Beglaubigte Abschrift

Landgericht Wiesbaden
Aktenzeichen:
3 O 50/23

Verkündet am: 21.09.2023

, Justizangestellte
Urkundsbeamtin der Geschäftsstelle

Im Namen des Volkes

U r t e i l

In dem Rechtsstreit

- Klägerin -

Prozessbevollmächtigte:
Rechtsanwälte und Rechtsanwältinnen Wilde Beuger Solmecke, Kaiser-Wilhelm-Ring 27-29, 50672 Köln
Geschäftszeichen: 5923/22 dk

gegen

Meta Platforms Ireland Limited (zuvor Facebook Ireland Ltd), vertreten durch den Geschäftsführer (Director) Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland, Irland

- Beklagte -

Prozessbevollmächtigte:
Rechtsanwälte und Rechtsanwältinnen Freshfields Bruckhaus Deringer, Bockenheimer Anlage 44, 60322 Frankfurt am Main

hat das Landgericht Wiesbaden – 3. Zivilkammer – durch die Vorsitzende Richterin am Landgericht als Einzelrichterin auf die mündliche Verhandlung vom 10.08.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an die Klägerin 600,00 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit 03.03.2023 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerin alle künftigen Schäden zu ersetzen, die der Klägerin 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 250.000,00 €, ersatzweise an ihrem gesetzlichen Vertreter (Direktor) zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter (Direktor) vollstreckenden Ordnungshaft bis zu 6 Monaten, im Wiederholungsfall bis zu 2 Jahren zu unterlassen, personenbezogene Daten der Klägerin, namentlich Telefonnummer, Facebook ID, Familienname, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zu 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.

4. Die Beklagte wird verurteilt, an die Klägerin vorgerichtliche Rechtsanwaltskosten in Höhe von 354,62 € zu zahlen zuzüglich Zinsen seit 03.03.2023 in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Im Übrigen wird die Klage abgewiesen,

Von den Kosten des Rechtsstreits hat die Klägerin 1/3, die Beklagte 2/3 zu tragen.

Das Urteil ist vorläufig vollstreckbar, für die Klägerin bezüglich Ziffer 1 und Ziffer 4 des Urteils wegen der Kosten nur gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages, im Übrigen wird der Klägerin nachgelassen, die Vollstreckung hinsichtlich der Kosten durch die Beklagte gegen Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet.

Tatbestand:

Die Klägerin macht Ansprüche auf Schadenersatz, Auskunft, Unterlassung und Erstattung von vorgerichtlichen Anwaltskosten wegen Verletzung von Datenschutzbestimmungen durch die Beklagte geltend in Verbindung mit Verletzung von Persönlichkeitsrechten und Grundrechten der Klägerin.

Die Beklagte ist Betreiberin der Website www.facebook.com sowie der auf dieser Seite angebotenen Dienste. Diese ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Auf ihren persönlichen Profilen können Nutzer Angaben zu ihrer Person machen und in einem von der Beklagten vorgegebenem Rahmen darüber entscheiden, welche Gruppen von Nutzern auf ihre Daten zurückgreifen können. Die Beklagte steht bei Tools und Informationen zur Verfügung, damit Nutzer ihre Privatsphäre auf der Facebookplattform 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, Nutzer ID (immer öffentliche Nutzerinformation). Eine Eingabe der Handynummer ist hier nicht zwingend erforderlich. Zudem können über sogenannte Privatsphäreeinstellungen bei weiteren Informationen, die die Nutzer zur Verfügung gestellt bekommen, diese festlegen, über eine sogenannte „Zielgruppenauswahl“, wer beispielsweise Informationen wie etwa Telefonnummer, Wohnort, Standort, Beziehungsstatus, Geburtstag und E-Mail einsehen kann. Hier können die Nutzer statt der standardgemäß vorgegebenen Einstellung „öffentlich“ auswählen, dass beispielsweise nur „Freunde“ auf der Plattform oder „Freunde von Freunden“ die jeweilige Information einsehen können. Die „Suchbarkeits-Einstellungen“ legen fest, wer das Profil eines Nutzers anhand einer Telefonnummer finden kann. Wenn die Nutzer sodann im Rahmen ihres Profils eine Telefonnummer als Kontakt eingespeichert haben, lässt die Beklagte es zu, die Kontakte mit den auf der Plattform hinterlegten Telefonnummer abzugleichen, um die hinter der Nummer stehende Person als Freund hinzufügen zu können. Dazu ist es nicht erforder-

lich, dass der jeweils andere Nutzer seine Telefonnummer nach der Zielgruppeneinstellung als öffentlich gekennzeichnet hat. Es ist demnach möglich, Nutzer anhand einer Telefonnummer zu finden, solange die „Suchbarkeits-Einstellung“ für Telefonnummern auf der Standard-Voreinstellung „alle“ steht. Die Klägerin ist bei der Plattform Facebook angemeldet und nutzt die von der Beklagten angebotene Social-Media-Plattform insbesondere, um mit Freunden zu kommunizieren. Der Teilnahme bei der Beklagten liegen die Allgemeinen Geschäftsbedingungen der Beklagten zugrunde. Bei der Registrierung wird der jeweilige Nutzer auf die Datenrichtlinien der Beklagten hingewiesen. 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.

