Beglaubigte Abschrift

14 C 624/22

Amtsgericht Siegen

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

des Herrn

Klägers,

Prozessbevollmächtigte:

gegen

die Meta Platfoms Ireland Ltd., ertreten durch den Geschäftsführer (Director) Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland,

Beklagte,

Prozessbevollmächtigte:

hat das Amtsgericht Siegen
auf die mündliche Verhandlung vom 09.03.2023
durch die Richterin am Amtsgericht S

für Recht erkannt:

I.

1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in Höhe von 500,00€ nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 13.06.2022 zu zahlen.

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

b) die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne

eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.

4. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 280,60 € zu zahlen, zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 13.06.2022.

Im Übrigen wird die Klage abgewiesen.

II.

Die Kosten des Rechtsstreits tragen der Kläger zu 1/4 und die Beklagte zu 3/4.

III.

Das Urteil ist vorläufig vollstreckbar, für den Kläger wegen des Antrags zu 2) gegen Sicherheitsleistung in Höhe von 600€, wegen des Antrags zu 3) gegen Sicherheitsleistung in Höhe von 1200€.

Die Beklagte kann die Vollstreckung durch den Kläger im Übrigen gegen Sicherheitsleistung in Höhe von 110% des zu vollstreckenden Betrages abwenden, wenn nicht der Kläger vor der Vollstreckung Sicherheit in gleicher Höhe leistet.

IV.

Der Wert für den Rechtsstreit wird auf 2600€ festgesetzt.

Tatbestand

Die Parteien streiten über Ansprüche wegen behaupteter Verstöße gegen die Datenschutz Grundverordnung (DSGVO).

Der Kläger ist Nutzer der social-media Plattform „facebook.com“. Die Beklagte ist Anbieterin ebendieser auf dem Gebiet der europäischen Union. Die Plattform ermöglicht es Nutzern persönliche Profile und Informationen zu erstellen und diese in einem digitalen Freundeskreis und darüber hinaus zu teilen. Im Rahmen der Registrierung gab der Kläger seinen Vornamen, Nachnamen, sein Geburtsdatum und Geschlecht an. Die Mitteilung einer Handynummer ist fakultativ, gleichwohl gab der Kläger auch diese an. Auf der Registrierungsseite fand sich noch folgender Passus:

„Indem du auf Registrieren klickst, stimmst du unseren Nutzungsbedingungen zu. In unserer Datenrichtlinie erfährst du, wie wir deine Daten erfassen, verwenden und teilen“. Für die weiteren Einzelheiten wird auf die Registrierungsabbildung (klägerischer Schriftsatz v. 01.07.2022, dort auf Seite 9 ff.) Bezug genommen. Die Datenverwendungsrichtlinien enthielten u.a. Angaben dazu, welche der vom Nutzer erteilten Informationen immer öffentlich zugänglich sind – nämlich Name, Profil- und Titelbilder, Netzwerke, Geschlecht, Nutzername und Nutzer-ID – und die Angabe, dass öffentlich zugängliche Informationen jeder, also auch Personen außerhalb von der Plattform der Beklagten, sehen kann. Die Beklagte stellt ihren Nutzern der Plattform Erklärungen, was öffentliche Informationen sind und welche Informationen öffentlich sind, wie der Nutzer festlegen kann, wer die von ihm über die öffentlichen Informationen hinaus bereitgestellten Informationen sehen kann (Zielgruppenauswahl) und wer ihn anhand seiner E-Mail-Adresse oder seiner Telefonnummer, sofern er E-Mail-Adresse bzw. Telefonnummer auf der Plattform bereitgestellt hat, finden kann (Suchbarkeits- und Kontaktierungseinstellungen), zur Verfügung. Trifft der Nutzer keine Zielgruppenauswahl, richtet sich die Zugänglichkeit seiner über die öffentlichen Informationen hinausgehenden Informationen nach der Standardeinstellung, wonach Freunde des Nutzers die weiteren Informationen einsehen können. Dann gilt: „Inhalte, die öffentlich sind, können von jedem gesehen werden. Dazu zählen auch Personen, die nicht deine Freunde sind, die facebook nicht nutzen und die Inhalte über andere Medien wie Druckmedien, Rundfunk (z. B. Fernsehen) und andere Webseiten im Internet ansehen. Wenn du beispielsweise

unsere Dienste nutzt, um in Echtzeit einen öffentlichen Kommentar zu einer Fernsehsendung abzugeben, kann dieser Kommentar in der Sendung oder an einer anderen Stelle auf facebook erscheinen.

Welche Informationen sind öffentlich?

Informationen, die du teilst, die immer öffentlich sind: Einige Informationen, die du uns zur Verfügung stellst, wenn du dein Profil erstellst, sind öffentlich, z. B. dein Alter, dein Geschlecht, deine Sprache und dein Land. Darüber hinaus verwenden wir teilweise Informationen deines Profils, des sogenannten „öffentlichen Profils“, damit du leichter mit deinen Freunden und deiner Familie in Kontakt treten kannst. Dein öffentliches Profil umfasst deinen Namen, dein Geschlecht, deinen Nutzernamen und die Nutzer-ID (Kontonummer), dein Profilbild, dein Titelbild und deine Netzwerke. Diese Informationen sind ebenfalls öffentlich. Hier sind einige der Möglichkeiten, über die wir dich mit anderen Personen verbinden:

- Dein Name, Profilbild und Titelbild helfen den Menschen dabei, dich zu erkennen
- Dein Geschlecht hilft uns, dich zu beschreiben (z. B. „Füge sie als Freundin hinzu“).
- (…)
- Nutzername und Nutzer-ID (z. B. deine Kontonummer) befinden sich in der URL deines Profils
- (…).“

Passt der Nutzer die Suchbarkeits-Einstellungen nicht an, sieht die Standardeinstellung vor, dass alle Personen, die über die E-Mail-Adresse oder die Telefonnummer des Nutzers verfügen, das Profil des Nutzers, sofern dieser E-MailAdresse bzw. Telefonnummer bereitgestellt hat, finden können. Dies gelang über das digitale Contact-Import-Tool (CIT). Hiermit war es anderen Nutzern der Plattform möglich, einen Zugriff auf die Kontakt-Liste auf einem digitalen Endgerät (z.B. Smartphone, PC etc.) zu erlauben. Hiermit verbunden war ein automatisierter Abgleich zwischen den in der Kontakt-Liste enthaltenen Kontaktdaten (Telefonnummer oder E-Mail Adresse) und den der Plattformbetreiberin zugänglichen Kontaktdaten ihrer Nutzer. Kam es hier zu einer Korrelation, wurde das mit den Kontaktdaten korrelierende Profil dem suchenden Nutzer angezeigt.

Die Beklagte wies die Nutzer der facebook- Plattform in der EU im Zusammenhang mit dem Geltungsbeginn der DSGVO am 25. Mai 2018 auf die Datenrichtlinie hin. In Vorbereitung des Geltungsbeginns wurden die Nutzungsbedingungen und die Datenrichtlinie der Beklagten im April 2018 aktualisiert und die Beklagte forderte die Nutzer zur Überprüfung ihrer Privatsphäreeinstellungen auf.

