

Aktenzeichen:
53 O 255/23



Landgericht Stuttgart

Im Namen des Volkes

Urteil

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **WBS-LEGAL Rechtsanwälts GmbH & Co.KG**
Eupener Straße 67, 50933 Köln, Gz.:

gegen

Meta Platforms Ireland Ltd.
vertreten durch d. die Mitglieder des Board of Directors
Merrion Road,, Dublin 4, D04 X2K5, Irland
- Beklagte -

Prozessbevollmächtigte:
Rechtsanwälte **Freshfields Bruckhaus Deringer PartG mbB**
Josephsplatz 1, 90403 Nürnberg, Gz.:

wegen Persönlichkeitsrechtsverletzung, Verstöße gegen die Datenschutz-Grundverordnung

hat das Landgericht Stuttgart - 53. Zivilkammer - durch den Vorsitzenden Richter am Landgericht als Einzelrichter am 18.04.2024 aufgrund der mündlichen Verhandlung vom 18.04.2024 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz i.H.v. 750 Euro nebst Zinsen i.H.v. 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 10.01.2024 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. Im Übrigen wird die Klage abgewiesen.
4. Von den Kosten des Rechtsstreits haben der Kläger 4/5 und die Beklagte 1/5 zu tragen.
5. Das Urteil ist wegen Ziff. 1 und wegen der Kosten vorläufig vollstreckbar. Die Beklagte kann die Vollstreckung durch den Kläger durch Sicherheitsleistung i.H.v. 110 Prozent des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht der Kläger vor der Vollstreckung Sicherheit i.H.v. 110 Prozent des zu vollstreckenden Betrags leistet. Der Kläger kann die Vollstreckung durch die Beklagte durch Sicherheitsleistung i.H.v. 110 Prozent des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit i.H.v. 110 Prozent des zu vollstreckenden Betrags leistet.
6. Der Streitwert wird auf bis zu 7.000 Euro festgesetzt.

Tatbestand

Die Parteien streiten um Ansprüche auf Schadensersatz, Unterlassung, Auskunft im Zusammenhang mit der Nutzung der von der Beklagten betriebenen Plattform Facebook und eines Daten-Scraping-Vorfalles.

Im Jahr 2019 lasen Dritte – deren genaues Vorgehen ist zwischen den Parteien streitig – jedenfalls die Facebook-ID, den Namen und den Vornamen („Scraping“) über ein sogenanntes Contact-Import-Tool von Facebook aus zum Teil öffentlich zugänglichen Daten des Klägers bei Facebook aus. Die Beklagte geht davon aus, dass das Contact-Import-Tool zur Bestimmung der Telefonnummern der einzelnen Benutzer genutzt wurde. Mithilfe dessen Hilfe seien Kontakte hochgeladen worden, welche mögliche Telefonnummern von Nutzern enthielten, um so festzustellen, ob diese Telefonnummern mit einem Facebook-Konto verbunden sind. Soweit die Scraper hätten feststellen können, dass eine Telefonnummer mit einem Facebook-Konto verknüpft sei, hätten 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. Anfang April 2021 wurden diese Daten im Internet verbreitet.

Mit einer E-Mail des Prozessbevollmächtigten des Klägers vom 07.04.2023 forderte dieser die Beklagte zu einer Schadensersatzzahlung i.H.v. 500 Euro, zur Unterlassung einer – nach seiner Auffassung – rechtswidrigen Datenverarbeitung und zur Auskunft darüber auf, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht wurden (Anlage K 1). Dazu hat die Beklagte über ihre Prozessbevollmächtigten Stellung genommen (Anlage B 16).