Anfang April 2021 sind Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern im Internet öffentlich verbreitet worden, insbesondere Telefonnummern, E-Mail-Adressen, Facebook-ID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus und weitere korrelierende Daten. Grundlage war hier ein sogenanntes „Datenscraping“ im Jahr 2018, bei dem massenhaft automatisierten Sammeln der persönlichen Daten von den bis 533 Millionen Facebook-Nutzern. Beim „Scraping“ handelt es sich um 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 Nutzerbedingungen 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-Importe-Funktion). Zu diesem Zweck haben die Scraper mittels der Kontakt-Importer-Funktion Kontakte hochgeladen, welche mögliche Telefonnummern von Nutzern enthielten, um so festzustellen, ob diese Telefonnummer mit einem Facebook-Konto verbunden sind. Soweit dies festgestellt wurde, haben die Scraper die öffentlich einsehbaren Informationen (in Übereinstimmung der Zielgruppenauswertung des Nutzers) aus dem betreffenden Nutzerprofil kopiert und die Telefonnummern den abgerufenen öffentlich einsehbaren Daten sodann hinzugefügt. Die weiteren Einzelheiten hinsichtlich des Ablaufs sind zwischen den Parteien streitig.

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

Die Klägerin behauptet, ihre persönlichen Daten wie Telefonnummer, Vorname, Nachname, E-Mail-Adresse, Geschlecht und Geburtsdatum seien durch dieses Daten-Scraping abgegriffen worden. Es sei ihr zudem nicht bekannt, ob weitere Daten abgegriffen worden seien, da die Beklagte hierfür keine Auskunft erteilt habe. Durch die personenbezogenen Daten seien illegale Aktivitäten wie Internetbetrug und Veröffentlichungen in Hacker-Foren begünstigt worden. Insbesondere bestehe die Gefahr für gezielte Phishing-Attacken. Es sei auch nicht absehbar, welche Dritten hier Zugriff auf die Daten der Klägerin erhalten hätten und für welche konkret strafbaren Handlungen die Daten missbraucht werden würden bzw. könnten. Die Daten seien durch Unbekannte aus dem Datenbestand von Facebook mittels der Kontakt-Importe-Funktion zum Teil aus öffentlich zugänglichen Daten bei Facebook ausgelesen worden. Die Telefonnummer der Klägerin habe 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 Telefonnummern jeweils zu korrelieren sei mit Hilfe des Kontakt-Importer-Systems 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 übereinstimmten bzw. ob diese bei Facebook hinterlegt gewesen seien. Wenn dies der Fall gewesen sei, sei es dem Programm möglich gewesen, sämtliche Daten des Nutzers abzufragen und zu exportieren.

Dies ist nach Auffassung der Klägerin insbesondere dadurch ermöglicht worden, dass die Beklagte mangelnde Sicherheitsmaßnahmen vorgesehen habe, um ein Ausnutzen des bereitgestellten Kontakt-Importer-Tools zu verhindern. Insbesondere seien hier keine Sicherheits-Capchas (Abkürzung für „completely automated puplic turning test to tell computers and humans apart“), also ein vollständig automatisierter öffentlicher Test, um Computer von Menschen zu unterscheiden, verwendet worden, um sicherzustellen, dass es sich bei der Abfrage zur Synchronisierung um die Abfrage eines Menschen und nicht eine automatisch generierte Abfrage handelt. Es sei zudem nicht geprüft worden, ob eine derartige Vielzahl von Abfragen plausibel sei. Der massenhafte Zugriff auf die Facebook-Profile durch Dritte mit auffälligen Telefonnummernabfragen wäre durch ein einfaches IP-Lock erkennbar und blockierbar gewesen. Es sei eine Kombination mehrerer Maßnahmen erforderlich gewesen, angemessen und üblich, um die Sicherheit der Daten der Facebook-Nutzer zu gewährleisten. Es wäre beispielsweise auch eine Begrenzung der abgleichbaren Rufnummern oder Nutzung des Kontakt-Importer-Tools für Freunde von Freunden möglich gewesen. Zumindest aber wäre ein ausdrücklicher Hinweis auf die „offenen Standard-Einstellungen“ für die Suchbarkeit per Telefonnummern erforderlich gewesen, insbesondere bei erstmaliger Erhebung der Telefonnummer des Nutzers. Zudem sei die Einstellung zur Sicherheit der Telefonnummer auf Facebook so undurchsichtig und

kompliziert gestaltet, dass ein Nutzer tatsächlich keine sichere Einstellung erreichen könne. Auch die standardisierten Voreinstellungen bei der Beklagten hätten begünstigend für die Datenerhebung gewirkt.

Die Klägerin ist der Auffassung, sie habe einen erheblichen Kontrollverlust über ihre eigenen Daten erlitten und sei in einen Zustand großen Unwohlseins und großer Sorge über einen möglichen Missbrauch der Daten verblieben. Sie habe seit diesem Zeitraum dubiose Anrufe erhalten sowie jede Menge Spam-E-Mails. Weitere Unsicherheit sei dadurch gegeben, dass nicht ersichtlich sei, welche Daten im Einzelnen tatsächlich für Dritte einsehbar gewesen seien und hätten exportiert werden können.

