– Beglaubigte Abschrift –

Landgericht Hannover

Im Namen des Volkes

Urteil

18 O 157/22

Verkündet am 14.08.2023

_____
[redacted], Justizangestellte
als Urkundsbeamtin der Geschäftsstelle

In dem Rechtsstreit

[redacted]

- Kläger -

Prozessbevollmächtigte:
Wilde Beuger Solmecke Rechtsanwälte Partnerschaft mbB, Kaiser-Wilhelm-Ring 27 - 29, 50672 Köln
Geschäftszeichen: [redacted]

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:
Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB, Bockenheimer Anlage 44, 60322 Frankfurt am Main
Geschäftszeichen: [redacted]

hat das Landgericht Hannover – 18. Zivilkammer – durch die Vorsitzende Richterin am Landgericht [redacted], den Richter am Landgericht [redacted] und den Richter am Landgericht [redacted] auf die mündliche Verhandlung vom 04.07.2023 für Recht erkannt:

1. **Die Beklagte wird verurteilt, an den Kläger 500,- € nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 12.10.2022 zu zahlen.**

2. **Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen Schäden zu ersetzen, die dem Kläger durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten in dem Zeitraum Januar 2018 bis September 2019 entstanden sind 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,- €, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,**

    a. **personenbezogene Daten des Klägers, namentlich Telefonnummer, FacebookID, Familienname, Vorname, Geschlecht, 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 des Klägers auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontakt-Import-Tools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und im Fall der Nutzung der Facebook-Messenger-App hier ebenfalls explizit die Berechtigung verweigert wird.**

4. **Die Beklagte wird verurteilt, an den Kläger weitere 713,76 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 12.10.2022 zu zahlen.**

5. **Im Übrigen wird die Klage abgewiesen.**

6. **Von den Kosten des Rechtsstreits tragen der Kläger 14% und die Beklagte 86%.**

7. **Das Urteil ist für den Kläger hinsichtlich des Tenors zu Ziffer 3 gegen Sicherheitsleistung in Höhe 5.500,- €, im Übrigen gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar. Der Kläger kann die Vollstreckung der Beklagten abwenden durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrages, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet.**

8. **Der Streitwert wird auf 7.000,- € festgesetzt.**

Tatbestand

Der Kläger nimmt die Beklagte wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung im Zusammenhang mit einem sogenannten „Scraping-Vorfall“ (oder „Datenleck“) bei der Beklagten in Anspruch.

Der Kläger nutzt das von der Beklagten betriebene soziale Netzwerk Facebook. Diese Plattform ermöglicht nach einer Anmeldung die Kommunikation mit anderen Nutzern, insbesondere können private Fotos und Informationen geteilt werden. Auf ihren persönlichen Profilen können die Nutzer Angaben zu ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können. Die Beklagte stellt dabei Tools und Informationen zur Verfügung, damit Nutzer ihre Privatsphäre auf der Facebook-Plattform verwalten können. Damit Nutzer leichter mit anderen Nutzern in Kontakt treten können, müssen sie bestimmte Informationen bei der Registrierung angeben, die als Teil des Nutzerprofils immer öffentlich einsehbar sind. Dazu gehören Name, Geschlecht und Nutzer-ID. Eine Eingabe einer Telefon- bzw. Mobilfunknummer ist nicht zwingend erforderlich. Die Angaben „Land“, „Bundesland“, „Geburtsort“ und „weitere korrelierende Daten“ sind bei der Facebook-Plattform nicht als Eingabefelder vorgesehen. Hinsichtlich der weiteren Daten gibt es im Rahmen der Privatsphäre-Einstellungen Wahlmöglichkeiten für jeden Nutzer. Bei der sogenannten „Zielgruppenauswahl“ legt der Nutzer fest, wer einzelne Informationen auf seinem Facebook-Profil, wie etwa Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse, einsehen kann. So kann der Nutzer anstelle der standardmäßigen Voreinstellung „öffentlich“ auswählen, dass nur „Freunde“ auf der Facebook-Plattform, oder „Freunde von Freunden“ die jeweiligen Informationen einsehen können. Lediglich die Telefonnummer des Nutzers wird insoweit gesondert behandelt, als dass diese standardmäßig nicht für jedermann einsehbar ist. Die „Suchbarkeits-Einstellungen“ legen fest, wer das Profil eines Nutzers anhand u.a. einer Telefonnummer finden kann. Passt der Nutzer die Suchbarkeits-Einstellungen nicht an, sieht die Standardeinstellung vor, dass alle Personen, die über die Telefonnummer des Nutzers verfügen, das Profil des Nutzers, falls dieser seine Telefonnummer bereitgestellt hat, finden. Demnach war es möglich, Nutzer anhand einer Telefonnummer zu finden, solange ihre „Suchbarkeits-Einstellung“ für Telefonnummern auf der Standard-Voreinstellung „Alle“ eingestellt war. Daneben waren als Einstellungen nur „Freunde von Freunden“ oder „Freunde“ auswählbar. Ab Mai 2019 stand Nutzern auch die Option „Nur ich“ zur Verfügung.

Der Kläger hatte bei den Suchbarkeits-Einstellungen eine Änderung nicht vorgenommen, sodass die Standardeinstellung aktiv gewesen ist; für die Suchbarkeit

anhand der Telefonnummer waren die Einstellungen mithin auf „Alle“ gestellt (s. Anlage B 17).

Bei der für den Zugang zu der Plattform erforderlichen Registrierung wird der Nutzer aufgefordert, seinen Vor- und Nachnamen, sein Geburtsdatum, sein Geschlecht und ein entsprechendes Passwort anzugeben. In dem sich unter den genannten Angaben befindlichen Informationssegment heißt es sodann:

„Indem du auf „Registrieren“ klickst, stimmst du unseren Nutzungsbedingungen zu. In unserer Datenrichtlinie erfährst du, wie wir deine Daten erfassen, verwenden und teilen (…).“

Die Datenrichtlinie beinhaltet Informationen dazu, welche der vom Nutzer gemachten Angaben immer öffentlich sichtbar sind und so von jedermann - also auch von Personen außerhalb der Plattform - eingesehen werden können. Hierzu gehören der Name, das Profil- sowie Titelbild, das Geschlecht, der Nutzername und die jeweilige Nutzer-ID. Diese Angaben machte auch der Kläger als Nutzer des sozialen Netzwerks unter Zustimmung zu der vorbezeichneten Datenrichtlinie. Im Zuge der Aktualisierung der Nutzungsbedingungen und der Datenrichtlinie im April 2018 wies die Beklagte alle Nutzer in der EU auf die aktualisierte Datenrichtlinie hin und die Nutzer mussten den aktualisierten Nutzungsbedingungen zustimmen, um die Facebook-Plattform weiter nutzen zu können. Sowohl die Datenrichtlinie als auch die Nutzungsbedingungen vom 19. April 2018 waren in dem Hinweis unmittelbar verlinkt, so dass die Nutzer – inklusive des Klägers – direkten Zugriff auf deren Inhalt hatten.

Darüber hinaus stellte die Beklagte im sogenannten „Hilfebereich“ Erläuterungen zur Öffentlichkeit der jeweiligen Informationen zur Verfügung. Hierbei wurde dem Nutzer erklärt, dass und wie er einstellen kann, wer die über die immer öffentlich einsehbaren Angaben hinaus freiwillig getätigten Informationen einsehen kann (Zielgruppenauswahl). In dem Hilfebereich wurde der Nutzer auch darüber informiert, für welche Personengruppe er anhand seiner E-Mail-Adresse oder seiner Telefonnummer - sofern er hierzu im Bereich der Kontaktinformationen Angaben tätigte - im Netzwerk auffindbar ist (Suchbarkeits-Einstellungen).

Im Einzelnen heißt es im Hilfebereich:

Hilfe zum Thema „*Festlegen, wer sehen kann, was du teilst“*. Hier erfolgt eine Zusammenstellung zahlreicher möglicher Nutzerfragen im Zusammenhang mit den Privatsphäre-Einstellungen. Auf die Anlage B 2 wird Bezug genommen.