Der Kläger ist der Ansicht, ihm stehe ein Schadensersatzanspruch nach Art. 82 Abs. 1 DS-GVO zu. Die Beklagte verstoße gegen die DS-GVO, indem sie ohne ausreichende Grundlage i.S. von

Art. 6 und 7 DS-GVO Informationen i.S. von Art. 13, 14 DS-GVO verarbeite. Weiter habe sie gegen Grundsätze aus Art. 5 DS-GVO sowie gegen Art. 25, 32 und 34 DS-GVO verstoßen. Zudem habe sie Betroffenenrechte der Art. 15, 17 und 18 DS-GVO verletzt.

Von ihm seien Daten wie Telefonnummer, Name, Wohnort und E-Mail-Adresse abgegriffen worden. Ob noch mehr Daten entwendet worden seien, lasse sich mangels ausreichender Auskunft durch die Beklagte noch nicht angeben. Er habe deswegen einen erheblichen Kontrollverlust über seine Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch seiner, ihn betreffenden Daten verblieben. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannt Nummern und Adressen. Darüber hinaus erhalte er seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks. Oft würden auch bekannte Plattformen oder Zahlungsdienstleister wie Amazon oder Paypal impersoniert und durch Angabe der entwendeten Daten versucht, ein gesteigertes Vertrauen zu erwecken. Das habe dazu geführt, dass er nur noch mit äußerster Vorsicht auf jegliche E-Mails und Nachrichten reagieren könne und jedes Mal einen Betrug fürchte und Unsicherheit verspüre. Er gebe die Telefonnummer stets bewusst und zielgerichtet weiter und mache diese nicht wahl- und grundlos der Öffentlichkeit zugänglich. Die erkennbaren Auswirkungen der bestehenden Ängste, des Stresses, der Komfort- und Zeiteinbußen lägen darin, dass er sich mit dem Datenleak und der Herkunft der Daten auseinandersetzen müsse. Dies sei geeignet, zu einem belastenden Eindruck des Kontrollverlusts zu führen. Dass die benannten Daten in Kombination sogar im sog. Darknet gehandelt würden, vergrößere seine Ängste und seinen Stress. Daher sei ein Schadensersatz i.H.v. mindestens 1.000 Euro angemessen.

Aus der Verpflichtung der Beklagten zur Leistung von Schadensersatz aus dem dargestellten Schadensereignis folge auch die Pflicht, zukünftige – materielle – Schäden, die aufgrund der entwendeten Daten entstünden, zu tragen.

Ihm stehe ein Anspruch auf Unterlassung zu, seine personenbezogenen Daten in Zukunft nicht unbefugt, d.h. ohne vorherige ausreichende Belehrung, zu veröffentlichen und diese zukünftig unbefugten Dritten nicht zugänglich zu machen. Darüber hinaus könne er einen ergänzenden Auskunftsanspruch gegenüber der Beklagten geltend machen.

Wegen des weiteren Vortrags des Klägers wird auf die Klageschrift vom 13.12.2023 sowie auf die Schriftsätze vom 18.03.2023 und vom 03.04.2024 Bezug genommen.

Der Kläger beantragt:

1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadenersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000 Euro nebst Zinsen seit Rechtshängigkeit i.H.v. 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 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) bei Vorliegen einer Einwilligung des Klägers, die es der Beklagten erlaubt, Kontakte aufgrund eines Abgleichs mittels der Telefonnummer und des Facebookprofils vorzuschlagen, keine ausreichenden Maßnahmen nach dem Stand der Technik zu ergreifen, um das Ausnutzen des Systems für andere Zwecke als die Kontaktaufnahme zu verhindern,
 - b) die Telefonnummer der Klägerseite durch Kontaktvorschläge für Dritte, welche diese Telefonnummer abfragen, mit dem Facebookprofil des Klägers zu verknüpfen, solange der Kläger hierzu nicht ausdrücklich einwilligt.
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 i.H.v. 500,76 Euro zu zahlen zuzüglich Zinsen seit Rechtshängigkeit i.H.v. 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte ist der Ansicht, die Klage sei teilweise bereits unzulässig. Ihr seien Verstöße gegen die DS-GVO nicht anzulasten. Die Daten seien weder durch Hacking noch infolge eines Fehlers oder Sicherheitsverstoßes in ihrem System, sondern durch das automatisierte, massenhafte Sammeln von ohnehin öffentlich einsehbaren und damit nicht vertraulichen Daten erlangt und an anderer Stelle zugänglich gemacht worden. Die gesammelten Daten umfassten lediglich die immer öffentlichen Nutzerinformationen und diejenigen Daten, die entsprechend der jeweiligen „Zielgruppenauswahl“ öffentlich einsehbar seien.