Die Klägerin beantragt,

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

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

3. die Beklagte zu verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 €, ersatzweise an ihren gesetzlichen Vertreter (Direktor) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Direktor) zu vollstreckende Ordnungshaft bis zu 6 Monaten, im Wiederholungsfall bis zu 2 Jahren zu unterlassen,

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

   b) die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Information durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch

Verwendung des Kontakt-Importer-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 zu verurteilen, der Klägerin Auskunft über die die Klägerin betreffenden personenbezogenen 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 Kontakt-Importer-Tools erlangt werden konnten,

5. die Beklagte zu verurteilen, an die Klägerin vorgerichtliche Rechtsanwaltskosten in Höhe von 354,62 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet, es seien weder durch Hacker noch durch sonstige Dritte oder Schwachstellen im System der Beklagten und Sicherheitsverstöße Daten erlangt worden. Vielmehr seien die Daten von Dritten im Wege eines großangelegten Daten-Scrapings gescraped worden, hierbei handele es sich lediglich um das automatisierte Sammeln von öffentlich einsehbaren Daten von einer Website oder einer Anwendung. Soweit die insoweit erlangten Daten von der Facebook-Plattform stammen und Informationen über die Klägerin 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 alleine solche Daten gesammelt, die ohnehin öffentlich einsehbar seien und hätten diese öffentlich einsehbaren Daten auch anderweitig im Internet zugänglich gemacht. Dabei ermögliche das Kontakt-Importer-Tool den Nutzern nur, ihre Kontakte von ihren Mobilgeräten auf Facebook hochzuladen, um diese Kontakte auf der Facebook-Plattform zu finden und hier einfacher mit bereits bekannten Kontakten zusammenzukommen. Ein Export von Nutzerdaten sei hierdurch nicht ermöglicht. Die entsprechenden Telefonnummern seien von den Scrapern bereitgestellt worden. Das Kontakt-Importer-Tool habe es dann ermöglicht, die Klägerin im Einklang mit den Suchbarkeitseinstellungen anhand der Telefonnummer auf der Facebook-Plattform zu finden. Es sei auch nicht möglich, derartiges Scraping öffentlich einsehbarer Daten völlig zu verhindern, ohne den Zweck der Plattform durch Beseitigung der Funktion zu unterlaufen. Es gebe allenfalls Mittel, um Scraping zu begrenzen. Insbesondere stelle die Funktion, die von den Scrapern ausgenutzt werden, rechtmäßige, gewöhnliche Nutzerfunktionen dar. Die Beklagte habe angemessen technische und

organisatorische Maßnahmen ergriffen, um das Risiko von Scraping zu unterbinden. Die Klägerin sei wohl über die Einstellungsmöglichkeiten als auch über mögliche Konsequenzen der Einstellungen informiert gewesen. Sie habe sich entschieden, bestimmte Daten öffentlich einsehbar auf dem Facebook-Profil zu teilen. Die geltend gemachten Ansprüche seien deshalb gegenüber der Beklagten nicht berechtigt.

Entscheidungsgründe:

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

Das Landgericht Wiesbaden ist international, örtlich und sachlich zuständig. 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 dem Gericht des Mitgliedsstaates erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat. Daraus folgt die internationale Zuständigkeit, da die Klägerin ihren Wohnsitz in Hochheim am Main hat. Die örtliche Zuständigkeit ergibt sich aus Artikel 18 Abs. 1 Alt. 2 EuGVVO sowie Art. 79 Abs. 2 S. 2 DS-GVO. Die sachliche Zuständigkeit ergibt sich aus §§ 23 Nr. 1, 71 Abs. 1 GVG, da der Streitwert mehr als 5.000,00 € beträgt.

Der Klageantrag zu Ziffer 1) ist zulässig, dem steht nicht entgegen, dass hier kein konkreter Betrag geltend gemacht wird, sondern ein offener Antrag gestellt wird. Dies ist bei einem immateriellen Schadenersatzanspruch (Schmerzensgeld) zulässig, da die Bezifferung von einer Schätzung des Gerichts nach § 287 ZPO abhängt. Die Klägerin hat ihre Vorstellung geltend gemacht, in deren Höhe sich ein entsprechender Schadenersatzbetrag bewegen sollte. Zudem sind die hierfür erforderlichen Tatsachengrundlagen mitgeteilt worden, sodass der Antrag hinreichend bestimmt ist.

Auch der Antrag zu 2) als Feststellungsantrag ist hinreichend bestimmt, das erforderliche Feststellungsinteresse gem. § 256 Abs. 1 ZPO liegt vor, die Klägerin hat die Möglichkeit des Eintritts zukünftiger materieller Schäden hinreichend deutlich gemacht. Hierbei kommt es nicht darauf an, dass derartige Schäden wahrscheinlich sind. Der Eintritt des Schadens kann durchaus noch ungewiss sein. Dem Feststellungsinteresse steht es nicht entgegen, dass der Antrag sich auf bereits entstandene Schäden bezieht, aufgrund der Veröffentlichung der personenbezogenen Daten der Klägerin im Internet kann nicht ausgeschlossen werden, dass diese Daten

bereits zu illegalen Zwecken verwendet worden sind, die der Klägerin bislang noch nicht bekannt geworden sind. Auch der Antrag zu Ziffer 3 ist insgesamt zulässig.