Hilfe zum Thema „*Wie bearbeite ich allgemeine Infos in meinem Facebook-Profil und wie lege ich fest, wer sie sehen kann?*“ Hier heißt es: „*Hier findest du eine Übersicht darüber, wer was in deinem Profil sehen kann, sowie über die Funktionen, die du zur Sichtbarkeit der Inhalte in deinem Profil bzw. deiner Chronik verwenden kannst.“*

Es wurde den Nutzern erläutert, wie sie die allgemeinen Informationen in ihrem Facebook-Profil bearbeiten und wie sie durch die Anpassung ihrer Zielgruppenauswahl bestimmen können, wer auf diese Profil-Informationen zugreifen kann. Auf die Anlage B 3 wird Bezug genommen.

Weiter gab es die Rubrik „Hilfe zum Thema *´Wie lege ich fest, wer die Inhalte in meinem Profil auf Facebook sehen darf?*`“. Hier wurde erklärt, wie Nutzer die Zielgruppenauswahl für bestimmte Daten entsprechend ihren Vorstellungen anpassen können. Auf die Anlage B 4 wird Bezug genommen.

Daneben gab es die Rubrik „Hilfe zum Thema `*Wie kann ich festlegen, wer mich über meine E-Mail-Adresse oder Handynummer auf Facebook finden kann?*`“ Es heißt dort namentlich:

„Du kannst für deine E-Mail-Adresse und Telefonnummer jeweils einstellen, wer dich anhand dieser Informationen finden kann. Diese Einstellungen kannst du wie folgt ändern:

1. Klicke oben rechts auf einer Facebook-Seite auf und wähle „Einstellungen“ aus.

2. Wähle auf der linken Seite „Privatsphäre“ aus. Unter dem Abschnitt „Wer kann nach mir suchen?“ findest du eine Einstellung für deine E-Mail-Adresse und eine Einstellung für deine Telefonnummer.

3. Aus dem Menü neben der jeweiligen Einstellung kannst du auswählen, wer dich anhand dieser Informationen finden kann. Beachte bitte, dass du separat festlegen kannst, wer deine Telefonnummer und deine E-Mail-Adresse in deinem Profil sehen kann. Wenn du deine Telefonnummer oder deine E-Mail-Adresse in deinem Profil mit

jemandem teilst, kann diese Person dich anhand dieser Informationen finden. Erfahre, wie du festlegst, mit wem du deine E-Mail-Adresse oder Telefonnummer teilst.“

Auf die Anlage B 5 wird Bezug genommen.

Unter „Hilfe zum Thema *´Wozu verwendet Facebook meine Mobilnummer?`*“ heißt es:

„Möglicherweise verwenden wir deine Mobilnummer für diese Zwecke:

Um dir bei der Anmeldung zu helfen: Wenn du dein Passwort oder deine E-Mail-Adresse vergessen hast, über die du dich bei Facebook anmeldest, kannst [du] diese erfragen, indem du die mit deinem Konto verbundene Mobilnummer eingibst.

Um dein Konto mit Opt-in Funktionen wie die zweistufige Authentifizierung oder SMS-Nachrichten bei Logins über unbekannte Geräte zu schützen.

Um dir Personen, die du kennen könntest, vorzuschlagen, damit du dich mit ihnen auf Facebook verbinden kannst.

Beachte, dass du kontrollieren kannst, wer deine Telefonnummer sehen kann. Mehr dazu erfährst du in unserer Datenrichtline.“

Auf die Anlage B 6 wird Bezug genommen.

Nutzer können grundsätzlich ihre Kontakte von ihren Mobilgeräten mittels der sogenannten „Kontakt-Importer-Funktion“ bzw. dem Contact-Import-Tool“ (im Folgenden „CIT“) auf Facebook hochladen, um diese Kontakte auf der Facebook-Plattform zu finden und mit ihnen in Verbindung zu treten, ohne dass die im Profil hinterlegte Telefonnummer in der „Zielgruppenauswahl“ öffentlich gemacht worden wäre.

Die Beklagte betreibt neben der Facebook-Website eine Messenger-App, die von Facebook-Nutzern verwendet werden kann, um sich gegenseitig Nachrichten zu schicken. Nutzer melden sich dafür mit ihrem Facebook-Profil an. Die App und die gewöhnlichen Funktionen von Facebook sind über denselben Zugang zum Account verknüpft. Während des relevanten Zeitraums entsprachen die Einstellungen des Klägers zur Zielgruppenauswahl und Suchbarkeit im Messenger denen in seinem Facebook-Konto.

Zwischen Januar 2018 und September 2019 extrahierten („scrapten“; dt.: „schaben“, „kratzen“ – gemeint ist der Vorgang des Extrahierens, Kopierens, Speicherns sowie der Wiederverwendung fremder Inhalte im Netz) Dritte (Scraper) bestimmte Daten von Facebook-Profilen, indem sie die Kontakt-Importer-Funktion (CIT) nutzten und Kontakte mit möglichen Telefonnummern hochluden. Wenn Facebook anhand der möglichen Telefonnummer ein vorhandenes Facebook-Profil fand, luden die Scraper die öffentlich zugänglichen Informationen des entsprechenden Profils herunter. Die weiteren Einzelheiten hinsichtlich des Ablaufs des „Scrapings“ im vorliegenden Fall sind zwischen den Parteien streitig. Im Jahr 2019 lasen Dritte jedenfalls auch den Namen, den Vornamen, den Wohnort, das Geschlecht, den Arbeitgeber und den Beziehungsstatus des Klägers über das CIT von Facebook aus (s. Bl. 119 R d.A.). Die Telefonnummer wurde diesem „geleakten“ Datensatz hinzugefügt.

Zu der Vorgehensweise ist näher auszuführen: Der Abruf der Telefonnummern erfolgte hier nicht über das Facebook-Profil. Vielmehr wurden diese mit einem Prozess der sogenannten „Telefonnummernaufzählung“ bereitgestellt. Vor diesem Hintergrund luden die „Scraper“ mithilfe des „CIT“ fingierte Kontakte hoch, welche mögliche Telefonnummern von Nutzern enthielten, um festzustellen, ob diese Telefonnummern mit einem Facebook-Konto verbunden sind. Soweit sie feststellen konnten, dass eine Telefonnummer mit einem Facebook-Konto verknüpft war, kopierten sie die öffentlich einsehbaren Informationen aus dem betreffenden Nutzerprofil und fügten die Telefonnummer den abgerufenen, öffentlich einsehbaren Daten hinzu. Anfang April 2021 wurden die „gescrapten“ Daten einschließlich der o.g. Daten des Klägers im Internet verbreitet. Insgesamt wurden Daten von ca. 533 Millionen Facebook-Profilen im Internet verbreitet. Im April 2019 berichteten verschiedene Medien über diesen Vorfall.

Im Nachgang zu dem „Scraping“ führte die Beklagte proaktiv eine Schutzmaßnahme für den Kontakt-Importer der Facebook-Plattform ein, die darauf abzielte, einen übereinstimmenden Kontakt nur dann anzuzeigen, wenn die beiden Nutzer einander zu kennen schienen (der sogenannte „Social Connection Check“). Lud ein Nutzer seine Kontaktliste von seinem Mobiltelefon über den Kontakt-Importer der Facebook-Plattform hoch, wurde der übereinstimmende Nutzer nur dann dem importierenden Nutzer angezeigt, wenn (a) der importierende Nutzer einen Namen (sowie die Telefonnummer) für den hochgeladenen Kontakt importierte, der dem Namen des

übereinstimmenden Facebook-Nutzers ähnelte oder (b) der übereinstimmende Nutzer den importierenden Nutzer bereits in seinen Facebook-Kontakten hatte.

Mit außergerichtlicher E-Mail vom 02.06.2021 (Anlage K1) ließ der Kläger die Beklagte durch seine Prozessbevollmächtigten zur Zahlung von 500,- € bis zum 05.07.2021, zur Unterlassung der rechtswidrigen Verarbeitung der personenbezogenen Daten sowie zur Erteilung einer Auskunft, welche Daten im Zusammenhang mit dem im April 2021 bekannt gewordenen Datenschutzvorfall wann abhandengekommen seien, wo und wann diese verbreitet worden seien, ob die Sicherheitslücke durch mehrere Unbefugte ausgenutzt worden sei und welche Maßnahmen zukünftig zur Vermeidung einer Wiederholung ergriffen würden, innerhalb eines Monats auffordern. Die Beklagte erteilte daraufhin mit Schreiben vom 23.08.2021 Auskunft; wegen der Einzelheiten dieses Schreibens wird auf die Anlage K2 verwiesen.

