ZD 2019, 562 (566); Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82) kann ebenso wie Fehler bei der Information dazu führen, dass betroffene Personen überhaupt nicht wissen, dass ihre personenbezogenen Daten verarbeitet werden, sodass sie um die Möglichkeit gebracht werden, die sie betreffenden Daten zu kontrollieren und ihre Betroffenenrechte etwa auf Auskunft, Löschung oder Widerspruch geltend zu machen, was nach EG 75 einen (notwendig immateriellen) Schaden darstellt (zu Vorstehenden insgesamt Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 17-18d).

e) Gemessen an diesen Grundsätzen ist bei der Klagepartei ein immaterieller Schaden eingetreten.

Jedenfalls kann der Schaden - wie gezeigt - bereits in der Ungewissheit bestehen, ob personenbezogene Daten an Unbefugte gelangt sind. Zudem ist durch die unstreitig erfolgte, unbefugte, Erlangung der Daten durch Dritte beim Kläger ein Kontrollverlust seiner Daten eingetreten (EG 75). Dies genügt für den Eintritt eines Schadens (zur Höhe des immateriellen Schadens sogleich unten unter 12.).

9. Die gemäß den vorstehenden Ausführungen festgestellten Verstöße gegen die DS-GVO sind auch kausal für den bei dem Kläger entstandenen Schaden.

a) Der Verantwortliche haftet nach Art. 82 DS-GVO lediglich für kausal durch die rechtswidrige Verarbeitung verursachte Schäden (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 41). Eine Mitursächlichkeit des Verstoßes genügt jedoch (OLG Stuttgart ZD 2021, 375; LG Köln ZD 2022, 52 Rn. 21).

b) Dies ist der Fall.

aa) Der Verstoß der Beklagten gegen Art. 25 Abs. 2 DS-GVO ist (mit-)ursächlich für das „*Scraping*“ der Daten des Klägers. Aufgrund des Verstoßes gegen die Verpflichtung durch datenschutzfreundliche Vorein-

stellungen ist es erst möglich geworden, dass (öffentliche) personenbezogene Daten von Dritten abgegriffen worden sind, die im Fall einer anderen Voreinstellung (“*Nur ich*“) nicht durch „*Sraping*“ hätten abgegriffen werden können (ähnlich auch LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 98, juris).

bb) Die Verletzung der Informations- und Aufklärungspflichten des Art. 13 Abs. 1 lit. c) DS-GVO ist ebenso kausal für den bei dem Kläger entstandenen Schaden. Gemäß vorstehender Erwägungen hat die Beklagte den Kläger bereits bei Erhebung seiner Mobilfunknummer nur unzureichend über die Verwendung seiner Mobilfunknummer im Hinblick auf das CIT aufgeklärt, sodass bezogen auf die Mobilfunknummer eine rechtswidrige Verarbeitung vorliegt. Diese ist auch kausal für den beim Kläger entstandenen Schaden, da es durch die Verwendung des CIT und das anschließende Abgreifen der Daten durch Dritte im Wege des „*Scrapings*“ zu einem Kontrollverlust auf Seiten des Klägers kam.

cc) Auch der Verstoß gegen Art. 32, 24, 5 Abs. 1 f) DS-GVO ist für den eingetretenen Schaden kausal, denn durch die unzureichenden Schutzmaßnahmen ermöglichte bzw. erleichterte die Beklagte ein Ausnutzen des CIT durch Dritte in Form von "*Scraping*". Auch dieses hat einen Kontrollverlust über die personenbezogenen Daten zur Folge.

dd) Der Schaden beruht zudem kausal auf einem Verstoß gegen Art. 33 und Art. 34 DS-GVO. Zwar ist der geltend gemachte Kontrollverlust bereits durch das "*Scraping*" der Daten erstmals eingetreten. Durch die unterlassene Benachrichtigung des Klägers wurde ihm jedoch die Möglichkeit genommen, geeignete Maßnahmen zu ergreifen, um das Risiko des Missbrauchs seiner Daten zu minimieren. Auch die zuständige Datenschutzbehörde konnte mangels rechtzeitiger Meldung keine Schritte zur Risikominimierung und Absicherung der Daten einleiten (LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 135 - 140, juris).