Der Klägerin steht gegen die Beklagte ein Anspruch auf Schadenersatz in Höhe von 600,00 € aus Art. 82 Abs. 1 DS-GVO zu. Diese Anspruchsvoraussetzungen sind gegeben. Die Beklagte hat gegen Art. 25 Abs. 2 DS-GVO, gegen Art. 13 Abs. 1 c DS-GVO, gegen Art. 23, gegen Art. 24 i. V. m. Art. 25 Abs. 1 c DS-GVO, gegen Art. 33 DS-GVO und gegen Art. 34 Abs. 1 DS-GVO verstoßen.

Gemäß Art. 82 DS-GVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung einer materieller oder immaterieller Schaden entsteht, Anspruch auf Schadenersatz gegen den Verantwortlichen oder Auftragsverarbeiter. Gemäß Art. 82 Abs. 1 DS-GVO haftet der Verantwortliche für Schäden wegen „Verstößen gegen diese Verordnung“. Insoweit hat die Beklagte gem. Art. 25 Abs. 2 DS-GVO verstoßen. Hiernach hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen nur persönliche Daten, deren Verarbeitung für den jeweilig bestimmten Verarbeitungszweck erforderlich sind, 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. Die vom Nutzer veröffentlichten Informationen dürfen nicht ohne Einschränkungen der allgemeinen Öffentlichkeit zugänglich gemacht werden, sondern dies muss aktiv erst in den Privatsphäre-Einstellungen durch den Nutzer eingerichtet werden. Erforderlich für den Verarbeitungszweck im Sinne von Art. 25 Abs. 2 Satz 1 sind Daten nur dann, wenn der Verarbeitungszweck sich ohne sie nicht erreichen lässt. Derartige Daten darf der Verantwortliche auch ohne eine entsprechende Voreinstellung verarbeiten. Für solche Daten, die der Verantwortliche nicht notwendig verarbeiten muss, um die legitimen Zwecke der Verarbeitungserlaubnis erfüllen zu können, ist ihm der Weg der Voreinstellung demgegenüber verschlossen. Hier liegt ein Verstoß der Beklagten vor, bei der sogenannten „Zielgruppenauswahl“. Auf der Plattform der Beklagten legt der Nutzer fest, wer einzelne Informationen auf seinem Profil, wie etwa Telefonnummern, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adressen einsehen können darf. Dabei ist standardgemäß 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 und die hinter den Telefonnummern 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 der Telefonnummer zu finden, solange ihre „Suchbarkeits-Einstellung“ für Telefonnummer auch der Standardvoreinstellung „alle“ einge-

stellt ist. Dies so ermöglichte Datenerhebung ist nicht zwingend für die die Belange der Beklagten erforderlich, ebenso wenig zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten. Es mag zwar für die Nutzer der Facebook-Plattform je nach deren Auffassung durchaus nützlich und sinnvoll sein, erforderlich für die Nutzung schlechthin ist diese Art der Verbreitung von Daten allerdings nicht. Dies ergibt sich bereits daraus, dass diese Einstellungen nicht zwingend sind, sondern durchaus von den Nutzern auch andere, eingeschränkte Einstellungen gewählt werden können. Dies wäre dann nicht der Fall, wenn die Informationen unabdingbar gewesen wären.

Die Beklagte kann sich auch nicht darauf berufen, dass Sinn und Zweck der Facebook-Plattform es gerade sei, 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 Datenschutzgrundverordnung. Die Beklagte darf nicht durch die Definition ihres Leistungsangebotes den Umfang der zulässigen Datenverarbeitung unter Hintanstellung der Nutzerinteressen alleine an ihrem Interesse an der Vermarktung eines durch die Internetnutzung innerhalb und außerhalb von Facebook generierten Bestandes personenbezogener Daten der Nutzer ausgerichtet sein und über das für die Benutzer der sozialen Netzwerke erforderliche Maß hinausgehen. Es ist auch nicht ausreichend, dass die Nutzer über die Möglichkeit der Anpassung ihrer Suchbarkeitseinstellungen und Zielgruppenauswahl informiert werden. Bereits die Voreinstellung, die die Beklagte hinsichtlich einzelner Aspekte mit „öffentlich“ einräumt, läuft den Erfordernissen des Art. 25 Abs. 2 DS-GVO ausdrücklich zuwider. Die Beklagte kann sich auch nicht darauf berufen, hier einen „Hilfebereich“ zur Verfügung gestellt zu haben, da dieser nur von denjenigen Nutzern überhaupt aufgesucht wird, die die Notwendigkeit einer Änderung für sich wahrgenommen haben. Dass es bei einem Nutzer, der die Anmeldeprozedur mit vorgegebenen Einstellungen durchläuft, nicht notwendigerweise der Fall. Hierbei ist eher davon auszugehen, dass ein Interessent, der die Angebote der Beklagten nutzen möchte, davon ausgeht, dass er am einfachsten durch die Anmeldung kommt, wenn er die vorgenannten Einstellungen akzeptiert und wahrnimmt, dabei geht der Nutzer auch davon aus, dass dies die Einstellungen sind, die seinen Interessen am ehesten entsprechen. Dass hierbei Verstöße gegen die Datenschutzgrundverordnung vorliegen können, ist nicht jedem Benutzer bekannt, nicht jeder Benutzer wird überhaupt daran denken, dass dies möglich sein könnte.