In der Zeit von Januar 2018 bis September 2019 sammelten Dritte unter Nutzung automatisierter IT-Verfahren eine Vielzahl der auf der Plattform der Beklagten verfügbaren öffentlichen Informationen (sog. Scraping). Das Vorgehen in allen Einzelheiten ist bis heute nicht öffentlich bekannt. Allerdings wird allseits von folgendem Vorgehen ausgegangen: Die Dritten (sog. Scraper) erstellten Listen mit möglichen Telefonnummern und luden diese in das CIT der Plattform hoch, um so festzustellen, ob die hochgeladenen Telefonnummern mit einem Konto eines Nutzers verbunden sind. Der Kontakt-Importer gab, sofern eine der hochgeladenen Telefonnummern mit dem Konto eines Nutzers verknüpft war, diese Information, also den Umstand der Verknüpfung von Telefonnummer und Konto, an die Dritten. Dies war jedoch nur möglich, wenn der Nutzer die originäre Suchbarkeits- und Kontaktierungseinstellungen auf der Plattform nicht geändert hatte, der fragliche Nutzer also der Suche über das CIT gegenüber allen anderen Nutzern offenstand. Die Scraper fügten sodann den öffentlich zugänglichen Informationen aus dem betreffenden Profil des Nutzers die mit dem Konto verknüpfte Telefonnummer hinzu.

Anfang April 2021 wurden die so erlangten Datensätze von über 500 Mio. Nutzern aus mehreren Ländern sowie die mit diesen Datensätzen verknüpften persönlichen Daten (Telefonnummern, Name, Vorname, Geschlecht, Herkunftsland etc.) im Internet frei zum Download bereitgestellt. Hierzu gehörten auch die immer öffentlich zugänglichen Informationen des Profils des Klägers und die mit seinem Konto verknüpfte Telefonnummer.

Der Kläger verlangte über seine Prozessbevollmächtigten zunächst Auskunft über die ihn bei der Plattform der Beklagten betreffenden Daten. Mit Schreiben vom 07.10.2021 (siehe Anlage K 1, Bl. 57 der Akte) forderte der Kläger die Beklagte über seinen Prozessbevollmächtigten zur Zahlung von 500 EUR Schadenersatz, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft über den Datenabgriff im April 2021 auf.

Mit Schreiben vom 23.08.2021 (Anlage K 2, Bl. 82 ff. der Akte) teilte die Beklagte dem Kläger mit, dass unter den abgegriffenen Daten auch die des Klägers enthalten waren und lehnte die Erfüllung weiterer Ansprüche ab. Die Prozessbevollmächtigten der Beklagten übermittelten dem Prozessbevollmächtigten des Klägers eine dezidierte Anleitung zur Einsichtnahme in seine bei der Plattform der Beklagten hinterlegten Informationen und deren Verwendung. Wegen des Inhalts wird auf Bl. 85 ff. der Akte Bezug genommen.

Die irische Datenschutzbehörde DPC verhängte gegen die Beklagte am 28.11.2022 eine Geldbuße in Höhe von 265 Mio. Euro. Die Behörde führte aus, dass die Beklagte es nicht ausreichend verhindert habe, dass etwa 533 Mio. Datensätze mit

persönlichen Informationen von Facebook-Nutzern und -Nutzerinnen abgegriffen und veröffentlicht wurden. Die vorbezeichnete Entscheidung ist nicht rechtskräftig. Die Beklagte hat hiergegen Rechtsmittel eingelegt.

Der Kläger ist der Ansicht, die Beklagte verstoße gegen die DSGVO, indem sie ohne ausreichende Grundlage im Sinne der Art. 6 und 7 DSGVO Informationen im Sinne von Art. 13, 14 DSGVO verarbeite, Daten unbefugten Dritten zugänglich mache sowie seine Rechte aus Art. 15, 17 und 18 DSGVO und seine Betroffenenrechte gemäß Art. 15, 17 und 18 DSGVO verletzte.

Der Kläger behauptet dazu, sämtliche seiner Daten auf „privat“ gestellt zu haben. Zur Sichtbarkeit seiner Telefonnummer habe er die Einstellung „nur ich“ gewählt. Seine Telefonnummer sei letztlich wegen einer Sicherheitslücke mit den restlichen Personendaten korreliert und Bestandteil des jeweiligen unbefugt verbreiteten Datensatzes geworden, wobei ihm die genaue Herangehensweise unbekannt sei. Soweit die Beklagte behaupte, er habe bei den Suchbarkeitseinstellungen seit 2013 angegeben, dass „everyone“ durch „search by Phone“ suchen könne, bestreite er dies mit Nichtwissen. Sicher sei aber, dass es Unbekannten gelungen sei, die Telefonnummern konkreten facebook- Profilen zuzuordnen, ohne dass in den entsprechenden Profilen die hinterlegten Telefonnummern öffentlich freigegeben worden seien. Er - der Kläger - behauptet, das „scrapen“ sei nur möglich gewesen, weil die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten Tools zu verhindern und weil die Einstellungen zur Sicherheit der Telefonnummer auf facebook so undurchsichtig und kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Nur so hätten auch seine Daten auf sog. Hackerforen wie „raidforums.com“ geraten können. Die Daten seien dann für sog. Phishing Attacken genutzt worden.

Der Beklagten sei die fehlerhafte Funktion des Contact-Import-Tools (CIT), namentlich diejenige, die es anderen facebook – Nutzern ermögliche, über ihr Adressbuch Telefonnummern von anderen facebook- Nutzern hochzuladen, ohne dass diese darin eingewilligt hätten, bekannt gewesen. Die Beklagte biete vor diesem Hintergrund die Löschung der Nummer aus der Adressbuch- Datenbank.

Facebook sei „datenschutzunfreundlich“ eingestellt, es werde unnötig zwischen Datenschutzrichtlinien und Cookie-Verwendung differenziert, obwohl die Verwendung von Cookies - so meint der Kläger - ein inhärent datenschutzrechtliches Thema sei. Der gesamte Anmeldevorgang sei intransparent und für den Anwender verwirrend. Dies führe letztlich - so behauptet der Kläger - dazu, dass Nutzer im

Vertrauen und mit dem Ziel, mehr persönliche Sicherheit zu erreichen, ihre Telefonnummern auf facebook preisgäben. Die neben der von der Beklagten betriebene Website noch betriebene Messenger-App als Schnittstelle für die facebook- Applikation auf Mobilgeräten und die besagte Website seien miteinander verknüpft. Bei erster Anmeldung frage der Messenger-Dienst die Synchronisierung bereits an, ohne über die Risiken der Verwendung aufzuklären. Es könne separat auf der App eingestellt werden, ob eine Synchronisierung erfolgen solle, ohne über Risiken aufzuklären. Insgesamt gebe es drei verschiedene Einstellungsmöglichkeiten zur Verwendung der Telefonnummer, über die ein Nutzer - so auch er als Kläger - keine transparenten Informationen für eine Gewährleistung einer effektiven digitalen Sicherheit erhalte. Diese Sicherheitslücke werde seit 2019 ausgenutzt, ohne dass die Beklagte etwas dagegen unternehme. Er - der Kläger - habe so ungewollt die Kontrolle über seine Daten verloren und werde bis heute wiederholt ungewollt von Unbekannten via E-Mail und SMS mit dubiosen Aufforderungen zum Anklicken von unbekannten Links kontaktiert. Außerdem erhalte er auch regelmäßig Anrufe von unbekannten Telefonnummern. Ihm sei insofern ein kausaler Schaden entstanden.