10. Die Beklagte handelte hinsichtlich der festgestellten Verstöße auch schuldhaft. Die Beklagte kann sich hinsichtlich der einzelnen Verstöße nicht nach Art. 82 Abs. 3 DS-GVO entlasten (vgl. auch LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, juris).

a) Demnach gelingt eine Befreiung nur, wenn der Verantwortliche oder der Auftragsverarbeiter nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Damit wird die Verantwortlichkeit der Beklagten widerleglich vermutet. Zwar ist der Begriff der Verantwortlichkeit im Sinne des § 82 Abs. 3 DS-GVO nicht näher definiert. So wird dieser vorwiegend mit dem Begriff des Verschuldens gleichgesetzt (vgl. OLG Stuttgart 31.3.2021 - 9 U 34/21; Gola/Heckmann/Gola/Piltz, 3. Aufl. 2022, DS-GVO Art. 82 Rn. 24; Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 49). Teilweise wird dies hingegen nicht angenommen mit der Folge, dass Art. 82 DS-GVO möglicherweise als Gefährdungshaftungstatbestand zu begreifen sei, sodass dem Verantwortlichen oder Auftragsverarbeiter unabhängig von jedwedem Verschulden lediglich ganz ungewöhnliche Kausalverläufe, die jeder Lebenserfahrung widersprechen, sowie Fälle höherer Gewalt und weit überwiegenden eigenen Fehlverhaltens der betroffenen Person nicht anzulasten seien (Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 82 Rn. 18).

b) Hierauf kommt es vorliegend jedoch nicht an. Denn der Beklagten gelingt weder der Nachweis fehlenden Verschuldens noch des Vorliegens ganz ungewöhnlicher Kausalverläufe, eines Falles höherer Gewalt oder weit überwiegenden eigenen Fehlverhaltens des Klägers. Das wäre nur dann der Fall, wenn sie sämtliche Sorgfaltsanforderungen erfüllt hat und ihm nicht die geringste Fahrlässigkeit vorzuwerfen ist (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 54 m.w.N.; Spindler/Schuster/Spindler/Horváth, 4. Aufl. 2019, DS-GVO Art. 82 Rn. 11). Die Beklagte kann sich hinsichtlich der Verstöße gegen Art. 25 Abs. 2 DS-GVO (dazu aa), Art. 13 Abs. 1 lit. c) DS-GVO (dazu bb), gegen Art. 32, 24, 5 Abs. 1 lit. f) DS-GVO (dazu cc), gegen Art. 33 DS-GVO (dazu dd) und gegen Art. 34 Abs. 1 DS-GVO (dazu ee) jedoch nicht entlasten.

aa) Einem Verstoß gegen Art. 25 Abs. 2 DS-GVO wohnt praktisch immer

eine Erhöhung der Gefahr eines Schadens inne. Eine Exkulpation ist dann nicht bzw. nur unter erschwerten Bedingungen möglich (Kühling/Buchner/Hartung, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 31; Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 25 Rn. 77). Gründe, warum es der Beklagten nicht möglich gewesen wäre, bei den "*Suchbarkeits-Einstellungen*" für Telefonnummern die Standard-Voreinstellung statt auf "*Alle*" lediglich auf die Option "*Nur ich*" einzustellen, sind nicht ersichtlich.

bb) Hinsichtlich des Verstoßes gegen Art. 13 Abs. 1 lit. c) DS-GVO kann sich die Beklagte ebenfalls nicht entlasten. Die Beklagte ist - wie festgestellt - der ihr nach Art. 13 Abs. 1 lit. c) DS-GVO auferlegten Informations- und Aufklärungspflicht nicht in vollständigem Umfang nachgekommen. Sie hat die Klagepartei zum Zeitpunkt der Datenerhebung seiner Mobilfunknummer nicht ausreichend über die Zwecke der Verarbeitung dieser Nummer aufgeklärt. Nach Art. 13 Abs. 1 lit. c) DS-GVO sind indes die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, zum Zeitpunkt der Erhebung der Daten mitzuteilen. Dem hat die Beklagte zumindest hinsichtlich der Verwendung der Mobilfunknummer für das von ihr verwendete Contact-Import-Tool nicht genügt. Gründe, warum es der Beklagten nicht möglich gewesen wäre die Klagepartei im Rahmen des Anmeldevorgangs hinreichend über die Verwendung der Mobilnummer für das von der Beklagten verwendete Contact-Import-Tool aufzuklären, sind nicht ersichtlich. Eine Änderung der Datenschutzhinweise wäre ohne weiteres möglich gewesen.