Der Kläger ist der Ansicht, die Beklagte habe gegen die DSGVO verstoßen. Sie habe seine betreffenden personenbezogenen Daten ohne Rechtsgrundlage und ausreichende Informationen verarbeitet, weil die Informationen unübersichtlich und unvollständig seien. Weiterhin habe die Beklagte seine Daten unbefugten Dritten zugänglich gemacht und hierbei zahlreiche DSGVO-Pflichten verletzt.

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 so undurchsichtig und kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne.

Die Datenschutzeinstellungen der Beklagten seinen 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 widerspräche allerdings den Grundsätzen eines nutzerfreundlichen Datenschutzes und den in der DSGVO niedergelegten Prinzipien der „privacy by default“ (= datenschutzfreundliche Voreinstellungen) und „privacy by design“ (= Datenschutz durch Technikgestaltung). Ihre Daten seien nach dem damaligen Stand der Technik bei der Beklagten nicht ausreichend geschützt gewesen.

Der Kläger behauptet zudem, dass er durch den Scraping-Sachverhalt einen erheblichen Kontrollverlust über seine Daten erlitten habe und in einem Zustand großen Unwohlseins und Sorge über einen möglichen Missbrauch seiner Daten verbleibe, was sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen, aber auch in der ständigen Sorge, dass die veröffentlichten Daten von Kriminellen für unlautere Zwecke verwendet werden könnten, manifestiere.

Die Beklagte habe darüber hinaus weder ihn noch die zuständige Aufsichtsbehörde über den Datenschutzverstoß informiert und sei mithin ihren Informationspflichten gem. Art. 33 und 34 DSGVO und auch dem Anspruch auf Auskunft aus Art. 15 DSGVO nicht in ausreichendem Maße nachgekommen.

Der Kläger hält einen immateriellen Schadensersatz in Höhe von 1.000,- € für angemessen. Aus der Verpflichtung der Beklagten zur Leistung von Schadensersatz aus dem dargestellten Schadensereignis folge auch die Pflicht, zukünftige Schäden, die aufgrund der entwendeten Daten entstünden, zu tragen. Er habe weiter einen Anspruch auf Unterlassung, seine personenbezogenen Daten in Zukunft unbefugt, d.h. konkret ohne vorherige ausreichende Belehrung, zu veröffentlichen und diese zukünftig unbefugten Dritten zugänglich zu machen. Der Kläger habe Anspruch auf weitere Auskunft, insbesondere über die konkreten Empfänger der personenbezogenen Daten.

Der Kläger beantragt, wie folgt zu erkennen:

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 hält die Klage bereits aus verschiedenen Gründen für unzulässig.

Die Beklagte meint, der Sachverhalt und Vorgang zum sogenannten Scraping sei falsch wiedergeben. Der klägerische Vortrag beruhe auf einem Missverständnis zum Scraping als solchen. Der Kläger habe nicht substantiiert dargetan, welche Daten gescrapt worden sein sollen. Die Beklagte bestreitet einen Datenschutzverstoß und das

Unterlassen des Schließens einer technischen Schwachstelle. Vielmehr seien lediglich automatisch gesammelte öffentlich einsehbare Daten entweder von der App oder der Website Facebook durch Dritte in Form des Scraping abgerufen worden. Das Abrufen habe im Einklang mit den jeweiligen Privatsphäre-Einstellungen „öffentlich“ auf der Facebook-Plattform gestanden.

Die Beklagte 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. Die Beklagte ist weiter 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. Den Anforderungen des Art. 25 DSGVO sei genügt. Es dürfe dabei der zentrale Zweck von Facebook, sich mit Freunden, Familien und Gemeinschaften zu verbinden, nicht außer Betracht bleiben. Eine Melde- oder Benachrichtigungspflicht habe nicht bestanden, weil es an einer Verletzung der Sicherheit i. S. d. Art. 4 Nr. 12 DSGVO und an einer unbefugten Offenlegung von Daten fehle. Schließlich fehle es an einem immateriellen Schaden. Art. 82 DSGVO umfasse keine Verstöße gegen Art. 13-15, 24, 25 DSGVO. Ein kompensationsgeeigneter messbarer Schaden sei auch nicht dargelegt. Selbst bei einem angenommenen vorübergehenden Kontrollverlust über personenbezogene Daten des Klägers wäre dies nicht der Beklagten zuzurechnen, weil die öffentliche Einsehbarkeit den Privatsphäre-Einstellungen des Klägers entsprochen habe. Schließlich fehle es an einer schlüssigen Darlegung der Kausalität.

Die Klage wurde der Beklagten entsprechend Auskunft zum Sendestatus über www.deutschpost.de am 11.10.2022 zugestellt.

Die Kammer hat den Kläger persönlich angehört. Wegen des Ergebnisses der Anhörung wird auf das Protokoll der mündlichen Verhandlung vom 04.07.2023 Bezug genommen (Bl. 219 ff. d.A.).

Im Übrigen wird wegen der weiteren Einzelheiten des Sach- und Streitstandes auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen verwiesen.

Entscheidungsgründe

Die Klage ist zulässig, aber nur teilweise begründet.

A. Die Klage ist zulässig.

I. Das Landgericht Hannover ist international, sachlich und örtlich zuständig.

1) Deutsche Gerichte sind international zuständig.

a) Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 2. Alt. EuGVVO (Brüssel Ia VO).

Gemäß Art. 1 Abs. 1 EuGVVO ist die EuGVVO sachlich anwendbar auf Zivil- und Handelssachen. Vorliegend handelt es sich um eine Zivilsache.

Die Zuständigkeit der deutschen Gerichtsbarkeit folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 2. Alt. EuGVVO. Ein ausschließlicher Gerichtstand gemäß Art. 24 EuGVVO ist hier 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 Verbraucher. Er gibt an, einen Nutzungsvertrag mit der Beklagten geschlossen zu haben über die Nutzung der Social-Media-Plattform Facebook mittels eines Benutzerkontos zu privaten Zwecken. Als doppelrelevante Tatsache reicht in der Zulässigkeit das Behaupten von Tatsachen, aus denen sich ein solcher vertraglicher Anspruch ergeben kann.

Der Kläger hat seinen Wohnort in Springe Eldagsen in Deutschland.

b) 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. Auftragsverarbeitende sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten.

Die Beklagte selbst erklärt, dass sie in den meisten Fällen die Rolle als Verantwortliche bekleide. Lediglich, wenn sie Werbekunden bediene, könne sie ausnahmsweise als Auftragsverarbeitende fungieren (https://www.facebook.com/business/gdpr). Die Beklagte ist zudem keine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

Der Kläger als betroffene Person hat seinen Wohnsitz in Deutschland. Die deutsche Gerichtsbarkeit ist international zuständig.

2) Das Landgericht Hannover ist gemäß §§ 23 Nr. 1, 71 Abs. 1 GVG sachlich zuständig. Der Streitwert liegt bei über 5.000,- €.

3) Die örtliche Zuständigkeit folgt aus Art. 18 Abs. 1 2. Alt. EuGVVO.

Danach 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. Das Landgericht ist unabhängig davon nach Art. 79 Abs. 2 S. 2 DSGVO, § 44 Abs. 1 S. 2 BDSG örtlich zuständig (besonderer Gerichtsstand).

Der Kläger hat seinen Wohnsitz in Springe Eldagsen und damit im Bezirk des angerufenen Gerichts.

II) Die Klage ist hinreichend bestimmt.

1) Der Zulässigkeit der Klage steht nicht die Unbestimmtheit des Klageantrags zu 1) (§ 253 Abs. 2 ZPO) entgegen.

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. 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 (vgl. Greger in: Zöller, 33. Aufl. 2020, § 253 ZPO Rn. 14). Diese Voraussetzungen liegen hier vor. Der Kläger hat einen Mindestbetrag angegeben.

Dabei liegen entgegen der Auffassung der Beklagten auch nicht zwei Streitgegenstände (Verhalten vor dem Scraping-Vorfall einerseits und Geschehen nach diesem Vorfall andererseits) vor. Maßgeblich ist insoweit der sogenannte zweigliedrige Streitgegenstandsbegriff; danach wird der Streitgegenstand durch den Antrag und den zu seiner Begründung vorgetragenen Lebenssachverhalt als gleichwertige Elemente gebildet; demgemäß lässt sich der Streitgegenstand definieren als das Begehren der vom Kläger auf Grund eines bestimmten Lebenssachverhalts beantragten Entscheidung; dabei wird der Lebenssachverhalt aus allen Tatsachen gebildet, die bei einer natürlichen, vom Standpunkt der Parteien ausgehenden Betrachtungsweise zu dem durch den Vortrag des Klägers zur Entscheidung gestellten Tatsachenkomplex gehören (vgl. MüKoZPO, 6. Aufl., ZPO vor § 253 Rn. 32, 33, m.w.N., beck-online). Diese Betrachtungsweise verbietet vorliegend eine Differenzierung des Geschehens vor und nach dem Scraping, denn die Umstände nach dem Scraping stellen die Fortsetzung des Sachverhaltes bis zu diesem Zeitpunkt dar.