Durch den Verstoß gegen Art. 25 Abs. 2 DS-GVO wird hier ein Ersatzanspruch der Klägerin ausgelöst. Der entgegenstehenden Auffassung ist nicht zu folgen, die wegen des organisatorischen Charakters von Art. 25 DS-GVO einen Anspruch aus Art. 82 Abs. 1 DS-GVO nicht annimmt. Dem ist nicht zu folgen, da eine Datenverarbeitung auch dann eine Haftung auslösen kann, wenn bei dem eigentlichen Verarbeitungsvorgang vor- oder nachgelagerte Pflichten ver-

letzt werden. Auch solcherlei Pflichtverstöße können einen Schadenersatzanspruch begründen, wenn diese im Zusammenhang mit einer Datenverarbeitung stehen und dies letztlich zu einem Schaden auf Seiten der Klägerin führt. Dies ergibt sich hier insbesondere daraus, dass bei einer Voreinstellung, die mit Art. 25 Abs. 2 DS-GVO konform gewesen wäre, ein Abgreifen der Mobiltelefonnummer der Klägerin so, wie letztlich geschehen, nicht ohne weiteres möglich gewesen wäre, denn bei einer entsprechenden Voreinstellung der Suchbarkeits-Einstellung wäre die Telefonnummer nicht öffentlich zugänglich gewesen, sondern allenfalls aufgrund einer individuellen Auswahl der Klägerin.

Darüber hinaus ist die Beklagte der ihr nach Art. 13 Abs. 1 c DS-GVO auferlegten Informations- und Aufklärungspflicht nicht in vollständigem Umfang nachgekommen. Hierdurch wird die Beklagte als Verantwortliche verpflichtet, bestimmte Informationen über die betreffende Datenverarbeitung von sich aus, d. h. ohne besondere Aufforderung, zur Verfügung zu stellen. Im Einzelnen ergeben sich Informationspflichten aus Art. 13 zum einen, wenn die Daten bei der betroffenen Person erhoben werden, zum anderen aber auch, zu welchem Zweck die Daten weiterverarbeitet werden. Die Angaben müssen vollständig und so detailliert sein, dass die betroffene Person sich ein Bild davon machen kann, mit welchen Datenverarbeitungen zu rechnen ist. Mit dieser Information legt somit der Verantwortliche den Verarbeitungszweck oder die Verarbeitungszwecke gegenüber der betroffenen Person verbindlich fest. Gegen diese Voraussetzungen hat die Beklagte verstoßen, sie hat zum Zeitpunkt der Datenerhebung der Klägerin nicht in ausreichendem Maße mitgeteilt, zu welchem Zweck die Mobilfunknummer verarbeitet werden könnte. Die entsprechende Information hätte hier zum Zeitpunkt der Erhebung der Daten mitgeteilt werden müssen. Dem hat die Beklagte zumindest hinsichtlich der Verwendung der Mobilfunknummer der Klägerin für das von ihr verwendete Kontakt-Importer-Tool nicht genügt. Durch dieses Tool wird dem Nutzer ermöglicht, die in seinem Smartphone gespeicherten Kontakte mit den auf Facebook registrierten Nutzerprofilen abzugleichen, 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. Aus den vorliegenden Unterlagen ist allerdings nicht ersichtlich, dass die Klägerin hierüber aufgeklärt worden wäre. Es wird nicht deutlich genug darauf hingewiesen, dass nicht nur die Klägerin ihre Mobilfunknummer nutzen kann, sondern auch andere Nutzer die Klägerin über diese Nummer finden können. Die eigene Möglichkeit mit Hilfe der Mobilfunknummer Kontakte herzustellen, impliziert hier nicht automatisch, dass auch andere Nutzer ohne eine entsprechende ausdrückliche Freigabe durch die Klägerin diese über ihre Mobilfunknummern ermitteln können. Auf diese Möglichkeit, die für einen Nutzer wesentlich beeinträchtigender sein kann, wird nicht ausreichend hingewiesen. Es wird die Möglichkeit für den Nutzer selbst, mit anderen in Kontakt zu treten, in den

Vordergrund gestellt, was regelmäßig ja auch Sinn und Zweck einer entsprechenden Nutzung der Plattform der Beklagten sein dürfte.

Auch ein Verstoß gegen Art. 13 Abs. 1 c DS-GVO kann einen Ersatzanspruch nach Art. 82 Abs. 1 DS-GVO auslösen.