cc) Hinsichtlich des Verstoßes gegen Art. 32, 24, 5 Abs. 1 lit. f) DS-GVO kann sich die Beklagte ebenfalls nicht entlasten. Die Beklagte verstieß aufgrund unzureichender Sicherheitsmaßnahmen bezüglich der Nutzung des Contact-Import-Tool auch gegen Art. 32, 24, 5 Abs. 1 lit. f) DS-GVO. Der Verweis der Beklagten auf fehlende Rechtsprechung, aufsichtsbehördliche Leitlinien oder Literatur hinsichtlich des Umgangs mit Scraping-Sachverhalten verhilft dieser nicht zu einer Exkulpation. Es lässt sich hieraus schon nicht entnehmen, dass die Beklag-

te sämtliche Sorgfaltsanforderungen erfüllt hat oder ihr nicht die geringste Fahrlässigkeit vorzuwerfen ist. Vielmehr nutzten Dritte bereits erkannte oder erkennbare Angriffswege, um auf Daten zuzugreifen, sodass die Nichtverantwortlichkeit des Verantwortlichen nicht nachgewiesen werden kann (Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 15; Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 54). Scraping ist ausweislich des Beklagtenvorbringens "*eine gängige Taktik*". Es war jedenfalls erkennbar, dass das CIT durch Scraping ausgenutzt werden kann. Dies begründet sich bereits aus dem Umstand, dass die Beklagte selbst Schutzmaßnahmen behauptet und somit von der Notwendigkeit dieser ausgeht.

dd) Die Beklagte hat zudem ihre Meldepflicht aus Art. 33 DS-GVO schuldhaft verletzt (zum Verstoß siehe oben). Gründe warum es der Beklagten nicht möglich gewesen wäre, ihrer bestehenden Meldepflicht nachzukommen, sind nicht ersichtlich. Dass sie der Meinung war, sie sei nicht zur Meldung verpflichtet, lässt das Verschulden nicht entfallen.

ee) Die Beklagte hat auch schuldhaft gegen Art. 34 Abs. 1 DS-GVO verstoßen. Gründe warum es der Beklagten nicht möglich gewesen wäre, ihrer gegenüber der Klagepartei bestehenden Informationspflicht nachzukommen, sind nicht ersichtlich.

11. Die Klagepartei hat sich auch kein Mitverschulden nach § 254 Abs. 1 BGB anrechnen zu lassen.

a) Es kann dahinstehen, ob ein Mitverschulden des Geschädigten im Rahmen von Art. 82 DS-GVO überhaupt zu berücksichtigen ist (vgl. dazu nur Bergt in Kühling/Buchner, DS-GVO - BDSG 3. Aufl. DS-GVO Art. 82 Rn. 59 mit Fn. 181; LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 100 - 102, juris).

b) Jedenfalls tritt ein etwaiges Mitverschulden des Klägers (§ 254 BGB), weil er die Datenschutzeinstellungen seines Facebook-Profils nicht geändert hat und dadurch auch den Zugriff der Daten-Scraper mit ermöglicht hat, hinter die Verstöße der Beklagten vollkommen zurück. Denn das Verhalten des

Klägers – die von der Beklagten vorgegebenen Voreinstellungen zu belassen – ist gerade von der Beklagten intendiert und mit Blick auf den von ihr angenommenen Sinn und Zweck der Facebook-Plattform gewünscht. Dann aber kann die Beklagte sich, wenn sich die Gefahren, die sich durch ihr verordnungswidriges Verhalten ergeben, realisiert haben, nicht darauf berufen, es sei am Kläger dies im Sinne des Schutzes seiner personenbezogenen Daten zu korrigieren (vgl. auch OLG Koblenz, Urteil vom 18.05.2022 – 5 U 2141/21, BeckRS 2022, 11126 Rn. 78; Frenzel in Paal/Pauly, DS-GVO – BDSG 3. Aufl. DS-GVO Art. 82 Rn. 19). Das gilt umso mehr für das Contact-Import-Tool, über dessen Funktionsweise und die damit verbundenen Gefahren seitens der Beklagten nicht aufgeklärt wird.