Die Beklagte behauptet, dass es Hauptzweck der Facebook-Plattform sei, andere Nutzer zu finden und mit diesen in Kontakt zu treten, woran sich auch die standardmäßigen Voreinstellungen orientierten. Die „Scrapper“ hätten dementsprechend lediglich die diesem Zweck dienenden Funktionen ausgenutzt. 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.

Zudem habe sie ihren Nutzern – so auch dem Kläger – alle erforderlichen Informationen zur Datenverarbeitung zur Verfügung gestellt und umfassend über die Möglichkeiten der Anpassung ihrer Privatsphäre-Einstellungen informiert. Zudem lege sie den Nutzern – schon in der Datenrichtlinie – durch Beispiele dar, welche Konsequenzen sich aus dem Teilen bestimmter Daten ergeben könnten. Der Kläger sei daher 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.

Es fehle auch an einem ersatzfähigen und vor allem kausalen Schaden des Klägers, abgesehen davon rechtfertigten die von ihm behaupteten Verstöße nicht einen Ersatzanspruch nach Art. 82

Abs. 1 DS-GVO. Eine konkrete, spürbare persönliche Beeinträchtigung durch den Scraping-Sachverhalt sei vom Kläger nicht dargelegt.

Angesichts dessen sei auch der Klageantrag zu 2 mangels Verstoßes gegen die DS-GVO unbegründet, im Übrigen habe der Kläger nicht dargelegt, dass ein zukünftiger Eintritt eines Schadens wahrscheinlich sei. Ebenso wenig bestehe ein Unterlassungsanspruch oder ein weitergehender Auskunftsanspruch.

Wegen des weiteren Vorbringens der Beklagten wird auf die Klageerwiderung vom 28.09.2022 und den Schriftsatz vom 10.04.2024 Bezug genommen.

Vor dem erkennenden Einzelrichter fand am 18.04.2024 eine mündliche Verhandlung statt, in der der Kläger persönlich angehört worden ist und auf deren Protokoll Bezug genommen wird.

Entscheidungsgründe

Die Klage ist zulässig und auch zu einem geringen Teil – im aus dem Tenor ersichtlichen Umfang – begründet.

A.

Die Klage ist zulässig.

I.

Das Landgericht Stuttgart ist international, örtlich und sachlich zuständig.

1. Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 EuGVVO.

Ein ausschließlicher Gerichtsstand gemäß Art. 24 EuGVVO ist nicht ersichtlich. 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.

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

2. Das Landgericht Stuttgart ist örtlich zuständig. Das folgt zum einen aus Art. 18 Abs. 1 Alt. 2 EuGVVO, zum anderen aus Art. 79 Abs. 2 Satz 2 DS-GVO.

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

II.

Auch sonst begegnet die Klage durchgreifenden Bedenken hinsichtlich ihrer Zulässigkeit nicht.

1. Der Klageantrag zu 1 ist nicht unbestimmt.

2. Das Feststellungsinteresse gemäß § 256 Abs. 2 ZPO für den Klageantrag zu 2 steht nicht in Frage.

Ein Feststellungsantrag ist schon zulässig, wenn die Schadensentwicklung noch nicht abgeschlossen ist und der Kläger seinen Anspruch deshalb ganz oder teilweise nicht beziffern kann. Ein Feststellungsinteresse ist nur zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen. Das kann indes bei dem hier in Rede stehenden Daten-Scraping-Vorfall mit der behauptet unkontrollierten Nutzung gescrapter Daten bei verständiger Würdigung angesichts der erst im Jahr 2021 erfolgten Veröffentlichung (noch) nicht angenommen werden. Es ist nicht ausgeschlossen, dass irgendein materieller Schaden – hierauf beschränkt der Kläger sein Begehren ausweislich der Replik vom 18.03.2024 – entstehen könnte.