Zudem lag bei der Beklagten als Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO auch ein Verstoß gegen Art. 32, 24, 5 Abs. 1 f DS-GVO vor. Gemäß Art. 32 Abs. 1 Halbsatz 1 DS-GVO ist die Beklagte dafür verantwortlich, entsprechend dem Stand der Technik, der damit verbundenen Risiken sowie der Rechte und Freiheiten der Nutzer geeignete technische und organisatorische Maßnahmen zu schaffen, um ein dem Risiko angemessenes Schutzniveau zu gewähren. Hierdurch wird die als Generalauftrag gestaltete Datensicherheitsmaßnahme des Art. 24 DS-GVO konkretisiert, die Regelung dient damit u. a. der Gewährleistung der Absicherung der Datenschutzgrundsätze, der Vertraulichkeit und Integrität nach Art. 5 Abs. 1 f DS-GVO. Entsprechend sollen insbesondere personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen davor geschützt werden, dass Dritte diese unbefugt oder unrechtmäßig verarbeiten oder es unbeabsichtigt zu einem Verlust, einer Zerstörung oder Schädigung der Daten kommt. Die DS-GVO legt zur Bemessung der Geeignetheit der Maßnahmen insbesondere fest, dass diese ein dem Risiko der Verarbeitung angemessenes Schutzniveau erreichen müssen. Dabei kommt es letztlich darauf an, wie groß das Risiko ist, das den Rechten der betroffenen Person droht und wie hoch die Wahrscheinlichkeit eines Schadeneintritts ist. Ein absolutes Schutzniveau wird hierdurch nicht gefordert. Dieses muss vielmehr, je nach Verarbeitungskontext, dem Risiko bezüglich der Rechte und Freiheiten der betroffenen Personen im Einzelfall angemessen sein. Ein Risiko kann somit nicht völlig ausgeschlossen werden. Diesen Voraussetzungen genügen allerdings die Schutzmaßnahmen der Beklagten nicht. Gerade das Kontakt-Importer-Tool ermöglicht einen unbefugten Zugang im Sinne von Art. 32 Abs. 2 GS-GVO. Ein entsprechender Schutz lag hier offensichtlich nicht vor, da dieses Tool gerade wie im vorliegenden Fall zu Missbrauchszwecken genutzt werden konnte. Es wird hier mit Dritten eine Zuordnung von Telefonnummern zum Nutzerprofil ermöglicht. Es kann in Erfahrung gebracht werden, welche konkrete Person hinter der fraglichen Telefonnummer steht. Über den Rückgriff auf das Nutzerprofil können sodann weitere Informationen über diese Person eingeholt werden. Dies birgt für den Nutzer das Risiko von gezielten Phishing-Attacken, Identitätsdiebstahl und weiterem Missbrauch der Daten und damit dem Eintritt von materiellen oder immateriellen Schäden. Aufgrund dieses hohen Risikos sind auch die Anforderungen an entsprechende Schutzmaßmaßnahmen entsprechend hoch anzusetzen. Dabei war der Beklagten nach eigenen Angaben die Funktionsweise des „Scrapings“ durchaus bekannt, die Beklagte hat dies aber letztlich als unvermeidbares Risiko angesehen. Hierbei hätten entsprechende Scraping-Versuche bereits effektiver vorgebeugt werden können. Beispielsweise sind sogenannte Capcha-Abfragen bereits bei relativ geringen Risiken im Umgang mit personen-

bezogenen Daten durchaus üblich. Derartige Maßnahmen hat die Beklagte hier offensichtlich nicht ergriffen. Beispielsweise hätten auch Sicherheitsvorkehrungen dadurch getroffen werden können, dass lediglich über eine Telefonnummer-Abfrage der Zugang zu den Daten gewährleistet wird, sondern hier weitere Angaben erforderlich gewesen wären, beispielsweise die entsprechende Nennung eines Namens, der der Telefonnummer zugeordnet werden kann. Dies hätte einen Zugriff alleine über entsprechend generierte Telefonnummern erheblich erschwert, da eine Kombination aus Zahlen und Buchstaben beispielsweise nicht derart häufig willkürlich zusammengestellt werden könnte. Auch eine Begrenzung der abgleichbaren Rufnummer durch eine entsprechende zahlenmäßige Einschränkung hätte hier durchaus zum Erfolg führen können und für einen Zugriff auf auch erhöhte Schranken aufbauen können, dies letztlich für den Zugriff von außen völlig unattraktiv machen können. Dass möglicherweise im Einzelfall nicht sämtliche Risiken ausgeschlossen werden könnten, steht dem nicht entgegen. Hier handelt es sich gerade nicht um einen Einzelfall, sondern wie unstreitig um einen Fall, bei dem über 500 Millionen Nutzer der Facebook-Plattform betroffen waren. Gerade derartige großflächige Angriffe wären durch geeignete Maßnahmen der Beklagten durchaus zu verhindern gewesen. Weitere von der Beklagten hier dargestellte Schutzmaßnahmen sind ersichtlich erst nach dem streitgegenständlichen Vorfall vorgenommen worden, diese können somit nicht zu einer Entlastung der Beklagten führen. Letztlich hat die Beklagte auch ihre Meldepflicht aus Art. 33 DS-GVO verletzt. Eine Verletzung des Schutzes personenbezogener Daten hätte demnach spätestens 72 Stunden nach der Verletzung bekanntgemacht werden müssen gem. Art. 55 DS-GVO gegenüber der zuständigen Aufsichtsbehörde. Es hat hier auch eine massive Verletzung personenbezogener Daten vorgelegen, wie bereits ausgeführt.