2) Der Klagantrag zu 2) – Feststellungsanspruch – ist ebenfalls hinreichend bestimmt.

Die Antragsformulierung „alle künftigen Schäden […] die entstanden sind und / oder noch entstehen werden“, lässt sich zwanglos dahingehend auslegen, dass damit all diejenigen möglichen Schäden gemeint sind, die erst nach Schluss der mündlichen Verhandlung entstehen oder vorher entstanden sind, dem Kläger aber erst nach dem vorgenannten Zeitpunkt bekannt werden.

3) Der Antrag zu 3) - Unterlassungsanspruch - ist hinreichend bestimmt.

Zwar ist die Formulierung „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ auslegungsbedürftig, so dass Vollstreckungsprobleme

denkbar sind. Allerdings ist nach höchstrichterlicher Rechtsprechung eine gewisse Auslegungsbedürftigkeit zur Gewährleistung effektiven Rechtsschutzes hinzunehmen (BGH, GRUR 2015, 1237, Rn. 15, BGH NJW 2004, 2080). Der Kläger kann nicht einschätzen, was die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen beinhalten, was dann dazu führt, dass das Vollstreckungsorgan gegebenenfalls Wertungen vornehmen muss. Es wäre verfehlt im Lichte des effektiven Rechtsschutzes i. S. d. Art. 19 GG, würde von dem Kläger verlangt, dass er für eine hinreichend konkrete Antragstellung den aktuellen Stand der Technik selbst ermitteln muss. Dies gilt umso mehr, als sich der Stand der Technik künftig fortlaufend ändern mag.

III. Es besteht zudem ein Feststellungsinteresse gemäß § 256 Abs. 1 ZPO bezüglich des Antrags zu 2).

Der Kläger hat sein Feststellungsinteresse gemäß § 256 Abs. 1 ZPO hinreichend dargelegt. 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 (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 dargelegten unkontrollierten Nutzung gescrapter Daten ist bei verständiger Würdigung zumindest nicht gänzlich ausgeschlossen, dass irgendein materieller oder immaterieller Schaden künftig noch entstehen könnte.

Die Frage, ob auch eine gewisse Wahrscheinlichkeit für einen künftigen Schadenseintritt besteht, ist als solche der Begründetheit des Feststellungsantrags anzusehen.

IV. Es besteht auch ein Rechtsschutzinteresse bzgl. des Antrags zu 3) (Unterlassung) soweit die Telefonnummer betroffen ist.

Die Beklagte meint, weil der Kläger durch Anpassung seiner Suchbarkeitseinstellungen es selbst verhindern könne, dass sein Profil anhand ihrer Telefonnummer gefunden werden könne – und dies später auch getan habe – bestehe insoweit für den Unterlassungsanspruch kein Rechtsschutzinteresse; weshalb der Kläger weiterhin ein Interesse an der gerichtlichen Klärung haben sollte für eine rein potenzielle Möglichkeit

des Auslesens der Telefonnummer bei einem künftigen Scraping-Vorfall, sei bloße Spekulation und unsubstantiiert.

Diese Argumentation greift nicht durch. Das Rechtsschutzbedürfnis soll nur objektiv sinnlose Klagen verhindern; wegen des grundsätzlich bestehenden Justizgewährungsanspruchs darf diese Zulässigkeitsvoraussetzung nur unter ganz besonderen Umständen verneint werden; hiervon zu trennen ist dabei die materielle Berechtigung des Klagebegehrens; im Zweifel muss schon aus Rechtskraftgründen die Zulässigkeit angenommen und gegebenenfalls dann (erst) die Begründetheit des Anspruchs verneint werden, dies gilt insbesondere dann, wenn sich die Schutzwürdigkeit der klägerischen Position erst aufgrund näherer Prüfung materiell-rechtlicher Fragen beurteilen lässt, dann darf das Rechtsschutzbedürfnis nicht verneint werden (vgl. Zöller-Greger, ZPO, 34. Aufl., Vor § 253 Rn. 18).

B. Die Klage ist teilweise begründet.

I. Der Antrag zu Ziffer 1) (Schadensersatz) ist in Höhe von 500,- € begründet.

Der Kläger hat gegen die Beklagte einen Anspruch auf Schadensersatz aus Art. 82 DSGVO in Höhe von 500,- €.

1) Eine Pflichtverletzung der Beklagten in diesem Sinne ist gegeben.

a) Zum einen liegt ein Verstoß gegen Art. 13 DSGVO vor. Die Beklagte ist den ihr nach Art. 13 DSGVO auferlegten Informations- und Aufklärungspflichten nicht in vollständigem Umfang nachgekommen.

aa) Bei Art. 13 DSGVO handelt es sich um Konkretisierungen der Grundsätze nach Maßgabe von Art. 5 Abs. 1 DSGOV.

„Die in Art. 5 Abs. 1 niedergelegten Grundsätze werden in Einzelvorschriften der DS-GVO konkretisiert. Der Grundsatz der Rechtmäßigkeit wird vor allem in den Vorschriften über die Rechtmäßigkeit der Datenverarbeitung ausgestaltet (Art. 6 Abs. 1). Das Transparenzprinzip ist Grundlage für die Anforderungen an die Art und Weise und den Inhalt der Information und Benachrichtigung der betroffenen Personen (vor allem in Art. 7 Abs. 2, Art. 12–15 und Art. 34).“ (Ehmann/Selmayr/Heberlein, 2. Aufl. 2018, DS-GVO Art. 5 Rn. 6)

bb) Bei der Vorschrift des Art. 13 DSGVO handelt es sich um eine solche, die zu dem Kreis der eine Schadensersatzpflicht gemäß Art. 82 DSGVO auslösenden Vorschriften zählt.

Die Kammer verkennt dabei nicht die restriktive Gegenauffassung:

> *„Es fehlt an einer schadenersatzauslösenden Pflichtverletzung der Beklagten im Sinne der DS- GVO.*
>
> *Soweit der Kläger der Beklagten mehrere Verstöße vorwirft, nämlich*
>
> *- ungenügende Information und Aufklärung über die Verarbeitung der sie betreffenden Daten durch ungenügende Aufklärung zu den Fragen der Verwendung und Geheimhaltung der Telefonnummer (Art. 5 Abs. 1 a DSGVO),*
>
> *- unmittelbaren Verstoß gegen Art. 13, 14 DSGVO, die konkrete Informationspflichten enthielten, die seitens der Beklagten nicht eingehalten worden seien, - ungenügender Schutz der personenbezogenen Daten der Nutzer von F. (Art. 24, 32 DSGVO),*
>
> *- unvollständige Auskunftserteilung nach Art. 15 DSGVO, da nicht mitgeteilt worden sei, welchen Empfängern die Daten des Klägers durch Ausnutzung des Kontaktimporttools zugänglich gemacht worden seien (Art. 33, 34 DSGVO)*
>
> *sind solche Verstöße schon nicht vom Schutzzweck des Art. 82 DSGVO umfasst.*
>
> *Art. 82 Abs. 1 DSGVO legt fest, dass jeder Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter hat. Art. 82 Abs. 2 DSGVO regelt den anspruchsbegründenden Sachverhalt. Gemäß Art. 82 Abs. 2 S. 1 DSGVO haftet danach jeder an einer Verarbeitung von Daten beteiligte Verantwortliche für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Anknüpfungspunkt für eine Haftung ist also eine der Verordnung nicht entsprechende Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO.*
>
> *Gemäß Art. 4 Nr. 2 DSGVO ist Verarbeitung jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im*

Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, durch den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Die behauptete Verletzung von bloßen Benachrichtigungspflichten bzw. Informationsrechten ist hingegen nicht erfasst (AG Strausberg, Urteil vom 13.10.2022, 25 C 95/21, BeckRS 2022, 27811, Rn. 17).