3. Darüber hinaus ist auch das Unterlassungsbegehren des Klageantrags zu 3 hinreichend bestimmt i.S. von § 253 Abs. 2 Nr. 2 ZPO.

B.

Die Klage ist hinsichtlich des begehrten immateriellen Schadensersatzes teilweise begründet (unten I), in Bezug auf das Feststellungsbegehren des Klageantrags zu 2 begründet (unten II), im Klageantrag zu 3 (unten III) dagegen nicht begründet, ebenso wenig im Klageantrag zu 4 (unten IV) und zu 5 (unten V).

I.

Dem Kläger steht gegen die Beklagte, die als Verantwortliche i.S. von Art. 4 Nr. 7 DS-GVO anzusehen ist, ein Anspruch auf – immateriellen – Schadensersatz i.H.v. 750 Euro aus Art. 82 Abs. 1 DS-GVO zu (Klageantrag zu 1), deren zeitlicher, sachlicher und räumlicher Anwendungsbereich hier eröffnet ist (vgl. OLG Stuttgart, Urteil vom 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883 Rn. 150 ff.).

1. Art. 82 Abs. 1 DS-GVO erfordert nach seinem Wortlaut einen Verstoß gegen die DS-GVO. Gegen welche Vorschrift der DS-GVO verstoßen wurde, ist insoweit zunächst nicht relevant.

Gemäß Art. 82 Abs. 1 DS-GVO haftet der Verantwortliche für Schäden wegen „Verstoßen 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 (vgl. OLG Stuttgart, Urteil vom 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883 Rn. 164).

2. Dem Kläger steht im Hinblick auf das Verhalten der Beklagten im Vorfeld des Daten-Scraping-Vorfalles ein Anspruch auf immateriellen Schadensersatz i.H.v. 750 Euro zu.

a) Der Beklagten sind insofern jedenfalls Verstöße gegen Art 25 Abs. 2 DS-GVO und Art. 13 DS-GVO anzulasten.

aa) Ein relevanter Verstoß der Beklagten ist zunächst darin zu sehen, dass diese gegen die sich aus Art 25 Abs. 2 DS-GVO ergebende Verpflichtung verstoßen hat.

(1) Danach 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 Privatsphäreinstellungen durch den Nutzer eingerichtet werden (so Hartung in Kühling/Buchner, DS-GVO - BDSG 3. Aufl. DS-GVO Art. 25 Rn. 26).

(2) Das ist durch die Beklagte nicht gewährleistet.

Aus ihrem eigenen Vortrag in der Klageerwiderung ergibt sich, dass der Umstand, dass die Telefonnummer des Klägers „öffentlich“ war, darauf beruhte, dass er dies in den Voreinstellungen nicht geändert hat, nachdem – wie die Beklagte zugesteht – die Standard-Einstellung für die Suchbarkeit von Telefonnummern während des relevanten Zeitraums „Alle“ gewesen ist. Nicht

ausreichend ist insoweit, dass – worauf die Beklagte abstellt – etwaige Einstellungen vom Nutzer geändert werden können. Dasselbe gilt für den von der Beklagten angeführten „Privatsphäre-Check“.

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).

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).

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. Facebook 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 Vor-

einstellung, 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 „Hilfereich“ 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).

bb) Darüber hinaus ist die Beklagte der ihr nach Art. 13 DS-GVO auferlegten Informations- und Aufklärungspflicht nicht in vollständigem Umfang nachgekommen.

(1) Die Beklagte hat den Kläger 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.