12. Der dem Kläger zuzuerkennende Schadensersatz für den erlittenen immateriellen Schaden ist entsprechend seinem Begehren für den lediglich als gerechtfertigt angesehen Ersatzanspruch wegen der Verstöße im Zusammenhang mit dem Daten-Scraping-Vorfall mit **600 Euro** zu bemessen (§ 287 Abs. 1 Satz 1 ZPO, vgl. BAG Urteil vom 05.05.2022 – 2 AZR 363/21, BeckRS 2022, 20229 Rn. 14; LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 103, juris - dort 300 €).

a) Damit kann einerseits der Ausgleichs- und Genugtuungsfunktion genügt werden, andererseits der generalpräventiven Funktion des immateriellen Schadensersatzes hinreichend Rechnung getragen werden. Zum einen ist – mit Blick auf den generalpräventiven Auftrag des Art. 82 DS-GVO (vgl. Gola/Piltz in Gola/Heckmann, DS-GVO – BDSG, 3. Aufl. DS-GVO Art. 82 Rn. 5) – insoweit zu berücksichtigen, dass die Art und Weise der Datenerhebung durch die Beklagte systematisch gegen die Vorgaben der DS-GVO verstößt, um damit Sinn und Zweck der von ihr betriebenen Facebook-Plattform zu fördern. Ein Vergleich mit den bisher in Deutschland für andere Fälle von Persönlichkeitsrechtsverletzungen ausgeurteilten Beträgen kommt nach hiesiger Auffassung zwar nicht in Betracht. Für die Festlegung der Höhe des Schadensersatzes für immaterielle Schäden kann deshalb auch auf die Wertungen der Kriterien zur Bußgeldbemessung zurückgegriffen werden. Von besonderer Bedeutung sind jedenfalls die drohenden Folgen, wofür auch die Verknüpfbarkeit zu berücksichtigen ist (zu Vorstehenden insgesamt Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 17-18d). Gerade

bei immateriellen Schäden ist zu berücksichtigen, dass der geschuldete Schadensersatz „eine wirklich abschreckende Wirkung“ haben muss. Der Zweck der Abschreckung kann nur durch die Ausurteilung ausreichend hoher immaterieller Schadensersatzansprüche erfüllt werden. Die Einführung eines Strafschadensersatzes ist damit jedoch nicht bezweckt (zu Vorstehenden insgesamt Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 17-18d).

b) Gemessen daran ist ein immaterieller Schadensersatzanspruch i.H.v. 600 € angemessen (§ 287 ZPO).

aa) Beim Kläger ist jedenfalls ein Kontrollverlust seiner Daten eingetreten, der bei der Höhe des immateriellen Schadensersatzanspruchs zu berücksichtigen ist.

bb) Soweit der Kläger im Rahmen seiner informatorischen Anhörung glaubhaft angab, er handele generell vorsichtig hinsichtlich seiner Daten hat er jedoch überdies auch angegeben, dass sich sein Verhalten seit Kenntnis des „Scraping-Sachverhalts“ nicht wesentlich geändert habe, sodass eine veränderte Verhaltensweise nicht angenommen und mithin auch bei der Höhe des immaterieller Schadensersatzanspruch nicht zu berücksichtigen ist.

cc) Soweit der Kläger behauptet, er bekäme seit dem Vorfall regelmäßig Anrufe, Spam-Emails und SMS, die eine betrügerische Absicht offenbarten, sind die Angaben des Klägers zwar glaubhaft. Jedoch kann nicht ohne weiteres angenommen werden und steht nicht zur Überzeugung des Gerichts fest, dass diese Anrufe, SMS und E-Mails erst durch die konkreten Verstöße der Beklagten und den streitgegenständlichen „Scraping-Vorfall“ ermöglicht wurden. Vielmehr können diese auch auf einer anderweitigen - unbefugten - Datenabreifung und/oder Datenweitergabe beruhen.

dd) Auch ist bei der Bemessung der Umfang der Daten des Klägers, die abgegriffen worden sind, zu berücksichtigen. Sicherlich ist die Telefonnummer darunter, die über den Vorfall mit seinem Namen verbunden werden kann, ebenso auch das Profil bei Facebook, so dass der