Zudem kann ein Verstoß gegen Art. 34 Abs. 1 DS-GVO festgestellt werden. Hiernach ist die betroffene Person von einer Verletzung des Schutzes personenbezogener Daten zu unterrichten, wenn hieraus voraussichtlich ein hohes Risiko für persönliche Rechte und Freiheiten zu befürchten ist. Diese Benachrichtigung muss auch grundsätzlich gegenüber der betroffenen Person direkt erfolgen. Eine derartige konkrete Information hat die Beklagte nach Offenbarung der Verletzung des Schutzes personenbezogener Daten im Jahr 2019 nicht gegenüber der Klägerin vorgenommen. Dass durch die Verletzung des Schutzes personenbezogener Daten sich hier ein hohes persönliches Risiko ergeben hat, wurde bereits ausgeführt.

Ein Verstoß gegen Art. 15 Abs. 1 DS-GVO liegt demgegenüber nicht vor. Die Klägerin hatte die Beklagte außergerichtlich zur Auskunft aufgefordert, eine entsprechende Auskunft wurde von der Beklagten auch erteilt. Weitergehende darüber hinaus gehende Auskunftsansprüche stehen der Klägerin nicht zu. Die Beklagte hat hier eindeutig zu erkennen gegeben, nach ihrer Auffassung eine entsprechende Auskunft erteilt zu haben, die vollständig und abschließend war. Auf die Frage, ob diese Auskunft inhaltlich zutreffend ist oder nach Vorstellung der Klägerin vollständig ist, kommt es hierbei nicht an.

Aufgrund der vorgenannten Umstände hat die Klägerin Anspruch auf Ersatz eines immateriellen Schadens. Der Begriff des Schadens ist hier unter Berücksichtigung der Ziele der Datenschutzgrundverordnung weit auszulegen. Der Anspruch ergibt sich aus Art. 82 der Datenschutzgrundverordnung, sodass hier der Schadensbegriff europarechtlich anzusehen ist, nationale Erheblichkeitsschwellen oder andere Einschränkungen sind hierbei nicht zu berücksichtigen. Es kommt auch nicht darauf an, ob hier ausschließlich schwerwiegende Persönlichkeitsrechtsverletzungen angenommen werden können. Vorliegend ist es demgegenüber so, dass bei Verstößen gegen datenschutzrechtliche Normen der Datenschutzgrundverordnung grundsätzlich immer auch von einem immateriellen Schaden auszugehen ist. Dies begründet sich bereits daraus, dass mit einer rechtswidrigen Zugänglichmachung von Daten bereits ein Identitätsdiebstahl vorliegt, die betroffene Person keinerlei Kontrolle mehr über die Verwendung ihrer Daten hat und in keiner Weise eingrenzen kann, wer des Weiteren über ihre Daten verfügen kann. Hier ist auch die Frage einer missbräuchlichen Nutzung der Daten nicht fernliegend, vielmehr ist die Befürchtung der Klägerin, dass ihre Daten zu weiteren Straftaten u. ä. benutzt werden sollten, durchaus nachvollziehbar. Ansonsten wäre auch nicht erklärlich, inwieweit ein Datendiebstahl in derart großem Umfang überhaupt unternommen werden sollte, wenn hier nicht weitere Gründe vorliegen, um die so erlangten Daten auch entsprechend zu rechtswidrigen Zwecken zu nutzen. Damit steht zur Überzeugung des Gerichts fest, dass hier auch bei der entsprechenden Datenpanne nicht lediglich von einem subjektiv unguten Gefühl der Betroffenen ausgegangen werden kann, sondern hier tatsächlich nachvollziehbar ist, dass erhebliche Beeinträchtigungen befürchtet werden, was zu einem immateriellen Schadenersatz führt. Grundsätzlich steht das Recht an den die Person betreffenden Daten lediglich dieser zu und die Person ist berechtigt, in gewissem Umfang darüber zu verfügen. Alleine durch die Anmeldung auf der Plattform der Beklagten hat sich die Klägerin hier nicht sämtliche Rechte bezüglich ihrer dort vorhandenen Daten begeben, sondern hätte grundsätzlich auch steuern können, wie und an wen diese Daten weitergegeben werden könnten. Das Vertrauen darauf ist massiv gestört worden, auch dies lässt eine psychische Beeinträchtigung durchaus nachvollziehbar erscheinen. Wie bereits zuvor ausgeführt, war eine derartige Ermöglichung des „Daten-Leaks“ durch die Beklagte als rechtswidrig und schuldhaft anzusehen. Auch ein Mitverschulden der Klägerin gem. § 254 Abs. 1 BGB kann hier nicht angenommen werden. Jedenfalls würde ein etwaiges Mitverschulden, weil die Klägerin die Datenschutzeinstellungen ihres Facebook-Profils nicht geändert hat und dadurch auch den Zugriff der Daten-Scraper mitermöglicht hat, hinter die Verstöße der Beklagten zurücktreten. Denn das Verhalten der Klägerin, die die von der Beklagten vorgegebenen Voreinstellungen schlicht und einfach belassen hat, ist gerade von der Beklagten initiiert und mit Blick auf den von ihr angenommenen Sinn und Zweck der Facebook-Plattform durchaus auch gewünscht gewesen. Unter diesen Umständen kann die Beklagte sich, wenn sich die Gefahr, die sich durch ihr ordnungswidriges Verhalten ergeben hat, realisiert hat, nicht darauf berufen, es sei dem Kläger dies im Schutze