(2) Dem hat die Beklagte zumindest hinsichtlich der Verwendung der Mobilfunknummer für das von ihr verwendete Contact-Import-Tool nicht genügt.

Dadurch ermöglicht die Beklagte 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. So können diese Kontakte auf der Facebook-Plattform gefunden, und es kann mit ihnen in Verbindung getreten werden.

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“ 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.

(3) Angesichts des Vorstehenden kann hier auch nicht von einer wirksamen 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).

cc) Ob die Beklagte im Vorfeld des Daten-Scraping-Vorfalles weitere Pflichtverletzungen in Ansehung der DS-GVO begangen hat (vgl. dazu OLG Stuttgart, Urteil vom 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883 Rn. 193 ff.; OLG Hamm 15.08.2023, Urteil vom 15.08.2023 – 7 U 19/23, GRUR-RS 2023, 22505 Rn. 64 ff.), kann für die hier zu treffende Entscheidung dahinstehen, da sich daraus weitere Konsequenzen für den dem Kläger insofern zuzubilligenden Schadensersatzanspruch nicht ergeben können. Denn es besteht sich hinsichtlich der vom Kläger der Beklagten vorgeworfenen Verstöße letztlich kein weitergehender Unrechtsgehalt als derjenige, der bereits aus den Verstößen gegen Art. 25 Abs. 2 DS-GVO und aus Art. 13 DS-GVO folgt.

b) Die Beklagte kann sich mit Blick auf den Daten-Scraping-Vorfall nicht nach Art. 82 Abs. 3 DS-GVO entlasten.

aa) Insofern kann dahinstehen, ob überhaupt ein Verschulden erforderlich ist bzw. ob die Haftung nach Art. 82 DS-GVO zur Sicherstellung eines möglichst wirksamen Schadensersatzes als Gefährdungshaftung gestaltet ist (so z.B. Geissler/Ströbel, NJW 2019, 3414).

bb) Denn der Beklagten ist bereits nach ihrem eigenen Vorbringen eine Entlastung, hinsichtlich derer ihr die Darlegungs- und Beweislast obliegt (vgl. nur Nemitz in Ehmann/Selmayr, DS-GVO 2. Aufl. Art. 82 Rn. 19), nicht gelungen.

Sie bringt vor, dass die Daten-Scraper Verfahren eingesetzt hätten, um in großem Umfang Daten mit automatisierten Tools und Methoden zu sammeln, was nach den Nutzungsbedingungen von Facebook untersagt gewesen sei. Damit räumt sie die technische Möglichkeit des Abgreifens von Daten durch die von ihr gewählte Architektur der Facebook-Plattform ein. Wenn aber der Beklagten bewusst ist, dass Daten-Scraper bestimmte Funktionen missbrauchen können, dann wäre es an der Beklagten gewesen, gerade das zu unterbinden. Auch wenn das dem eigenen Verständnis der Facebook-Plattform zuwiderlaufen mag, dem Interesse der Nutzer an der Wahrung ihrer datenschutzrechtlichen Belange entspreche das indes sehr wohl.

Die Beklagte trägt überdies nichts Konkretes dazu vor, was sie gegen die ihr bekannte Möglichkeit unternommen haben will. Auch der Hinweis, dass die Telefonnummern von den Daten-Scrapern „bereitgestellt“ worden sei, entlastet die Beklagte nicht. Es wäre an ihr gewesen, ein solches automatisiertes Verfahren zu verhindern.

c) Dem Kläger ist im Zusammenhang mit dem Daten-Scraping-Vorfall auch ein nach Art. 82 DS-GVO ersatzfähiger – immaterieller – Schaden entstanden, für den die Verstöße der Beklagten gegen die DS-GVO kausal waren.

aa) Nach der Rechtsprechung des Europäischen Gerichtshofs geht aus dem Wortlaut von Art. 82 Abs. 1 DSGVO klar hervor, dass das Vorliegen eines „Schadens“, der entstanden ist, eine der Voraussetzungen für den in dieser Bestimmung vorgesehenen Schadenersatzanspruch darstellt, ebenso wie das Vorliegen eines Verstoßes gegen die DS-GVO und eines Kausalzusammenhangs zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind.