Kläger über diesen Weg kontaktiert werden kann. Weitergehende Daten, die eine Kontaktaufnahme ermöglichen könnten, sind – nach derzeitigem Kenntnisstand – nicht von Dritten gescrapt worden. Daher ist der mögliche Schaden, auch wenn die Gefahr eines Identitätsdiebstahls nicht ausgeschlossen werden kann, im Grunde für den Kläger letztlich noch überschaubar (LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 104, juris).

ee) Aufgrund des eingetretenen Kontrollverlusts hält das Gericht einen immateriellen Schadensersatzanspruch i.H.v. 600 € für angemessen (§ 287 ZPO).

13. Der Zinsanspruch folgt aus §§ 288, 291 BGB

II. Nachdem dem Kläger ein Schadensersatzanspruch nach Art. 82 Abs. 1 DS-GVO zusteht, ist auch der Klageantrag Ziff. 2 begründet. Es ist nicht ausgeschlossen, dass der Kläger künftig infolge der Verstöße der Beklagten gegen die DS-GVO auch materielle Schäden erleidet (LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 110, juris).

III. Darüber hinaus kann der Kläger die mit dem Klageantrag zu 3 beanspruchte Unterlassung – in weiten Teilen – erfolgreich gegenüber der Beklagten geltend machen (LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 111, juris; a.A. abstellend auf das Einverständnis zur Veröffentlichung von Daten: LG Essen, Urteil vom 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818; LG Gießen, Urteil vom 03.11.2022 – 5 O 195/22, GRUR 2022, 30480 und LG Bielefeld, Urteil vom 19.12.2022 – 8 O 182/22, GRUR-RS 2022, 38375).

1. Soweit es für den vorbeugenden Unterlassungsschutz eine gesonderte Anspruchsgrundlage in der DS-GVO nicht gibt, bleibt im Hinblick auf die Vorgaben des Art. 79 DS-GVO entweder ein Rückgriff auf § 823 Abs. 2, § 1004 BGB analog möglich, um Schutzlücken zu vermeiden (vgl. nur OLG München, Urteil vom 19.01.2021 – 18 U 7243/19, juris Rn. 62), oder ein solcher Anspruch folgt mit Blick auf die unrechtmäßige Datenverarbeitung seitens der Beklagten aus Art. 17 Abs. 1 lit. d DS-GVO, falls man annimmt, aus dem dort normierten Löschungsrecht lasse sich auch ein Unterlassungsanspruch herleiten (vgl. BGH, Urteil vom 13.12.2022 – VI ZR 60/21 Rn. 10; zum Ganzen auch: OLG Frankfurt, Urteil vom 14.04.2022 – 3 U 21/20, GRUR-RS 2022, 10537).

2. Die Beklagte hat gegen Art. 25 Abs. 2 DS-GVO, Art. 13 Abs. 1 lit. c) DS-GVO, gegen Art. 32, 24, 5 Abs. 1 lit. f) DS-GVO, gegen Art. 33 DS-GVO und gegen Art. 34 Abs. 1 DS-GVO verstoßen. Diese Rechtsverstöße geben dem Kläger einen darauf bezogenen Anspruch auf Beseitigung und künftige Unterlassung.

   a) Daher kann der Kläger verlangen, dass die Beklagte es unterlässt, personenbezogenen Daten (Telefonnummer, Facebook-ID, Familienname, Vorname, Geschlecht, Stadt, Beziehungsstatus) unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen. In gleicher Weise kann der Kläger beanspruchen, dass die Beklagte es unterlässt, dass seine Mobilfunknummer trotz einer Einstellung auf „privat“ noch durch Verwendung des Contact-Import-Tools verwendet werden kann, es sei denn, es wird ausdrücklich die Einwilligung hierzu erteilt.

   b) Ausgenommen davon sind indes die Daten „Land“ und „Bundesland“, die – nach dem vom Kläger unbestritten gebliebenen Vorbringen der Beklagten – nicht Gegenstand der Angaben auf der Facebook-Plattform sind. Insoweit ist der Unterlassungsanspruch teilweise nicht begründet und daher abzuweisen.