Der Kläger meint, die Beklagte habe auch nach dem Vorfall 2019 nicht adäquat reagiert. Sie habe versäumt, die zuständige Datenschutzbehörde „Irish Data Protection Commission“ unverzüglich zu informieren. Soweit vorgerichtlich Auskünfte über abgegriffene Daten mitgeteilt worden seien, sei diese Auskunft ungenügend.

Die Datenschutzeinstellungen der Beklagten seien undurchsichtig und kompliziert gestaltet, denn es bestehe eine Flut an Einstellungsmöglichkeiten allein für die Sicherheit der Mobilnummer. Aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte und nicht selbstständig ändere. Dies widerspreche - so meint der Kläger weiter - allerdings den Grundsätzen eines nutzerfreundlichen Datenschutzes und dem in der DSGVO niedergelegten Prinzips der „privacy by default“.

Die Auskunft, die die Beklagte ihm habe zukommen lassen, sei unzureichend. Das Antwortschreiben der Beklagten enthalte lediglich allgemein gehaltene Informationen zu den auf facebook verarbeiteten Daten sowie einen Link zur Seite der Beklagten, auf der die Daten über einen individuellen Nutzer gespeicherten Daten eingesehen werden könnten. Dieses Vorgehen allein sei schon nicht geeignet, dem nach Art. 15 DSGVO umfassenden Auskunftsanspruch gerecht zu werden. Unabhängig davon enthalte das „Auskunftsschreiben“ der Beklagten aber auch keinerlei konkrete Aussagen dazu, welche Daten der Klägerseite im Wege des Scrapings von unbekannten Dritten abgegriffen worden seien. So bleibe offen, wann genau die Daten entwendet worden seien oder wie viele verschiedene Beteiligte diese Funktion hinsichtlich seiner - des Klägers - Daten ausgenutzt hätten.

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, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

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

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

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

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte meint, der Sachverhalt und Vorgang zum sog. Scraping sei falsch wiedergeben. Der klägerische Vortrag beruhe auf einem Missverständnis zum Scraping als solchem. Es sei unschlüssig und unsubstantiiert, welche Daten des Klägers genau gescrapt worden sein sollen. Sie - die Beklagte - bestreite die Begehung eines Datenschutzverstoßes und eines Unterlassens des Schließens einer technischen Schwachstelle. Vielmehr seien - so behauptet die Beklagte - lediglich automatisch gesammelte öffentlich einsehbare Daten entweder von der App oder der Website facebook gescraped worden. Es seien lediglich öffentlich einsehbare Daten durch Dritte in Form des Scrapings abgerufen worden, was nach den Nutzungsbedingungen von facebook untersagt gewesen sei und noch untersagt sei. Das Abrufen habe im Einklang mit den jeweiligen Privatsphäre-Einstellungen „öffentlich“ auf der facebook-Plattform gestanden. Es seien allenfalls öffentlich einsehbare Daten abgerufen und an anderer Stelle erneut zugänglich gemacht worden. Sie - die Beklagte - stelle allen Nutzern, inklusive dem Kläger, alle in Art. 13 und 14 DSGVO festgelegten Informationen zur Datenverarbeitung zur Verfügung, die sie zum Zeitpunkt der Datenerhebung im Anwendungsbereich der Datenrichtlinie durchführe. Sie ist daher der Ansicht, nicht gegen die Transparenzpflichten der DSGVO verstoßen zu haben. Es habe zudem eine umfassende und transparente Information über die Möglichkeit der Anpassung ihrer Suchbarkeits-Einstellungen und Zielgruppenauswahl gegeben, woraus sich nachvollziehbar ergebe, wer bestimmte persönliche Informationen, die der Nutzer in seinem facebook- Profil hinterlegt habe, einsehen könne. Diese Einstellungen habe - so behauptet die Beklagte - der Kläger jederzeit anpassen können.

Soweit die Klägerseite auf eine „Benachrichtigung“ abstelle, sei eine solche nicht an sie adressiert gewesen oder ihr selbst zugegangen. Tatsächlich handele es sich nicht um eine „aktuelle Benachrichtigung der Beklagten an ihre Nutzer“. Vielmehr sei es ein Tool, welches die Beklagte auch Nicht-Nutzern zur Verfügung stelle, um zu überprüfen, ob Dritte ihre Telefonnummer bzw. ihre E-Mail-Adresse über die Kontakt-Importer-Funktion hochgeladen hätten. Sei dies der Fall, könne über das dargestellte Tool die Löschung der Telefonnummer bzw. der E-Mail-Adresse aus der betreffenden Kontaktdatenbank erreicht und verhindert werden, dass die Telefonnummer erneut über die Kontakt-Importer-Funktion in diese Datenbank

hochgeladen werde. Da die Klagepartei nach ihrem eigenen Vortrag ihre Telefonnummer selbst auf der Facebook-Plattform hinterlegt habe, sei dieses Tool für das vorliegende Verfahren ersichtlich irrelevant und könne keinesfalls die behauptete Kenntnis der Beklagten von der angeblich „fehlerhafte[n] Funktion des Contact-Import-Tools“ belegen.

Zu den konkreten vom Kläger gewählten Einstellungen behauptet sie - die Beklagte weiter -, dass der Kläger seit der Anmeldung die Suchbarkeitseinstellungen auf „öffentlich“ belassen habe, obwohl es hinreichende Hinweise und Erläuterungen gebe, welche Einstellungen wo und in welchem Umfang möglich seien.

Die Beklagte ist der Ansicht, nicht gegen Art. 24, 32 DSGVO verstoßen zu haben, sondern vielmehr angemessene technische und organisatorische Maßnahmen ergriffen zu haben, das Risiko von Scraping zu unterbinden und Maßnahmen zur Bekämpfung von Scraping zu ergreifen. Es fehle konkreter Vortrag, welche Maßnahmen in welchem Umfang nicht genügen würden. Außerdem müsse eine solche Beurteilung ex ante und nicht ex post erfolgen. Den Anforderungen des Art. 25 DSGVO sei genügt. Es dürfe dabei der zentrale Zweck von facebook, mit Freunden, Familien und Gemeinschaften sich zu verbinden, nicht außer Betracht bleiben. Es bestehe keine Melde- oder Benachrichtigungspflicht, da es an einer Verletzung der Sicherheit i. S. d. Art. 4 Nr. 12 DSGVO und an einer unbefugten Offenlegung von Daten fehle. Unabhängig davon habe sie - die Beklagte - wegen der Medienberichterstattung freiwillig eine Vielzahl von Maßnahmen ergriffen, über Scraping und Begrenzungsmöglichkeiten einschließlich einer Änderung von Privatsphäre-Einstellungen zu informieren.