Dabei ist der begehrte Ersatz eines „immateriellen Schadens“ nicht davon abhängig, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat. Zudem ist es unerheblich, ob der infolge eines erwiesenen Verstoßes gegen die Bestimmungen der DS-GVO von der betroffenen Person behauptete „immaterielle Schaden“ mit einer zum Zeitpunkt ihres Schadenersatzantrags bereits erfolgten missbräuchlichen Verwendung ihrer personenbezogenen Daten durch Dritte verbunden ist oder ob er mit ihrer Angst verknüpft ist, dass eine solche Verwendung in Zukunft erfolgen könnte. Daher kann sich die betroffene Person auch auf ihre Befürchtung berufen, dass ihre personenbezogenen Daten aufgrund des eingetretenen Verstoßes gegen die DS-GVO in Zukunft von Dritten missbräuchlich verwendet werden (vgl. EuGH, Urteil vom 14.12.2023 – C-340/21, BeckRS 2023, 35786 Rn. 77 ff.).

bb) Dies zugrunde gelegt, muss eine Person, die von einem Verstoß gegen die DS-GVO betroffen ist, der für sie negative Folgen gehabt hat, nachweisen, dass diese Folgen einen immateriellen Schaden i.S. von Art. 82 DSGVO darstellen. Dabei ist zu prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann (vgl. EuGH, Urteil vom 14.12.2023 – C-340/21, BeckRS 2023, 35786 Rn. 84 f.; dazu auch OLG Hamm, Beschluss vom 21.12.2023 – 7 U 137/23, GRUR-RS 2023, 37310 Rn. 6).

Dies zugrunde gelegt, vermag der Einzelrichter auf der Grundlage der persönlichen Anhörung des Klägers festzustellen (§ 286 ZPO), dass die festgestellten Pflichtverletzungen der Beklagten kausal für einen immateriellen Schaden ist.

(1) Zunächst ist – anders als von der Beklagten angenommen – davon auszugehen, dass auch die Mobiltelefonnummer des Klägers Gegenstand des Daten-Scrapings geworden ist. Denn diese stand den Daten-Scrapern vorab nicht zur Verfügung, erst durch die Verbindung mit den weiteren Daten haben diese eine dem Kläger zuzuordnende Telefonnummer erlangt, nicht nur eine elf- oder zwölfstellige Zahl ohne jeden nachvollziehbaren Bezug zu einer Person.

(2) Der Kläger hat überzeugend, ohne erkennbar zu übertreiben und nachvollziehbar im Rahmen seiner persönlichen Anhörung dargelegt, dass er SMS und Nachrichten über WhatsApp erhält, die – aufgrund der Verknüpfung mit seiner Mobiltelefonnummer, der er nur für private Zwecke nutzt – ohne Zweifel als Spam einzuordnen sind. Er hat dabei auch Einsicht in sein Smartphone gewährt und sowohl eine entsprechende WhatsApp-Nachricht – weitere wurden aufgrund der Sperrung von Nummern nicht mehr angezeigt – als auch diverse SMS gezeigt. Zudem hat er in seiner Anrufliste telefonische Kontaktversuche von bei ihm nicht eingespeicherten Nummern gezeigt, die erkennbar einen Bezug zu seiner Person nicht haben.

(3) Ferner konnte der Kläger auch eine hinreichende zeitliche Einordnung geben, die es für den Einzelrichter als erwiesen erscheinen lässt, dass eine Verbindung des ersten Auftretens solcher Kontaktaufnahmen mit der Veröffentlichung seiner Daten bei Facebook besteht, auch wenn der Kläger – nachvollziehbar – einen ganz konkreten Zeitpunkt nicht benennen kann.