Der Schutzbereich des Art. 82 DSGVO als hier maßgebliche Anspruchsgrundlage umfasst ebensowenig Verstöße gegen Artikel 34 DSGVO (s. a.: OLG Stuttgart, Urteil vom 31.3.2021, 9 U 34/21, juris Rn. 61; LG Düsseldorf, Urteil vom 28.10.2021, 16 O 128/20, GRUR-RS 2021, 33076, Rn. 27; LG Bonn, Urteil vom 1.7.2021, 15 O 372/20, juris, Rn. 41). Schließlich lässt sich auch von vornherein aus Artikel 24 DSGVO kein entsprechendes subjektives Recht herleiten (Taeger/Gabel, DSGVO, 4. Auflage 2022, Artikel 24, Rn. 89).

Selbiges gilt für Art. 25 DSGVO (Taeger/Gabel, DSGVO, a. a. O., Art. 25, Rn. 100). Daher kann auch dahin stehen, ob Verstöße etwa gegen Artikel 13, 14 und 34 (in diesem Sinne verneinend auch AG Straußberg, Urteil vom 13.10.2022, 25 C 95/21, juris, Rn. 19) durch die Beklagte erfolgten, da auch sie nicht unter den Schutzbereich des Art. 82 DSGVO fallen, weil auch sie „lediglich" Informationspflichten über die Verarbeitung enthalten, nicht aber die Verarbeitung als solche zum Gegenstand haben."

(LG Görlitz Endurteil v. 27.1.2023 – 1 O 101/22, BeckRS 2023, 1148 Rn. 30-34)

Die Kammer schließt sich indes der Rechtsauffassung an, nach der der Kreis derjenigen Pflichten, deren Verletzung gemäß Art. 82 DSGVO Schadensersatzpflichten auslösen, auch die Verletzung von Informations- und Aufklärungspflichten erfasst:

„Gemäß Art. 82 Abs. 1 DS-GVO haftet der Verantwortliche für Schäden wegen „Verstößen gegen diese Verordnung". Grund und damit unabdingbare Voraussetzung der Haftung ist eine Pflichtverletzung, wenngleich es auf einen Schutznormcharakter der verletzten Vorschrift nicht ankommt, der Begriff der Pflichtverletzung also denkbar weit gefasst ist und letztlich jede Verletzung

materieller oder formeller Bestimmungen der Verordnung einschließt (vgl. OLG Stuttgart, Urteil vom 31.03.2021 - 9 U 34/21, BeckRS 2021, 6282 Rn. 25; Kreße in Sydow/Marsch, DS-GVO | BDSG, 3. Aufl. DS-GVO Art. 82 Rn. 7; a.A. Gola/Piltz in Gola/Heckmann, DS-GVO - BDSG, 3. Aufl. DS-GVO Art. 82 Rn. 5).“

(LG Stuttgart Urt. v. 26.1.2023 – 53 O 95/22, BeckRS 2023, 1098 Rn. 44)

Danach sind namentlich auch Verstöße gegen Art. 13 DSGVO von Art. 82 DSGVO erfasst:

„Ein Verstoß gegen Art. 13 DS-GVO kann - entgegen der Annahme der Beklagten - ohne weiteres einen Schadensersatzanspruch nach Art. 82 DS-GVO nach sich ziehen (vgl. nur Schmidt-Wudy in BeckOK-Datenschutzrecht, Stand: 01.11.2022 DS-GVO Art. 13 Rn. 18; Franck in Gola/Heckmann, DS-GVO - BDSG, 3. Aufl. DS-GVO Art. 13 Rn. 64; a.A. LG Essen, Urteil vom 10.11.2022 - 6 O 111/22, GRUR-RS 2022, 34818).“

(LG Stuttgart Urt. v. 26.1.2023 – 53 O 95/22, BeckRS 2023, 1098 Rn. 64)

In der Abwägung der Argumente ist die zweitgenannte Ansicht überzeugender:

Die restriktive Auffassung wird u.a. auf Erwägungsgrund 146 S. 1 zur DSGVO gestützt, der auf die Verarbeitung Bezug nimmt:

„Zunächst muss bei einer Verarbeitung gegen die DS-GVO verstoßen worden sein. Zwar wurde im Verfahren zum Erlass der DS-GVO die Einbeziehung sämtlicher Handlungen über eine Verarbeitung hinaus in Art. 82 debattiert. Letztlich wurde der Wortlaut von Art. 82 insoweit zwar offen formuliert, der Erwägungsgrund 146 S. 1 dafür umso klarer auf Schäden infolge einer Verarbeitung begrenzt. Der Begriff der Verarbeitung ist jedoch weit gefasst, und hinsichtlich anderer Handlungen oder Unterlassungen bestehen andere Anspruchsgrundlagen.“

(Ehmann/Selmayr/Nemitz, 2. Aufl. 2018, DS-GVO Art. 82 Rn. 8)

Wörtlich lautet dieser Erwägungsgrund:

„Erwägungsgrund 146 S. 1: „Der Verantwortliche oder der Auftragsverarbeiter sollte Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen.“

Die Beschränkung auf Verletzungen im Rahmen der (i.R.d.) Datenverarbeitung widerspräche indes dem Wortlaut des Art. 82 Abs. 1 DSGVO und v.a. – und letztlich entscheidend – dem Ziel des Art. 82 DSGVO. Wären nämlich Verstöße gegen die Informations- und Aufklärungspflichten von dem Schadensersatz-Regime ausgenommen, drohte eine erhebliche Schutzlücke. Bereits mit der unterlassenen Aufklärung ergeben sich erhebliche Gefährdungslagen für den Nutzer, was es rechtfertigt, entsprechende Pflichtverstöße unmittelbar mit einer Schadensersatzrechtsfolge zu belegen.

cc) Es liegt auch im konkreten Fall eine Verletzung des Art. 13 Abs. 1 lit. c DSGVO vor.

(a) Gemäß Art. 13 DSGVO hat der Verantwortliche eines Datenverarbeitungsprozesses gegenüber dem Betroffenen, dessen personenbezogene Daten verarbeitet und bei diesem erhoben werden, umfangreiche Informations- und Aufklärungspflichten zu erfüllen. Nach Art. 13 Abs. 1 lit. c DSGVO besteht eine Informationspflicht insbesondere dahingehend, dass der Verantwortliche dem Betroffenen die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung mitteilt. Sinn und Zweck dieser Regelung ist, dass der Betroffene eines Datenverarbeitungsprozesses unter Berücksichtigung der Grundsätze einer fairen und transparenten Verarbeitung von personenbezogenen Daten nicht nur über die Existenz des Verarbeitungsvorganges, sondern darüber hinaus auch über die Zwecke der Verarbeitung unterrichtet wird (Ehmann/Selmayr/Knyrim, 2. Aufl. 2018, DS-GVO Art. 13 Rn. 1).

(b) Teilweise wird in der Rechtsprechung in Fällen wie dem vorliegenden die Auffassung vertreten, die Beklagte habe diese Anforderungen erfüllt (so z.B. LG Heilbronn Urt. v. 13.1.2023 – 8 O 131/22, BeckRS 2023, 330, und dort besonders die Rn. 28-30).

(c) Nach der Gegenauffassung hat die Beklagte ihren Pflichten gem. Art. 13 Abs. 1 lit. c) DSGVO in Fällen wie dem hiesigen nicht genügt.