Schließlich - so meint die Beklagte darüber hinaus - fehle es an einem immateriellen Schaden. Art. 82 DSGVO umfasse keine Verstöße gegen Art. 13-15, 24, 25 DSGVO. Zudem fehle es an einem Verstoß gegen Art. 82 DSGVO. Ein kompensationsgeeigneter messbarer Schaden sei auch nicht dargelegt. Die Klagepartei habe keine spürbare Beeinträchtigung erlitten. Für einen immateriellen Schaden sei aber eine spürbare tatsächliche Beeinträchtigung persönlichkeitsbezogener Belange von einigem Gewicht erforderlich Eine solche Beeinträchtigung habe die Klagepartei, auch im Rahmen ihrer informatorischen Anhörung, nicht dargelegt. Der Kontrollverlust über personenbezogene Daten des Klägers sei schon nicht ihr - der Beklagten - zuzurechnen, weil die öffentliche Einsehbarkeit den Privatsphäre-Einstellungen des Klägers entsprochen habe.

Schließlich fehle es an einer schlüssigen Darlegung der Kausalität.

Mangels Verstoßes gegen die DSGVO sei der (ohnehin unzulässige) Feststellungsantrag unbegründet. Der Unterlassungsanspruch scheitere an einer Erstbegehungs- und einer Wiederholungsgefahr.

Anwaltskosten seien mangels Verzuges unbegründet.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird ergänzend auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen Bezug genommen.

Der Kläger ist in dem Termin vom 09.03.2023 angehört worden. Es wird insoweit auf das Sitzungsprotokoll vom 09.03.2023 Bezug genommen.

Entscheidungsgründe

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

A) Zulässigkeit

I. Die Klage ist zulässig.

Das Amtsgericht Siegen ist international, sachlich und örtlich zuständig.
Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 2. Alt EuGVVO (Brüssel LaVo). Gemäß Art. 1 Abs. 1 EuGVVO ist die EuGVVO sachlich anwendbar auf Zivil- und Handelssachen. Vorliegend handelt es sich um eine Zivilsache. Die deutsche Gerichtsbarkeit folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 2. Alt EuGVVO. Ein ausschließlicher Gerichtsstand gemäß Art. 24 EuGVVO ist nicht ersichtlich. Gemäß Art. 18 Abs. 1 2. Alt 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 seinen Wohnsitz hat. Der Kläger ist gemäß Art. 17 Abs. 1 EuGVVO unzweifelhaft Verbraucher. Der Kläger hat seinen Wohnort in Deutschland. Die internationale Zuständigkeit deutscher Gerichte ergibt sich ferner aus Art. 79 Abs. 2 DSGVO. Danach können Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat, es sei denn, es handelt

sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist. Gemäß Art. 4 Nr. 7, 8 DSGVO sind Verantwortliche natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Auftragverarbeitende sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Die Beklagte ist Verantwortliche im Sinne dieser Normen.

Die örtliche Zuständigkeit folgt aus Art. 18 Abs. 1 2. Alt. EuGVVO und Art. 79 Abs. 2 S. 2 DSGVO, § 44 Abs. 1 S. 2 BDSG, die sachliche aus § 23 GVG.

Der Zulässigkeit der Klage hinsichtlich der Feststellungsanträge steht nicht ein mangelndes Feststellungsinteresse des Klägers entgegen.
Der Kläger hat sein Feststellungsinteresse gemäß § 256 Abs. 2 ZPO hinreichend dargelegt. Ein Feststellungsantrag ist schon zulässig, wenn die Schadensentwicklung noch nicht abgeschlossen ist und der Kläger seinen Anspruch deshalb ganz oder teilweise nicht beziffern kann (vgl. OLG Hamm, Urteil vom 21. Mai 2019 - 9 U 56/18 -, Rn. 22, juris). 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 (vgl. BGH, Beschluss vom 09. Januar 2007 - VI ZR 133/06 -, juris; BGH, Urteil vom 16. Januar 2001 - VI ZR 381/99 -, juris; Saarländisches Oberlandesgericht Saarbrücken, Urteil vom 20. Februar 2014 - 4 U 411/12, Rn. 46, juris, m.w.N.).
Bei den behaupteten Verstößen gegen die DSGVO mit der behauptet dargelegten unkontrollierten Nutzung gescrapter Daten ist bei verständiger Würdigung zumindest nicht ausgeschlossen, dass irgendein materieller oder immaterieller Schaden entstehen könnte. Es ist insbesondere nicht völlig ausgeschlossen, dass der Kläger infolge der Veröffentlichung seiner Telefonnummer in Verbindung mit seinem Namen sowie weiteren persönlichen Daten einen irgendwie gearteten Schaden erleidet.

Soweit die Beklagte fehlende hinreichende Bestimmtheit einwendet, greift dies nicht. Der Klageantrag Ziffer 1. ist hinreichend bestimmt.
Da die Bemessung der Höhe des Schmerzensgeldes in das Ermessen des Gerichts gestellt ist, ist die Stellung eines unbezifferten Zahlungsantrags ausnahmsweise zulässig. Ein Verstoß gegen den in § 253 Abs. 2 Nr. 2 ZPO normierten Bestimmtheitsgrundsatz liegt dann nicht vor, wenn die Bestimmung des Betrages von einer gerichtlichen Schätzung nach § 287 ZPO oder vom billigen Ermessen des

Gerichts abhängig ist (BGH, Urteil vom 1. Februar 11966 – VI ZR 196/64, juris Rn. 12). Die nötige Bestimmtheit soll hier dadurch erreicht werden, dass der Kläger in der Klagebegründung die Berechnungs- bzw. Schätzgrundlagen umfassend darzulegen und die Größenordnung seiner Vorstellungen anzugeben hat (Zöller/Greger, ZPO, 34. Aufl. 2022, § 253 ZPO Rn. 14). Diese Voraussetzungen liegen hier vor. Der Kläger hat sowohl in der Klagebegründung als auch im Klageantrag Ziffer 1.) einen Mindestbetrag von 1.000,00 € angegeben.
Soweit die Beklagte meint, der Antrag zu Ziffer 1. sei deshalb unbestimmt sei, weil er auf zwei Lebenssachverhalten beruhe und damit zwei Streitgegenstände betreffe, deren Verhältnis zueinander nicht hinreichend bestimmt sei, ist dies unzutreffend. Es ist nur ein Lebenssachverhalt zu beurteilen, nämlich derjenige, ob die Beklagte vor dem Scraping durch Dritte im April 2021 hinreichende Datenschutzvorkehrungen getroffen hatte und danach etwaige Lücken geschlossen hat bzw. ihre Nutzer unzureichend bzw. intransparent informiert hat.

Der Klageantrag zu Ziffer 2. ist ebenfalls hinreichend bestimmt. Aus dem Inhalt des Klageantrags wird hinreichend ersichtlich, dass es dem Kläger um den Ersatz „künftiger“ Schäden geht, die aus dem streitgegenständlichen „Scraping- Vorfall“ resultieren. Die Verwendung der Vergangenheitsform „entstanden sind“ mag missverständlich sein und einer Auslegung offenstehen, führt aber nicht zur Unbestimmtheit des Klageantrags. Der Kläger hat ebenfalls die Zukunftsform „noch entstehen werden“ verwendet, die offensichtlich mit dem Ersatz „künftiger“ Schäden vereinbar ist.