(4) Nach alledem ist beim Kläger zum einen ein Kontrollverlust über seine persönlichen Daten festzustellen. Dazuhin hat er zum anderen auch glaubhaft dargelegt, inwiefern er durch die Nachrichten und Anrufe, die er erhält, beeinträchtigt ist, so dass sich der Schaden nicht nur in Gestalt eines Kontrollverlustes manifestiert, sondern auch in der konkreten Beeinträchtigung z.B. durch die Erforderlichkeit, Nachrichten zu löschen, Nummern zu sperren und Vorsicht walten zu lassen, um nicht doch versehentlich eine dieser Spam-Nachrichten zu öffnen.

cc) Das Scraping der Daten des Klägers ist ohne die Verletzung der Pflichten der Beklagten nach Art. 25 Abs. 2 DS-GVO und nach Art. 13 DS-GVO nicht denkbar. Aufgrund des Verstoßes gegen die Verpflichtung eines Datenschutzes durch Voreinstellung und durch den unterbliebenen Hinweis auf die Auffindbarkeit der Telefonnummer bei Nutzung des Contact-Import-Tools ist es erst möglich geworden, dass personenbezogene Daten von Dritten abgegriffen worden sind.

Eine Mitursächlichkeit ist ausreichend, eine alleinige Kausalität nicht gefordert (vgl. nur LAG Baden-Württemberg, Urteil vom 25.02.2021 – 17 Sa 37/20, ZD 2021, 436 Rn. 85), daher ist insofern nicht erheblich, dass der Kläger nach der erstmaligen Anmeldung bei Facebook die Datenschutzeinstellungen nicht geändert hat.

Angesichts dessen, dass der Kläger nachvollziehbar und für das Gericht überzeugend erläutert, dass er nach Bekanntwerden des Datenlecks bei Facebook die Einstellung seines Kontos überprüft hat, ist überdies auch anzunehmen, dass er bei zutreffender Information und Aufklärung sich mit der Suchbarkeit in Bezug auf die Telefonnummer nicht einverstanden erklärt und diese Funktion gegebenenfalls deaktiviert hätte.

d) Ein etwaiges Mitverschulden des Klägers (§ 254 BGB) deswegen, weil er die Datenschutzeinstellungen seines Facebook-Profiles nicht geändert hat und dadurch auch den Zugriff der Daten-Scraper mit ermöglicht hat, tritt 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.

Vor diesem Hintergrund 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).

e) Der dem Kläger zuzuerkennende Schadensersatz für den erlittenen immateriellen Schaden ist mit 750 Euro zu bemessen (§ 287 Abs. 1 Satz 1 ZPO).

aa) 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. Andererseits ist auch 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.

bb) Soweit in Rede steht, dass die Beklagte – was anzunehmen sein sollte – überdies ihre Meldepflicht aus Art. 33 DS-GVO verletzt hat und dass sie – was ebenfalls anzunehmen sein sollte – den Kläger nicht entsprechend ihrer unverzüglich zu erfüllenden Verpflichtung aus Art. 34 Abs. 1 DS-GVO informiert hat, lässt sich hierauf eine Erhöhung des dem Kläger zuzubilligenden Schadens nicht stützen.

Durch die Verletzung dieser Pflichten hat sich der Schaden des Klägers nicht vertieft. Der maßgebliche Vorwurf an die Beklagten ergibt sich daraus, dass es möglich war, dass ein Daten-Scraping stattfand.

3. Aufgrund der nach Auffassung des Klägers unzureichenden Auskunft im Zusammenhang mit dem Daten-Scraping-Vorfall steht diesem ein Anspruch auf immateriellen Schadensersatz dagegen nicht zu.