3. Soweit die Beklagte darauf verweist, dass der Kläger durch eine Änderung der Einstellungen auf der Facebook-Plattform die von ihm gewünschte Rechtsfolge erreichen kann, steht dies Unterlassungsansprüchen des Klägers nicht entgegen. Durch mögliche, vom Kläger selbst vorzunehmende Änderungen von Einstellungen in seinem Facebook-Profil ist eine Wiederholungsgefahr nicht entfallen, und der Kläger kann grundsätzlich Unterlassung jeder einmal getätigten rechtswidrigen Datenverarbeitung verlangen. Denn im Fall eines rechtswidrigen Eingriffs in ein geschütztes Rechtsgut des Betroffenen besteht nach ständiger Rechtsprechung des Bundesgerichtshofs eine tatsächliche Vermutung für das Vorliegen der Wiederholungsgefahr. An eine Entkräftung der Vermutung sind strenge Anforderungen zu stellen, im Regelfall bedarf es hierfür der Abgabe einer strafbewehrten Unterlassungsverpflichtungserklärung gegenüber dem Gläubiger des Unterlassungsanspruchs. Eine solche hat die Beklagte hier nicht abgegeben, sie geht vielmehr von der Wirksamkeit der von ihr angenommenen Einwilligung aus (zum Vorstehenden insgesamt LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 112 - 118, juris).

4. Die Ordnungsmittelandrohung folgt aus § 890 ZPO.

IV. Nachdem die Beklagte einen etwaigen Auskunftsanspruch des Klägers bereits erfüllt hat (vgl. oben I. Ziff. 7.) kann dieser insoweit den mit dem Klageantrag zu 4 geltend gemachten Anspruch nicht erfolgreich durchsetzen (so auch LG Essen, Urteil vom 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818; LG Gießen, Urteil vom 03.11.2022 – 5 O 195/22, GRUR 2022, 30480 und LG Bielefeld, Urteil vom 19.12.2022 – 8 O 182/22, GRUR-RS 2022, 38375; LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 119, juris).

V. Im Rahmen des ihm zustehenden materiellen Schadensersatzanspruchs nach Art. 82 Abs. 1 DS-GVO kann der Kläger auch die Erstattung vorgerichtlich angefallener Rechtsanwaltsgebühren beanspruchen.

Ausgehend von den in Ansatz zu bringenden Gegenstandswerten für die jeweiligen Klageanträge (dazu unten D) ist der Kläger hier hinsichtlich eines Begehrens erfolgreich, dessen Wert mit bis zu 5.600 € anzunehmen ist (Klageantrag 1 erfolgreich 600 €; Klageantrag Ziff. 2 und 3 vollständig erfolgreich, da die geringfügige Abweisung hinsichtlich des Datums „Bundesland“ nicht ins Gewicht fällt, Wert 5.000 €). Hinzuzurechnen ist noch das zunächst nicht erfüllte Auskunftsverlangen (250 Euro). Insgesamt ergeben sich daher Gebühren nach Ziff. 2300, 7002, 7008 VV RVG i.H.v. 627,13 €, die ebenfalls nach §§ 288, 291 BGB zu verzinsen sind (LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 120 - 121, juris).

D.

Die Kostenentscheidung folgt aus § 92 Abs. 1 ZPO, wobei das teilweise Unterliegen hinsichtlich der Anträge zu 1 und zu 3 ebenso wie hinsichtlich des Antrags zu 4 zu Lasten des Klägers zu berücksichtigen ist.

Die Entscheidung zur vorläufigen Vollstreckbarkeit hat ihre Rechtsgrundlage in § 709 ZPO bzw. §§ 709, 711 ZPO.

Der Streitwert ist mit insgesamt bis zu 7.000 Euro festzusetzen (Antrag zu 1: 1.000 Euro, Antrag zu 2: 500 Euro, Antrag zu 3: 5.000 Euro, Antrag zu 4: 250 Euro; vgl. dazu OLG Stuttgart, Beschluss vom 03.01.2023 – 4 AR 4/22 und LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 122 - 124, juris).

Rechtsbehelfsbelehrung:

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

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

Landgericht Stuttgart
Urbanstraße 20
70182 Stuttgart

einzulegen.

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

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

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

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

[redacted]
Richter am Landgericht