Der Klageantrag zu Ziffer 3. ist ebenso hinreichend bestimmt. Auch wenn die Formulierung „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ auslegungsbedürftig ist und nicht auszuschließen ist, dass sich insofern Vollstreckungsprobleme ergeben, ist nach höchstrichterlicher Rechtsprechung eine gewisse Auslegungsbedürftigkeit zur Gewährleistung effektiven Rechtsschutzes hinzunehmen (vgl. hierzu BGH, Urteil vom 21. Mai 2015 – I ZR 183/13, juris Rn. 13). Je nach dem Stand der Technik sind dabei verschiedene, aufeinander aufbauende Sicherheitsmaßnahmen möglich, die nicht näher konkretisiert werden können. Der Kläger kann nämlich nicht einschätzen, was die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen beinhalten. Dies führt dann dazu, dass das Vollstreckungsorgan gegebenenfalls Wertungen vornehmen muss. Vom Kläger kann nach Auffassung des Gerichts nicht verlangt werden, für eine hinreichend konkrete Antragstellung den aktuellen Stand der Technik selbst zu ermitteln.

Die Verbindung mehrerer Klageanträge ist zulässig gemäß § 260 ZPO.

B) Begründetheit

Die Klage ist in dem aus dem Urteilstenor ersichtlichen Umfang begründet, im Übrigen unbegründet.

I. Antrag zu Ziffer 1.): Zahlung

Der Kläger hat einen Anspruch auf Zahlung eines immateriellen Schadensersatzes aus Art. 82 Abs. 1 DSGVO in Höhe eines Betrages von 500,00€.

Nach Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Die Auftragsverarbeiter hingegen haften nicht schlechthin für sämtliche Schäden, die aufgrund einer Verarbeitung entstanden sind, an der sie beteiligt waren. Erforderlich ist vielmehr, dass der Auftragsverarbeiter entweder seinen Pflichten nicht nachgekommen ist, die die DSGVO speziell den Auftragsverarbeitern auferlegt, oder er die rechtmäßig erteilten Anweisungen des Verantwortlichen nicht beachtet bzw. gegen diese gehandelt hat. Der Auftragsverarbeiter haftet somit nicht für bloße Rechtsverletzungen des Verantwortlichen, solange er nicht eigene Pflichten verletzt hat. Erforderlich für eine Haftung nach Abs. 2 ist, dass der Auftragsverarbeiter in der Vorschrift, deren Verletzung in Rede steht, explizit bezeichnet wird.

Anknüpfungspunkt für eine Haftung ist also eine der Verordnung nicht entsprechende Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO. Der Vorwurf liegt darin, die Datenverarbeitung durchgeführt zu haben, ohne dass sämtliche in der DSGVO statuierten Pflichten eingehalten wurden und deshalb ein Schaden entstanden ist. Das vorwerfbare Verhalten muss damit nicht zwangsläufig die Datenverarbeitung an sich sein. So wird häufig die Verarbeitung erst dadurch rechtswidrig, dass im Vorfeld Maßnahmen nicht ergriffen wurden, sodass die eigentlich verletzende Handlung bereits vor der Datenverarbeitung lag. Konsequenterweise kann daher bereits der Verstoß gegen solche Pflichten einen Anspruch auf Schadensersatz begründen. Verletzungshandlungen liegen damit vor, wenn die Rechte der betroffenen Personen oder Grundsätze der Datenverarbeitung nur unzureichend beachtet werden. Dies steht im Einklang mit Erwägungsgrund 146, wonach der Verantwortliche oder der

Auftragsverarbeiter Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit der DSGVO nicht im Einklang stehen, ersetzen sollte.

Gemäß Art. 4 Nr. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Hier in Rede stehen Name, Nutzer-ID sowie das Geschlecht des Klägers, ohne die die Nutzung der Plattform facebook nicht möglich ist, worauf direkt bei der Anmeldung hingewiesen wird. Damit ist es möglich, den Kläger zu identifizieren. Es handelt sich mithin um personenbezogene Daten. Die übrigen Daten wie Telefonnummer und E-Mail-Adresse sind ebenfalls personenbezogen, aber nicht in jedem Fall öffentlich.

Ein relevanter Verstoß der Beklagten ist vorliegend darin zu sehen, dass diese gegen die sich aus Art 25 Abs. 2 DSGVO ergebende Verpflichtung verstoßen hat.

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

Das ist aber 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 DSGVO. 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 Voreinstellung, die die Beklagten hinsichtlich einzelner Aspekte mit „öffentlich“ einräumt, läuft den Erfordernissen des Art. 25 Abs. 2 DSGVO 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).

Im Übrigen ist nicht anzunehmen, dass ein Verstoß gegen Art. 25 Abs. 2 DSGVO einen Ersatzanspruch nicht auszulösen vermag (so im Ergebnis z.B.: Nolte/Werkmeister in Gola/Heckmann, DS-GVO – BDSG, 3. Aufl. DS-GVO Art. 25 Rn. 3, 34). Vielmehr kann aus der Verletzung der sich aus Art. 25 DS-GVO ergebenden Pflichten eine Erhöhung der Gefahr eines Schadens resultieren (vgl. Manz in Sydow/Marsch, DS-GVO | BDSG, 3. Aufl. DS-GVO Art. 25 Rn. 77).

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

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

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 DSGVO 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.

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. Derlei vermag die Beklagte insbesondere im Rahmen der Klageerwiderung vom 28.09.2022 (Blatt 188 der Akte) nicht aufzuzeigen. 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, zumal auch in der vorgelegten „Datenrichtlinie“ der Anlage B 9 (Bl. 296 der Akte) in der Rubrik „Wie werden diese Informationen geteilt?“ noch nicht einmal im Ansatz hierauf hingewiesen wird.

Angesichts des Vorstehenden kann hier auch nicht von einer wirksamen Einwilligung des Klägers i.S. von Art. 6 Abs. 1 lit. a DSGVO 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).

Auch wenn dem Nutzer eine eigene Verantwortung zukommt, selbst zu entscheiden, ob und welche Daten er im Internet veröffentlicht, obliegt es doch facebook als dem verantwortlichen Plattformbetreiber, dem Nutzer durch datenschutzfreundliche Voreinstellungen die Entscheidung über die Veröffentlichung seiner Daten nicht zu erschweren und durch technische Maßname Scraping zu verhindern.

Ein Verstoß gegen Art. 13 DSGVO kann – entgegen der Annahme der Beklagten – ohne weiteres einen Schadensersatzanspruch nach Art. 82 DS-GVO nach sich ziehen (vgl. Franck in Gola/Heckmann, DS-GVO – BDSG, 3. Aufl. DS-GVO Art. 13 Rn. 64).

Ob die Beklagte im Vorfeld des Daten-Scraping-Vorfalls weitere Pflichtverletzungen in Ansehung der DSGVO begangenen hat, 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 DSGVO und aus Art. 13 DSGVO folgt.

Die Beklagte ist nicht nach Art 82 Abs. 3 DSGVO von ihrer Haftung befreit.
Eine Entlastung nach Art 82 Abs. 3 DSGVO findet nur statt bei einem Nachweis höherer Gewalt. Im Übrigen kann der Verantwortliche oder Auftragsverarbeiter nur vollständig von seiner Haftung befreit werden, wenn er „in keiner Weise“ für den schadensverursachenden Umstand verantwortlich ist (Sydow/ Marsch, DSGVO/ BDSG, 3. Auflage 2022, Rn. 18). Die kann indes nur angenommen werden, wenn ein Fehlverhalten der betroffenen Person vorliegt, die das Maß eines 100%igen Mitverschuldensanteils erreichen würde. Ein solches behauptet die Beklagte selbst schon nicht.