Diese Auffassung geht zunächst davon aus, dass es gerade auf die Informationen des Nutzers vor bzw. bei der Registrierung ankomme. Entsprechend der Legaldefinition des Art. 4 Ziffer 2 DSGVO entstünden die Informations- und Aufklärungspflichten bereits mit der Erhebung personenbezogener Daten. Teile der Verantwortliche dem Betroffenen bereits bei Datenerhebung die in Art. 13 Abs. 1 und Abs. 2 DSGVO vorgesehenen Informationen nicht vollständig oder inhaltlich unrichtig mit, verletze er seine Informationspflichten. Demgemäß komme es insbesondere auf die Informationen im „Hilfebereich", der nach Registrierung einsehbar und nutzbar ist, schon gar nicht an. Verwiesen wird für diese Rechtsauffassung auf die Entscheidung LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 65, 66, nach welcher

> *„es auf die Informationen im Hilfebereich schon nicht ankommen dürfte, da die Datenerhebung - entweder durch Hinzufügen der Mobilfunknummer bei der Registrierung oder bei den „Handy-Einstellungen" - bereits erfolgt ist und eine Aufklärung […] unterblieben ist".*

Im Übrigen geht diese Rechtsprechung davon aus, dass selbst dann, wenn man die Informationen aus dem Hilfebereich für die Aufklärung des Nutzers mitberücksichtigen würde, damit die Pflichten gemäß Art. 13 Abs. 1 lit. c DSGVO nicht hinreichend erfüllt wären. Eine Verletzung der Informations- und Aufklärungspflichten des Art. 13 Abs. 1 lit. c DSGVO könne zwar nicht schon darin gesehen werden, dass seitens der Beklagten kein Hinweis bei Erhebung der Daten der Mobilfunknummer des Klägers erfolgt ist, dass bei der voreingestellt für „Alle" freigegebenen Mobilfunknummer die Möglichkeit einer missbräuchlichen Datenabgreifung besteht. Diese Möglichkeit sei nämlich nie ganz auszuschließen und unterfalle der Risikosphäre der betroffenen Person, weil dem Risiko einer missbräuchlichen Verwendung von persönlichen Daten zwangsläufig jede Person ausgesetzt sei, die ihre persönlichen Daten im Internet preisgebe bzw. diese in sozialen Netzwerken teile. Die Beklagte habe den Netzwerk-Nutzer allerdings bei Erhebung der Daten seiner Mobilfunknummer unzureichend über den Zweck der Verwendung seiner Mobilfunknummer für das seitens der Beklagten verwendete Contact-Import-Tool (kurz: CIT) aufgeklärt. Hierdurch habe sie ihre Informations- und Aufklärungspflichten nach Art. 13 Abs. 1 lit. c) DSGVO verletzt.

Diese Rechtsprechung geht also davon aus, dass die Beklagte gegenüber den jeweiligen Klägern bei Datenerhebung eine Informations- und Aufklärungspflicht nach Art. 13 Abs. 1 lit. c) DSGVO dahingehend hatte, diese auch und gerade über die

beabsichtigte Verwendung seiner Mobilfunknummer für das CIT aufzuklären. Dies wird mit der spezifischen datenbezogenen Gefährdungslage durch das CIT begründet; durch die Verwendung des CIT ermögliche die Beklagte einem beliebigen Benutzer den Abgleich, der in seinem Smartphone gespeicherten Personenkontakte mit auf Facebook registrierten Benutzerprofilen, die ihr Benutzerprofil jeweils mit einer Mobilfunknummer verknüpft haben. Durch die Eingabe einer beliebigen Mobilfunknummer werde dem Benutzer ermöglicht, das mit der Mobilfunknummer verknüpfte Benutzerprofil zu identifizieren und die dort öffentlichen Daten einzusehen und ggf. zu verwenden.

(d) Die besseren Gründe sprechen aus Sicht der Kammer für die letztgenannte Auffassung, die einen Verstoß gegen Art. 13 Abs. 1 lit. c DSGVO bejaht. Die Beklagte ist der ihr auferlegten Informations- und Aufklärungspflicht nicht in vollständigem Umfang nachgekommen.

Nach Art. 13 Abs. 1 lit. c DS-GVO sind die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, zum Zeitpunkt der Erhebung der Daten mitzuteilen. Dem hat die Beklagte hinsichtlich der Verwendung der Mobilfunknummer für das von ihr verwendete Contact-Import-Tool (CIT) nicht genügt. Sie hat zum Zeitpunkt der Datenerhebung somit hinsichtlich der Mobilfunknummer nicht ausreichend über die Zwecke der Verarbeitung dieser Nummer aufgeklärt. Für die nach Art. 13 Abs. 1 lit. c DS-GVO erforderliche Aufklärung ist also davon auszugehen, dass sich diese gerade auf das CIT erstrecken muss, sodass eine Aufklärung über eine bloße „Auffindbarkeit“ anhand der Mobilnummer nicht ausreicht. Denn eine bloße „Auffindbarkeit“ kann so verstanden werden, dass andere Nutzer lediglich im Einzelfall die ihnen bekannte Mobilfunknummer eines Freundes oder Bekannten bei Facebook eingeben und diese Person finden können. Das CIT ermöglicht demgegenüber die Hochladung ganzer Kontaktlisten mit automatisiert-programmatischer Verknüpfung der Facebook-Profile. Damit verbindet sich aber auf der anderen Seite auch eine besondere Risikolage, weil somit eine Vielzahl von Suchaktionen gleichsam gebündelt erfolgen kann, was nicht zuletzt auch die Missbrauchsgefahr (etwa über fingierte Kontaktlisten mit auf „Glückauf“ ersonnenen Telefonnummern bei besonders vielen Teilnehmern) steigert. Gerade deswegen muss nicht nur über die „Auffindbarkeit“ via Mobilfunknummer, sondern auch spezifisch über die Funktionsweise des CIT aufgeklärt werden.

(e) Aus den vorgelegten Unterlagen ist nicht ersichtlich, dass die Beklagte über das CIT und seine Funktionsweisen aufgeklärt hat.

Zutreffend unterteilt die Rechtsprechung die betreffenden Informationen in drei Kategorien, nämlich:

- die Informationen in der Datenrichtlinie (aa),
- die Informationen im Hilfebereich (bb) sowie
- die bei der Registrierung bzw. späteren Hinzufügung einer Mobilfunknummer zur Verfügung gestellten Angaben (cc).

(aa) Den mit der Anlage B 9 und B 20 (Anlagenband Beklagte) überreichten Datenrichtlinien lässt sich eine Aufklärung über das von der Beklagte verwendete CIT nicht entnehmen.

Der Datenrichtlinie 2018 lässt sich auf den Seiten 3 und 4 unter der Überschrift *„Wie verwenden wir diese Informationen“* entnehmen, dass die von einem Benutzer preisgegebenen Informationen zur Bereitstellung, Verbesserung und Entwicklung der Dienste, zur Kommunikation mit dem die Informationen bereitstellenden Benutzer, zum Anzeigen und Messen von Werbeanzeigen und Diensten sowie zur Förderung der Sicherheit verwendet werden. Ein Hinweis auf die Verwendung der Mobilfunknummer für das CIT erfolgt nicht.

Auch den Hinweisen auf den Seiten 5 und 6 der Datenrichtlinie unter der Überschrift *„Wie werden diese Informationen geteilt“* lässt sich ein Hinweis auf die Verwendung der Mobilfunknummer für das CIT nicht entnehmen.

(bb) Auch mit dem Hilfebereich ist keine ausreichende Aufklärung über das CIT erfolgt:

Zunächst ist nochmals festzuhalten, dass es auf die dortigen Informationen, die erst nach Abschluss der Registrierung aufgerufen werden können und dem Nutzer gerade nicht bereits vor bzw. bei der Registrierung zur Verfügung gestellt werden, schon aus grundsätzlichen Erwägungen nicht ankommt.

Selbst wenn man dies anders bewerten wollte, wären die Informationen im Hilfebereich auch nicht ausreichend. Ein Hinweis auf die Verwendung des CIT lässt sich nämlich den dem Hilfebereich entnommenen Informationen, in das vorliegende Verfahren eingeführt als Anlagen B2 bis B6, nicht entnehmen. Die größte inhaltliche Nähe zum hier interessierenden Thema Suchbarkeit/CIT weisen die Inhalte der Anlagen B 5 und B 6 auf. Keine dieser Anlagen enthält hinreichende Informationen über die Verwendung des CIT.

Das gilt zunächst für die Inhalte der Anlage B5: Zwar wird in dem Abschnitt *„Wie kann ich festlegen, wer mich über meine E-Mail-Adresse oder Handynummer auf Facebook finden kann?“* (Anlage B 5) auf die Einstellungen der Suchbarkeit in Bezug auf E-Mail-Adressen und Telefonnummern eingegangen. Dem Nutzer wird mitgeteilt, aus dem Menü neben der jeweiligen Einstellung könne er auswählen, wer ihn anhand dieser Informationen finden kann. Damit könnte sich aber allenfalls eine Aufklärung darüber verbinden, dass dem Nutzer vor Augen geführt wird, dass er über eine von ihm angegebene Telefonnummer von bestimmten Personengruppen durch Eingabe derselben aufgefunden werden kann. Selbst dies wird aber nicht wirklich klar. So findet sich in der Anlage B5 (auch) der Satz: *„Wenn du deine Telefonnummer oder deine E-Mail-Adresse in deinem Profil mit jemandem teilst, kann diese Person dich anhand dieser Informationen finden. Erfahre, wie du festlegst, mit wem du deine E-Mail-Adresse oder Telefonnummer teilst“.* Dieser Satz ist schon für sich genommen irreführend. Denn es erscheint hiernach so, als müsste der Nutzer selbst aktiv werden und sich im Einzelfall entscheiden, die Telefonnummer oder E-Mail-Adresse „mit jemandem“, also naheliegend mit einer konkreten Person, zu teilen. Erst nach dieser Entscheidung werde die Auffindbarkeit anhand dieser Daten „freigegeben“. Diese Information klärt also nicht einmal über eine bloße Suchbarkeit anhand der Telefonnummer als solche auf, sondern führt gerade im Gegenteil zu Unklarheiten und Verwirrungen, wenn nicht gar zu der Annahme, eine solche Suchbarkeit sei ohne Einzelfallentscheidung des Nutzers, die Daten aktiv mit jemandem zu teilen, ausgeschlossen. Erst recht aber findet sich hier keine – nach hier vertretener Auffassung aber erforderliche (s.o.) – Aufklärung gerade über die Funktionsweise des CIT.