Zwar kann auch eine bloße Verletzung einer Auskunftspflicht nach Art. 15 DS-GVO insoweit einen Schadensersatzanspruch begründen (vgl. OLG Köln, Urteil vom 14.07.2022 – 15 U 137/21, GRUR-RS 2022, 17897 Rn. 15; Franck, ZD 2021, 680; a.A. 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).

Hier ist indes davon auszugehen, dass die Information des Klägers, wie sie mit Schreiben vom 08.05.2023 (Anlage B 16) erfolgt ist, dessen Anspruch nach Art. 15 DS-GVO erfüllt hat.

Eine Erfüllung ist dann anzunehmen, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamumfang 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).

Darüber hinaus kann im hier zu beurteilenden Einzelfall nicht angenommen werden, dass – selbst wenn die Auskunft der Beklagte nicht ausreichend gewesen wäre – ein hierauf begründeter Schadensersatzanspruch bestünde.

4. Der Zinsanspruch folgt aus §§ 288, 291 BGB (ab dem 10.01.2024, § 187 BGB analog).

II.

Nachdem dem Kläger ein Schadensersatzanspruch nach Art. 82 Abs. 1 DS-GVO zusteht, ist auch auf den Klageantrag zu 2 zu erkennen. Es ist nicht ausgeschlossen, dass der Kläger künftig infolge der Verstöße der Beklagten gegen die DS-GVO – auch – materielle Schäden erleidet.

III.

Dem Kläger steht der mit dem Klageantrag zu 3 geltend gemachte Unterlassungsanspruch nicht zu.

Gestützt auf den Beseitigungs- bzw. Löschungsanspruch aus Art. 17 DS-GVO kann nur die künftige Speicherung von persönlichen Daten verhindert werden, nicht aber deren Verarbeitung, auf die der Klageantrag zu 3 gerichtet ist (OLG Stuttgart, Urteil vom 22.11.2023 – 4 U 20/23, juris Rn. 556 ff.). Daneben sind Anspruchsgrundlagen deutschen Rechts gesperrt.

Der Anspruch kann auch nicht auf den Benutzervertrag der Parteien gestützt werden. Ein vertraglicher Unterlassungsanspruch aus § 280 Abs. 1 BGB setzt – ebenso wie ein gesetzlicher Unterlassungsanspruch entsprechend § 1004 Abs. 1 Satz 2 i.V.m. § 823 Abs. 1 BGB – eine Erstbegehungs- bzw. Wiederholungsgefahr voraus (BGH, Urteil vom 29.07.2021 – III ZR 179/20 Rn. 103). Mit Blick auf die tatsächlichen Umstände des Datenlecks, die hier weitgehend unstrittig sind, ist eine solche Wiederholungsgefahr indes nicht anzunehmen; allein mit dem vorangegangenen Verstoß kann dies hier nicht begründet werden. Die tatsächliche Vermutung der Wiederholungsgefahr knüpft an eine vollendete Beeinträchtigung an, deren Wiederholung aufgrund situativer Umstände naheliegt. Mit Blick darauf, dass hier die Ursache nicht bei der Beklagten sondern bei einem von dieser beauftragten Dienstleister gelegen hat, fehlt es insofern an einer hinreichenden Grundlage für eine Anknüpfung.

IV.

Nachdem die Beklagte einen etwaigen Auskunftsanspruch des Klägers bereits erfüllt hat (vgl. oben) kann dieser insoweit den mit dem Klageantrag zu 4 geltend gemachten Anspruch nicht erfolgreich durchsetzen.

V.

Ein Anspruch auf vorgerichtliche Rechtsanwaltskosten (Klageantrag zu 5) steht dem Kläger nicht zu (OLG Stuttgart, Urteil vom 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883 Rn. 282 ff.).

C.

Die Kostenentscheidung folgt aus § 92 Abs. 1 ZPO.

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: 500 Euro; vgl. dazu OLG Stuttgart, Beschluss vom 03.01.2023 – 4 AR 4/22).

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 übermit-

teln. 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.

Vorsitzender Richter am Landgericht