seiner personenbezogenen Daten möglich gewesen, einzugreifen. Bezüglich des Kontakt-Importer-Tools ist es allerdings so, dass über dessen Funktionsweise auch gar nicht entsprechend aufgeklärt worden war, sodass hier diesbezüglich auf keinen Fall ein Mitverschulden angenommen werden könnte.

Der Anspruch auf Ersatz des immateriellen Schadens ist entsprechend dem Begehren der Klägerin für den lediglich als gerechtfertigt angesehenen Ersatzanspruch wegen der Verstöße im Zusammenhang mit dem Daten-Scraping-Vorfall auf 600,00 € zu bemessen. Hiermit kann der Ausgleichs- und Genugtuungsfunktion des Schadenersatzanspruches für immaterielle Schäden ausreichend genüge getan werden. Hiermit ist der „Kontrollverlust“ der Klägerin über ihre Daten entsprechend berücksichtigt. Dass tatsächlich aufgrund der Vorfälle die Klägerin mit Anrufen, Spam-E-Mails u. ä. aufgrund dieser Vorfälle kausal beeinträchtigt ist, ist demgegenüber nicht nachgewiesen. Insoweit wirkt sich dies nicht erfüllend auf den Schadenersatzanspruch aus.

Da allerdings auch nicht ausgeschlossen werden kann, dass die Klägerin aufgrund des Datenverlustes tatsächlich in der Zukunft auch materielle Schäden erleiden kann, war auch dem Antrag zu Ziffer 2 stattzugeben.

Auch die geltend gemachten Unterlassungsansprüche seitens der Klägerin sind begründet. Auch wenn es in der Datenschutzgrundverordnung einen besonderen Unterlassungsanspruch hier nicht gibt, kann im Hinblick auf die Vorgaben des Art. 79 DS-GVO entweder ein Rückgriff auf § 823 Abs. 2, 1004 analog ermöglicht werden, um Schutzlücken zu vermeiden oder ein solcher Anspruch folgt mit Blick auf die unrechtmäßige Datenverarbeitung seitens der Beklagten aus Art. 17 Abs. 1 d DS-GVO, falls man annimmt, aus dem dort normierten Löschungsrecht lasse sich auch ein Unterlassungsanspruch herleiten. Die Beklagte hat gegen Art. 25 Abs. 2 DS-GVO, Art. 13 Abs. 1 c DS-GVO, Art. 32, Art. 25, 5 Abs. 1 f, gegen Art. 33 DS-GVO und Art. 34 Abs. 1 DS-GVO verstoßen. Diese Rechtsverstöße geben der Klägerin einen darauf bezogenen Anspruch auf Beseitigung der zukünftigen Unterlassung. Daher kann die Klägerin verlangen, dass die Beklagte es unterlässt, personenbezogene Daten, insbesondere Telefonnummern, unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen. In gleicher Weise kann sie beanspruchen, dass die Beklagte es unterlässt, personenbezogene Daten, insbesondere Telefonnummern, ohne Einholung der Einwilligung oder Erfüllung sonstiger gesetzlicher Erlaubnistatbestände zu verarbeiten. Dem steht auch nicht entgegen, dass die Klägerin durch entsprechende Änderung ihrer Einstellungen auf der Facebook-Plattform einen entsprechenden Zugriff selbst erschweren könnte. Hierdurch entfällt die Wiederholungsgefahr nicht. Die Klägerin kann grundsätzlich Unterlassung jeder einmal getätigten rechtswidrigen Datenverarbeitung verlangen. Im Falle eines rechtswidrigen Angriffs ist ein geschütztes Rechtsgut der Klägerin betroffen, es spricht deshalb eine tat-

sächliche Vermutung für das Vorliegen der Wiederholungsgefahr. Zur Entkräftung dieser Wiederholungsgefahr ist regelmäßig einer strafbewehrten Unterlassungserklärung erforderlich. Eine solche hat die Beklagte hier nicht abgegeben.

Die Androhung von Ordnungsmitteln rechtfertigt sich aus § 890 ZPO.

Der Anspruch auf Ersatz der außergerichtlichen Rechtsanwaltskosten ergibt sich im Rahmen des materiellen Schadenersatzes ebenfalls aus Art. 82 Abs. 1 DS-GVO.

Die Berechnung der Kostenverteilung ergibt sich aus dem Streitwert, der insgesamt auf 6.000,00 € festgesetzt wird.

Die Entscheidung zur vorläufigen Vollstreckbarkeit ergibt sich aus §§ 708 Nr. 11, 709, 711 ZPO.

Vorsitzende Richterin
am Landgericht

Beglaubigt
Wiesbaden, 28.09.2023

Urkundsbeamtin der Geschäftsstelle