Auch in der Hilfe zum Thema *„Wozu verwendet Facebook meine Mobilnummer?“* (Anlage B 6) finden sich keine hinreichenden Hinweise auf das CIT.

(cc) In Parallelverfahren hat die Beklagte teilweise auch zu Hinweisen im Rahmen der Registrierung bzw. bei Hinzufügung einer Mobilfunknummer im Rahmen sogenannten „Handy-Einstellungen“ vorgetragen (s. beispielhaft die tatsächlichen Feststellungen bei LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349, und dort im Besonderen Rn. 62-64). Selbst wenn die betreffenden Informationen aufgrund der Angaben in Parallelverfahren als „gerichtsbekannt“ zugrunde zu legen wären, ergäbe sich daraus nichts für eine hinreichende Aufklärung:

Dass die Beklagte die Nutzer über das durch sie verwendete CIT aufgeklärt hat, lässt sich der Rubrik *„Handy-Einstellungen“* sowie der Unterverlinkung durch einen Klick auf *„Mehr dazu“* nicht entnehmen. Dort findet sich zum einen die Aufklärung seitens der Beklagten über die Verwendung der Mobilfunknummer zum Zweck der „Zwei-Faktor-Authentifizierung“. Zum anderen erfolgt der Hinweis, dass durch das Hinzufügen der Mobilfunknummer eben diese mit dem Benutzerkonto verknüpft sei und der jeweilige Benutzer festlegen könne, welche Personen dessen Mobilfunknummer sehen und welche Personen nach der betroffenen Person suchen könnten. Ein weitergehender Hinweis, dass die betroffene Person gerade durch das CIT der Beklagten im Wege eines Kontaktabgleichs durch Eingabe einer Mobilfunknummer gefunden werden kann, lässt sich den Einstellungen gerade nicht entnehmen

(dd) Abschließend ist anzumerken, dass die vorgenannten Informationen auch nicht isoliert betrachtet werden dürfen. Vielmehr ist davon auszugehen, dass ein Nutzer nicht zwingend sämtliche der zu einem bestimmten Sachthema verfügbaren Informationen parallel zur Kenntnis nimmt.

Soweit daher einzelne Informationsbereiche bestimmte Inhalte oder Begrenzungen hinsichtlich der Datenverwendung nahelegen, muss sich die Beklagte daran festhalten lassen. Insoweit sind hier insbesondere die Inhalte gemäß Anlage K 6 im Hilfebereich zu würdigen. Dabei wird durch die dort enthaltene 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“* bereits in Bezug auf die bloße „Auffindbarkeit“ des Nutzers über eine eingegebene Telefonnummer 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, um seinerseits andere Facebook-Nutzer zu finden. Da zudem die Überschrift „*Möglicherweise verwenden wir*

deine Mobilnummer für diese Zwecke“ durchaus nahelegt, damit würden die Verwendungszwecke abschließend umschrieben, und sich auch sonst in Anlage K 6 keinerlei Hinweise auf die Suchbarkeit finden, kann hier der Eindruck entstehen, eine solche Auffindbarkeit sei nicht implementiert. Dass der Nutzer die Inhalte aus Anlage K 5, die wie oben dargestellt etwas weitergehend aufklären, parallel liest und all dies systematisch auslegt, kann nicht erwartet werden. Vielmehr widerspricht dies der Lebenserfahrung und –wirklichkeit.

In der Gesamtbetrachtung fehlt es also an einer hinreichenden Information jedenfalls über die Möglichkeiten des CIT, sodass von einem Aufklärungspflichtverstoß auszugehen ist.

b) Daneben liegt ein Verstoß gegen Art. 25 Abs. 1 DSGVO vor.

aa) In vergleichbaren Fällen wird hierzu in der Rechtsprechung Folgendes ausgeführt:

> *„aa) Die Beklagte hat gegen die ihr gemäß Art. 25 Abs. 1 DS-GVO auferlegte Obliegenheit verstoßen, geeignete Maßnahmen zu treffen, um die Rechte der klagenden Partei und ihre personenbezogenen Daten zu schützen.*
>
> *Nach Art. 25 Abs. 1 DS-GVO hat der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.*
>
> *[…]*
>
> *Die von der Beklagten implementierten Sicherheitsmaßnahmen waren nicht ausreichend, um die Rechte der klagenden Partei und ihre personenbezogenen Daten insbesondere vor unbefugter oder unrechtmäßiger Verarbeitung durch Dritte zu schützen. Dabei kann dahinstehen, ob die Beklagte die von ihr behaupteten Maßnahmen zur Bekämpfung von Scraping tatsächlich ergriffen hat, denn diese*

Maßnahmen waren jedenfalls für sich allein nicht geeignet, einen angemessenen Schutz der personenbezogenen Daten der klagenden Partei zu gewährleisten.

Die (angeblich) von der Beklagten implementierten Maßnahmen in Form von Ratenbegrenzung und Bot-Erkennungsmaßnahmen waren für die Zwecke des Art. 25 Abs. 1 DS-GVO nicht ausreichend, weshalb die Beklagte gegen Art. 25 Abs. 1 DS-GVO verstoßen hat. Insoweit befindet sich die Kammer im Einklang mit der irischen Datenschutzbehörde, die ebenfalls der Beklagten vorwirft, keine hinreichenden Sicherheitsmaßnahmen getroffen und damit gegen Art. 25 Abs. 1 DS-GVO verstoßen zu haben. Dabei berücksichtigt die Kammer, dass Scraping weit verbreitet und damit zum Zeitpunkt des Vorfalls unstreitig auch ein der Beklagten bekanntes Risiko gewesen ist. Hinsichtlich der von der Beklagten eingesetzten Übertragungsbeschränkungen war es nach dem eigenen Vortrag der Beklagten möglich, diese Beschränkungen zu umgehen. Trotz Kenntnis dieser Möglichkeit und auch des grundsätzlichen Risikos von „Scraping" hat es die Beklagte indessen unterlassen, weitergehende Maßnahmen zu treffen, was hier nach Auffassung der Kammer jedoch notwendig gewesen wäre. Es wäre für die Beklagte beispielsweise möglich gewesen, das Kontakt-Importer-Tool derart auszugestalten, dass eine Suche nach Nutzerprofilen nicht nur anhand von Telefonnummern erfolgen kann. Das Tool hätte beispielsweise neben der Telefonnummer weitere Variablen, wie den von dem Nutzer in seinem Adressbuch hinterlegten Vor- oder Nachname berücksichtigen können. Dies vor allem deshalb, weil Nutzer die Telefonnummern häufig mit dem dazugehörigen Klarnamen ihres Kontakts abspeichern. Entsprechend hat die Beklagte die Funktionsweise des Tools nach Bekanntwerden des Vorfalls auch umgestaltet."