Eine Exkulpation des Verantwortlichen oder Auftragsverarbeiters durch Nachweis der ordnungsgemäßen Auswahl und Überwachung seiner Angestellten – zB nach § 831 BGB – kommt darüber hinaus nicht in Betracht. Damit besteht die Haftung insbesondere auch bei einem Verschulden des Datenschutzbeauftragten des Verantwortlichen oder Auftragsverarbeiters. Denn einen solchen Entlastungsbeweis sieht die DSGVO zum einen nicht vor, zum anderen stünde dies dem Gebot des möglichst „wirksamen“ Schadensersatzanspruchs entgegen (Erwägungsgrund 146 S.6).

Der Kläger hat überdies einen Schaden erlitten. Dahinstehen kann dabei, ob ein Datenschutzverstoß als solcher für das Entstehen eines Schadensersatzanspruchs ausreicht oder es darüber hinaus der Darlegung und des Nachweises eines konkreten – auch immateriellen – Schadens bedarf (vgl. dazu OLG Frankfurt a.M., Urteil vom 02.03.2022 – 13 U 206/20, GRUR 2022, 1252 Rn. 59). Denn der Kläger hat einen darüber hinausgehenden Schaden behauptet und zur Überzeugung des Gerichts im Rahmen seiner persönlichen Anhörung nachvollziehbar erläutert.
Als immaterieller Schaden des Klägers stellt sich die mit dem Verlust der Datenkontrolle verbundene belastende Ungewissheit über das Schicksal seiner Daten dar. Es genügt, anders als die Beklagte meint, dass der Kläger ein ungutes Gefühl hat und Sorge vor weiteren Anrufen und „falschen“ Paketankündigungen etc.. Letzteres hat er glaubhaft im Rahmen seiner informatorischen Anhörung dargetan. Er hat auch glaubhaft und nachvollziehbar erklärt, dass er seine – auch hier in Rede stehende Telefonnummer- bereits seit seiner Jugendzeit habe, hiermit aber restriktiv umgegangen sei und dass er erst seit Mitte 21 Spamanrufe in vermehrtem Umfang, nämlich 3-5 Anrufen/ Monat und zusätzlich noch SMS mit z.B. falschen

Paketankündigungen. Der Kläger hat dies ohne besondere Belastungstendenz, unaufgeregt und ohne Übertreibung geschildert. Er war vielmehr bemüht, die Anzahl der Anrufe ganz korrekt wiederzugeben und hat auch mitgeteilt, dass es auch Mitte 2021 bereits Spamanrufe gab, eben in deutlich geringerem Umfang.

Der Schaden kann durchaus bereits in dem unguten Gefühl liegen, dass personenbezogene Daten Unbefugten bekannt geworden sind, insbesondere wenn nicht ausgeschlossen ist, dass die Daten unbefugt weiterverwendet werden, auch bereits in der Ungewissheit, ob personenbezogene Daten an Unbefugte gelangt sind. Dies gilt umso mehr, wenn wie hier, eine zunehmende Anzahl von „Spam"- Anrufen hiermit in Verbindung gebracht wird und es als „heikel" empfunden wird, wenn man falsche Paketankündigungen nicht von echten unterscheiden kann und dementsprechend nicht weiß, ob man diese gefahrlos öffnen und hierin enthaltene Links anklicken kann.

Dafür, dass darin ein immaterieller Schaden im Sinne von Art. 82 Abs. 1 DSGVO liegen kann, spricht der Erwägungsgrund 75 der DSGVO, wo dem Schadensbegriff auch der Verlust der Kontrolle über personenbezogene Daten zugeordnet wird.
Der Begriff des Schadens ist auf eine Art und Weise auszulegen, die den Zielen der Datenschutzgrundverordnung in vollem Umfange entspricht. Insoweit ist durch das Inkrafttreten der Datenschutzgrundverordnung eine Verschärfung im Vergleich zur bisherigen Rechtslage eingetreten. (…) Nach den Erwägungsgründen 146 der DSGVO, die zur Auslegung der Vorschrift mit heranzuziehen sind, soll die betroffene Person einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten. Verstöße müssen effektiv sanktioniert werden. Schadenersatz bei Datenschutzverstößen sollen eine abschreckende Wirkung haben, um der Datenschutzgrundverordnung zum Durchbruch zu verhelfen (effet utile)" (ArbG Dresden Urt. v. 26.8.2020 – 13 Ca 1046/20, BeckRS 2020, 26940 Rz. 14

Gegen die Annahme eines Kontrollverlustes kann auch nicht mit Erfolg eingewandt werden, der Kläger habe die Kontrolle besessen und dem Datenabgleich zugestimmt. Es muss hier nach Ansicht des Gerichts differenziert werden zwischen dem rechtmäßigen Datenabgleich durch Nutzer und dem Scraping durch Dritte zu rechtswidrigen Zwecken. Auch wenn der Nutzer durch seine Einstellungen die Möglichkeit des Datenabgleichs eröffnet, heißt das noch nicht, dass er damit auch sein Einverständnis erklärt, dass Dritte Daten „abgreifen" dürfen. Das geht über das akzeptable Maß an Eigenverantwortung des Nutzers deutlich hinaus.

Eine Bagatellgrenze/ Erheblichkeitsgrenze ist dem Wortlaut des Art 82 Abs. 1 DSGVO nicht zu entnehmen. Eine derartige Beschränkung ist auch nicht angezeigt (OLG Hamm (Urteil vom 20.01.2023 – I- 11 U 88/ 22 -, juris). Der immaterielle

Schaden ist daher grundsätzlich auszugleichen, mag er auch im Einzelfall nur zu einer geringfügigen Beeinträchtigung geführt haben. Letzteres ist dann im Rahmen derer Bemessung der Höhe des Schadensersatzes zu berücksichtigen.

Der Eintritt eines Schadens setzt auch nicht voraus, dass dem Betroffenen durch den Verstoß gegen die DSGVO ein spürbarer Nachteil entstanden ist oder es zu einer objektiv nachvollziehbaren Beeinträchtigung von persönlichkeitsbezogenen Belangen mit gewissem Gewicht gekommen ist.
Eine Einschränkung des Anspruchs in der DSGVO dahingehend, dass eine „Spürbarkeit“ eines Nachteils gegeben sein muss, findet in den hier anzuwendenden Vorschriften keine Grundlage und ist auch aus sonstigen Gründen nicht geboten (Gola/ Heckmann, DS-GVO, 3. Auflage 2022, Rn. 15). Es handelt sich auch hierbei letztlich ebenfalls um eine Erheblichkeitsschwelle, die weder in der DSGVO noch in der Rechtsprechung des EuGH eine Stütze findet (vgl. hierzu OLG Hamm, Urteil vom 20.01.2023 aaO, unter Verweis auf Buchner/Wessels, in ZD 2022, 251 (254)).

Der Verordnungsverstoß im Sinne der verordnungswidrigen Verarbeitung ist für das Scraping und den hieraus resultierenden Schaden ursächlich geworden. Was unter Ursächlichkeit zu verstehen ist, richtet sich im Ansatz nach nationalem Recht, wobei die Anforderungen an die Kausalität wegen des Effektivitätsgrundsatzes nicht überspannt werden dürfen und außerdem die in Abs. 3 enthaltenen Kausalitätsaspekte zu beachten (Sydow/Marsch, DSGVO/BDSG 3. Auflage 2022, Rn. 4, 7-8). Das Scraping der Daten des Klägers ist ohne die Verletzung der Pflichten der Beklagten nach Art. 25 Abs. 2 DSGVO und nach Art. 13 DSGVO 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. Hierauf beruhte der oben beschriebene klägerische Schaden.

Um dem Kläger den erlittenen immateriellen Schaden auszugleichen, ist von der Beklagten ein Betrag in Höhe von 500,00€ zu zahlen.
Für die Bemessung von Schadensersatzansprüchen nach Art. 82 Abs. 1 DSGVO enthält die DSGVO nur wenige Vorgaben. Aus dem Nebeneinander von materiellem und immateriellem Schaden folgt, dass auch solche Schäden auszugleichen sind, die sich nicht unmittelbar in Geld bemessen lassen. Nach Erwägungsgrund 146 Satz 3 sollte der Begriff des Schadens im Lichte der Rechtsprechung des Gerichtshofs zudem weit auf eine Art und Weise ausgelegt werden, die den Zielen der Verordnung in vollem Umfang entspricht. Nach Erwägungsgrund 146 Satz 6 sollten die

betroffenen Personen einen vollständigen und wirksamen Schadensersatz für erlittene Schäden erhalten.
Hiernach hat sich der Schadensersatz zuerst an dem Ziel des Schadensausgleichs zu orientieren. Das gilt, weil die Vorschrift nicht zwischen den Schadensarten differenziert, auch im Falle immaterieller Schäden (siehe Eichelberger, WRP 2021, 159, 162 ff.). Darüber hinaus wird bei immateriellen Einbußen auch die Genugtuungsfunktion Bedeutung erlangen und als ein Umstand bei der Schadensbemessung berücksichtigt werden können, wenn die Umstände des konkreten Falles hierfür Anlass geben (vgl. auch Eichelberger, WRP 2021, 159, 165). Letztlich können – wie dies auch bei Art. 340 Abs. 2 AEUV der Fall ist (vgl. EuGH, Urteil vom 30. Mai 2017 – C-45/15 P, juris, Rn. 48) – für die Bemessung des Ersatzanspruchs für immaterielle Schäden nur die Umstände des konkreten Einzelfalls entscheidend sein. Zu berücksichtigen sein können etwa Art, Schwere und Dauer des Datenschutzverstoßes, das Verhalten des Verantwortlichen sowie die Auswirkungen des Verstoßes für den Betroffenen (siehe EuGH, Urteil vom 30. Mai 2017 – C-45/15 P, juris, Rn. 52, zu Art. 340 Abs. 2 AEUV). Solche Kriterien sind nach Art. 83 Abs. 2 Satz 2 DSGVO auch bei der Verhängung von Geldbußen für Datenschutzverstöße zu berücksichtigen. Bei der Ermittlung der danach angemessenen Art der Entschädigung und der Bestimmung des gegebenenfalls zuzuerkennenden Schadensersatzbetrags haben die Gerichte einen erheblichen Spielraum (vgl. für Art. 340 Abs. 2 AEUV Schlussanträge des Generalanwalts N. Wahl vom 25. Juli 2018 in den verbundenen Rechtssachen C-138/17 P und C-146/17 P, juris, Rn. 86), den sie nach billigem Ermessen füllen müssen (siehe für Art. 340 Abs. 2 AEUV EuGH, Urteil vom 1. Februar 2017 – T-479/14, juris, Rn. 135, sowie Schlussanträge des Generalanwalts N. Wahl vom 25. Juli 2018 in den verbundenen Rechtssachen C-138/17 P und C-146/17 P, juris, Rn. 85 u. 101).
Das Gericht hält unter Berücksichtigung des Vorstehenden hier ein Schmerzensgeld von 500,00 EUR für angemessen, aber auch ausreichend, um einerseits der Ausgleichs- und Genugtuungsfunktion zu genügen, und andererseits der generalpräventiven Funktion des immateriellen Schadensersatzes hinreichend Rechnung zu tragen. Vorliegend hat das Gericht seiner Entscheidung zugrunde gelegt, dass sich die Beklagte nach den obigen Darlegungen einen Verstoßes gegen DSGVO vorwerfen lassen muss, der einen weitgehenden Kontrollverlust der personenbezogenen Daten des Klägers ermöglicht und begünstigt hat. Da jedoch-auch im Rahmen der informatorischen Anhörung des Klägers-keine besondere persönliche Betroffenheit von ihm festgestellt werden konnte, sind 500 € als ausreichend zu erachten.

II. Antrag zu Ziffer 2.): Feststellungsantrag

Auch der mit dem Klageantrag zu 2 geltend gemachte Feststellungsantrag ist begründet. Der Kläger hat gegenüber der Beklagten wegen Verletzung der DSGVO einen Anspruch auf Schadensersatz nach Art. 82 DS GVO. Die jeweiligen Gesetzesverletzung sind- wie oben bereits dargelegt- kausal für den unkontrollierten Datenverlust des Klägers.

III. Anträge zu Ziffer 3): Unterlassung
Der Kläger kann von der Beklagten Unterlassung verlangen.

Soweit es für den vorbeugenden Unterlassungsschutz eine gesonderte Anspruchsgrundlage in der DSGVO 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).

Die Beklagte hat – wie oben festgestellt – jedenfalls gegen Art. 13 und Art. 25 Abs. 2 DS-GVO verstoßen. Diese Rechtsverstöße geben dem Kläger einen darauf bezogenen Anspruch auf Beseitigung und künftige Unterlassung.
Daher kann der Kläger verlangen, dass die Beklagte es unterlässt, personenbezogenen Daten (Telefonnummer, Facebook-ID, Familienname, Vorname, Geschlecht, Stadt, Land Beziehungsstatus) unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen. Ausgenommen davon sind indes die Daten „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. 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.

Es besteht auch ein Unterlassungsanspruch hinsichtlich der Verarbeitung ohne Erfüllung der Informationspflicht hinsichtlich der Funktionsweise und der Verwendung

von Telefonnummern. Die Vermutung der Wiederholungsgefahr - die sich in der Regel aus der Rechtsverletzung ergibt – ist auch insofern nicht widerlegt. Eine Unterlassungserklärung liegt nicht vor. Es ergibt sich auch aufgrund der Umstände kein Entfallen der Wiederholungsgefahr. Insbesondere kann diese nicht mit dem Argument verneint werden, der Kläger habe sämtliche Informationen erhalten, die die in Rede stehende Art der Datenverarbeitung betreffen würden. Denn eine Verletzungshandlung begründet die Vermutung der Wiederholungsgefahr nicht nur für die identische Verletzungsform, sondern für alle im Kern gleichartigen Verletzungshandlungen, in denen das Charakteristische der konkreten Verletzungsform zum Ausdruck kommt (BGH, Urteil vom 22.09.2021- I ZR83/20-, Rn. 33 juris).

IV. Antrag zu Ziffer 4): Auskunft

Der geltend gemacht Anspruch auf Auskunft besteht nicht (mehr). Ein Anspruch auf Auskunftserteilung ergibt sich aus Art. 15 Abs. 1 a), c) DSGVO. Dem Kläger steht hiernach das Recht zu, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob betreffende personenbezogene Daten verarbeitet werden und – bejahendenfalls- ein weitergehendes Recht auf Auskunft über diese personenbezogenen Daten und über die a.) Verarbeitungszwecke und über c.) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen. Die Beklagte hat den Kläger aber informiert. Damit ist der Anspruch insoweit erfüllt und erloschen (§ 362 Abs. 1 BGB). Erfüllt im Sinne des § 362 Abs.1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die - gegebenenfalls konkludente - Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (vgl. BGH, Urteil vom 03.09.2020 - III ZR 136/18 = GRUR 2021,110). Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll.

Das ist hier der Fall.

Es ist zwar zutreffend, dass durch die Beklagte in dem außergerichtlichen Schreiben nicht die Frage beantwortet worden ist, welchen Empfängern die Daten des Klägers durch Ausnutzung des Kontakt-Import Tools im Sinne des Art. 15 Abs. 1 c) DSGVO zugänglich gemacht wurden. Das Scraping ist allerdings - wie vorstehend ausgeführt - von außen erfolgt und es ist weder konkret vorgetragen, noch erkennbar, dass für die Beklagte zu ersehen ist, wer diese Daten gescrapt hat. Die begehrte Auskunftserteilung ist daher unmöglich. Die Beklagte hat dem Kläger im Ergebnis also alle Informationen mitgeteilt, die ihr im Zuge des Scraping-Vorfalls zur Verfügung standen. Weitere Angaben kann, hiervon muss nach Vorstehendem ausgegangen werden- sie nicht machen. Sie ist folglich hierzu auch nicht verpflichtet.

Etwas anderes ergibt sich auch nicht aufgrund der vom Kläger in Bezug genommenen und übrigens lediglich in französischer Sprache (nicht umstellbar) verlinkten Entscheidung des EuGH vom 12.01.2023, RS. C-154/21. Der EUGH schreibt hierin ausdrücklich, dass es denkbar ist, dass es unter bestimmten Umständen nicht möglich ist, Informationen über konkrete Empfänger zu erteilen. Daher kann, so der EUGH, das Auskunftsrecht auf Informationen über die Kategorien von Empfängern beschränkt werden, wenn es nicht möglich ist, die Identität der konkreten Empfänger mitzuteilen, insbesondere wenn diese noch nicht bekannt sind. So liegt der Fall hier.

Dem Antrag der Beklagten auf Einräumung eines weiteren Schriftsatznachlasses war nicht zu entsprechen.
Die Beklagte ist nicht in Erklärungsnot geraten im Sinne des § 283 ZPO. Der bezeichnete Schriftsatz der Klägerseite vom 01.03.023 beinhaltet ganz überwiegend Rechtsausführungen und Verweise auf in anderen Verfahren ergangene Urteile, bei welchen sämtlich die hiesige Beklagte auch dort als Partei beteiligt war. Soweit überhaupt Tatsachenvortrag enthalten ist, bezieht sich dieser auf Streitpunkte, zu denen bereits in vorangegangenen Schriftsätzen des Klägers und der Beklagten Stellung genommen worden ist. Diese Streitpunkt entsprechen denen in einer Vielzahl von Parallelverfahren. Der Tatsachenvortrag ist überdies von geringem Umfang, übersichtlich und inhaltlich nicht schwierig. Die Beklagte war auch nicht außer Stande, sich hierzu zu erklären. Im Termin zur mündlichen Verhandlung vom 09.03.2023 ist die Sach- und Rechtslage erörtert worden und die Parteien hatten Gelegenheit zur Stellungnahme. Die Prozessbevollmächtigte der Beklagten hat hier auch Stellung genommen, insbesondere eben auch zum Inhalt des Schriftsatzes der Gegenseite vom 01.03.2023. Im Schriftsatz vom 20.03.2023 hat die Beklagte überdies Stellung genommen.

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

Die vorgerichtlichen Rechtsanwaltskosten sind in Höhe von 280,60€ als Teil des zu ersetzenden Schadens gemäß Art. 82 Abs. 1 DSGVO zu ersetzen. Im Umfang seines berechtigten Verlangens kann der Kläger gemäß §§ 280 Abs. 1, 2, 286 Abs. 2 BGB die vorgerichtlichen Rechtsanwaltskosten nach einem Gegenstandswert von 2000€ in Höhe von 280,60€ erstattet verlangen (1,3 Geschäftsgebühr Nr. 2300, 1008 VV RVG 215,86€ Auslagenpauschale 20,00€, Mehrwertsteuer 19%: 44,80€). Im Übrigen besteht kein Anspruch.

Die Kostenentscheidung beruht auf § 92 ZPO.

Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt den §§ 708 Nr. 11, 711 ZPO.

Die Wertfesetzung beruht auf § 3 ZPO i.V.m. § 64 GKG. Es wird insoweit auf die Gründe des Beschlusses des LG Siegen vom 09.05.2022 (Bl. 108 der Akte) Bezug genommen.

Rechtsbehelfsbelehrung:

Gegen dieses Urteil ist das Rechtsmittel der Berufung für jeden zulässig, der durch dieses Urteil in seinen Rechten benachteiligt ist,

1. wenn der Wert des Beschwerdegegenstandes 600,00 EUR übersteigt oder

2. wenn die Berufung in dem Urteil durch das Amtsgericht zugelassen worden ist.

Die Berufung muss **innerhalb einer Notfrist von einem Monat nach Zustellung** dieses Urteils bei dem Landgericht Siegen, Berliner Str. 22, 57072 Siegen, eingegangen sein. Die Berufungsschrift muss die Bezeichnung des Urteils, gegen das die Berufung gerichtet wird, sowie die Erklärung, dass gegen dieses Urteil Berufung eingelegt werde, enthalten.

Die Berufung ist, sofern nicht bereits in der Berufungsschrift erfolgt, binnen zwei Monaten nach Zustellung dieses Urteils gegenüber dem Landgericht Siegen zu begründen.

Die Parteien müssen sich vor dem Landgericht Siegen durch einen Rechtsanwalt vertreten lassen, insbesondere müssen die Berufungs- und die Berufungsbegründungsschrift von einem solchen unterzeichnet sein.

Mit der Berufungsschrift soll eine Ausfertigung oder beglaubigte Abschrift des angefochtenen Urteils vorgelegt werden.

Hinweis zum elektronischen Rechtsverkehr:
Die Einlegung ist auch durch Übertragung eines elektronischen Dokuments an die elektronische Poststelle des Gerichts möglich. Das elektronische Dokument muss für die Bearbeitung durch das Gericht geeignet und mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg gemäß § 130a ZPO nach näherer Maßgabe der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (BGBl. 2017 I, S. 3803) eingereicht werden. Auf die Pflicht zur elektronischen Einreichung durch professionelle Einreicher/innen ab dem 01.01.2022 durch das Gesetz zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013, das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017 und das Gesetz zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten und zur Änderung weiterer Vorschriften vom 05.10.2021 wird hingewiesen.
Weitere Informationen erhalten Sie auf der Internetseite www.justiz.de.

Beglaubigt
Urkundsbeamter/in der Geschäftsstelle
Amtsgericht Siegen

Verkündet am 30.03.2023

Hasenkamp, Justizbeschäftigte
als Urkundsbeamtin der Geschäftsstelle