(LG Lüneburg Urt. v. 24.1.2023 – 3 O 74/22, GRUR-RS 2023, 4813 Rn. 32-38)

bb) Die Gegenauffassung argumentiert wie folgt:

„Auch hat die Beklagte in der Klageerwiderung im Rahmen einer sekundären Darlegungslast substantiiert dargelegt, dass sie entgegen der pauschalen Behauptung des Klägers technische Maßnahmen ergriffen hat, um Scraping zu erschweren, indem sie nämlich eine Hürde implementiert hat, wonach Abfragen in gewissem Umfang von ein- und derselben IP-Adresse in einem bestimmten Zeitraum nicht möglich sind bzw. gestoppt werden, ebenso wie sie auch unter

Verweis auf diverse Artikel, deren Link sie ebenfalls bekannt gegeben hat, die User informiert hat und schließlich über ein Team verfügt, das sich einzig mit der Verhinderung von Missbrauch von Daten ihrer User beschäftigt. Angesichts dieser konkreten Ausführungen wäre von dem Kläger zu erwarten gewesen, dass er im Lichte dieses Vortrags weiter ausführt, warum er trotzdem von einem Verstoß gegen Art. 25 DSGVO ausgeht. Auch wenn man die Darlegungslast im Lichte der bereits zitierten Rechtsprechung des EuGH anders sieht, so wäre die Beklagte dieser nachgekommen, und der Kläger hätte dies nicht erheblich bestritten, so dass es auch insoweit nicht einer Beweisaufnahme bedurfte (LG Essen Urt. v. 10.11.2022 - 6 O 111/22, GRUR-RS 2022, 34818, Rn. 67). Die Klägerseite führt nicht näher aus, worin der Verstoß gegen Art. 25 DSGVO im Einzelnen vorliegen soll, insbesondere auch nicht, worin der DPC diese gesehen haben soll. Der Verweis auf Links ist soweit nicht als inhaltlich genügendes Bestreiten anzusehen (Bl. 366 f. d.A.). Auch führt ein Verstoß gegen Art. 25 DSGVO allein, wie von der Klägerseite zu der DPC vorgetragen, nicht zu einem Schadenersatzanspruch nach Art. 82 DSGVO (LG Essen Urt. v. 10.11.2022 - 6 O 111/22, GRUR-RS 2022, 34818 Rn. 47).“

(so LG Bielefeld, Urteil vom 10. März 2023 – 19 O 147/22 –, Rn. 46, juris)

cc) Die Kammer schließt sich aus folgenden Gründen der erstgenannten Auffassung an:

Zu beachten ist, dass die Beklagte nur unsubstantiiert ausführt, Übertragungsbeschränkungen hätten die Anzahl der konkreten Datenabfragen, die pro Nutzer oder IP-Adresse über einen bestimmten Zeitraum gestellt werden könnten, reduziert. Im Übrigen ist – wiederum allgemein – von „Maßnahmen zur Bot-Erkennung“ die Rede.

Auch wenn man davon ausgehen würde, dass die (primäre) Darlegungslast und damit auch Beweislast hierzu grundsätzlich bei der Klägerseite liegt, trifft die Beklagtenseite jedenfalls eine sekundäre Darlegungslast zu den von ihr getroffenen Sicherungsmaßnahmen. Es ist ohne weiteres ersichtlich, dass derartig allgemeine Ausführungen nicht genügen können. Eine „Reduzierung“ der Anzahl der Datenabfragen pro IP-Adresse lässt keinerlei Rückschlüsse auf die tatsächliche Quantität der möglichen Datenabfragen zu.

Im Übrigen ist zu berücksichtigen, dass eine „Reduzierung“ der Anzahl der Datenabfragen pro IP-Adresse für sich genommen schon keine hinreichende Sicherungsmaßnahme ist. Denn die „Scraper“ können ihr Abfrage-System mit allgemein verfügbaren Mitteln (etwa unter Nutzung von VPN-Services mit frei wählbaren IP-Adressen) so programmieren, dass die datenabfragenden IP-Adressen in relativ kurzfristigen Abständen wechseln.

Wie in der o.g. Entscheidung des Landgerichts Lüneburg ausgeführt, wäre das Kontakt-Importer-Tool derart auszugestalten gewesen, dass eine Suche nach Nutzerprofilen nicht nur anhand von Telefonnummern erfolgen kann. Das Tool hätte beispielsweise neben der Telefonnummer weitere Variablen, wie den von dem Nutzer in seinem Adressbuch hinterlegten Vor- oder Nachnamen, berücksichtigen können. Das betreffende Unterlassen muss die Klägerseite auch nicht explizit vortragen, weil das Gericht seinerseits bestimmen muss, ob die beklagtenseits ausdrücklich vorgetragenen Maßnahmen nach dem anzulegenden rechtlichen und infolgedessen auch technischen Maßstab ausreichend sind oder nicht. Für diese Beurteilung muss der jeweilige Maßstab (das „Soll“ als normative Vorgabe) durch das Gericht näher definiert werden. Diesem Soll wurde ersichtlich nicht genügt.

c) Zudem liegt ein Verstoß gegen Art. 25 Abs. 2 DSGVO vor.

Die Beklagte hat keine geeigneten technischen und organisatorischen Maßnahmen getroffen, mit denen sichergestellt wurde, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Hier geht es um „privacy per default“, also eine Maximierung des Datenschutzes durch datenschonende Voreinstellungen.

Die Suchbarkeit umfasste – unstreitig – automatisch die Telefonnummer der Nutzer. Die Suchbarkeits-Einstellungen hatte die Beklagte im hier relevanten Zeitraum auf „Alle“ voreingestellt, das heißt, dass jedermann mit der Telefonnummer nach einem Nutzerprofil suchen konnte und von jedermann auch über das Kontakt-Importer-Tool eine Verknüpfung zwischen Telefonnummer und dazugehörigem Nutzerprofil hergestellt werden konnte. Eine Ausnahme bestand nur dann, wenn der Nutzer nach seiner Registrierung die entsprechende Suchbarkeits-Einstellung in seinen Privatsphäre-Einstellungen aktiv änderte.

Mit der Bereitstellung dieses Systems machte die Beklagte die personenbezogenen Daten des Klägers ohne dessen Eingreifen einer unbestimmten Anzahl von Personen zugänglich. Das ist unter Beachtung des Nutzerinteresses, die personenbezogenen Daten zu schützen, welches gleichsam die „default option“ bildet (also: Schutzinteresse als Regel, Verzicht darauf durch Freigabe i.R.d. Suchbarkeit als Ausnahme), nicht angemessen. Dementsprechend hat auch die irische Datenschutzbehörde einen Verstoß der Beklagten gegen Art. 25 Abs. 2 DS-GVO angenommen (so zutreffend LG Lüneburg Urt. v. 24.1.2023 – 3 O 74/22, GRUR-RS 2023, 4813 Rn. 39, 40).

d) Der Kläger hat auch einen Schaden erlitten.

aa) Das Vorliegen eines Schadens stellt eine eigenständige Tatbestandsvoraussetzung des Art. 82 DSGVO dar. Ein Verzicht auf das – eigenständige – Erfordernis eines Schadens widerspräche dem Wortlaut des Art. 82 Abs. 1 DSGVO. Nach dieser Bestimmung wird der Schadensersatz gerade deshalb gewährt, weil zuvor ein Schaden entstanden ist. Es ist daher eindeutig erforderlich, dass der natürlichen Person durch einen Verstoß gegen die DSGVO ein Schaden entstanden ist (so auch: Generalanwalt beim EuGH Schlussantrag v. 6.10.2022 – C-300/21, BeckRS 2022, 26562 Rn. 27, 28).

bb) Damit kommt es vorliegend auf den positiven Nachweis eines über den bloßen Verstoß gegen die DSGVO hinausgehenden „Schadens“ an. Der Begriff des Schadens im Sinne von Art. 82 Abs. 1 DS-GVO ist - europarechtlich autonom und unter Berücksichtigung der in den Erwägungsgründen zur DSGVO niedergelegten Zielsetzungen - auszulegen (OLG Koblenz, Urteil vom 18.05.2022 - 5 U 2141/21, juris Rn. 72; OLG Hamm Urt. v. 20.1.2023 – 11 U 88/22, GRUR-RS 2023, 1263 Rn. 98).

(a) Bereits der Kontrollverlust über die Daten stellt nach dieser europarechtlich-autonomen Auslegung einen Schaden im Sinne des Art. 82 DSGVO dar.

Dies folgt deutlich aus den Erwägungsgründen zur DSGVO (vgl. auch OLG Düsseldorf, ZD 2022, 337 Rn. 41; OLG Hamm Urt. v. 20.1.2023 – 11 U 88/22, GRUR-RS 2023, 1263 Rn. 106: „*Hiernach reicht insbesondere ein Kontrollverlust der eigenen personenbezogenen Daten für die Annahme eines eingetretenen immateriellen Schadens aus*“).

In Erwägungsgrund 75, der sich mit Risiken für die Rechte und Freiheiten natürlicher Personen befasst, wird ausgeführt, diese Risiken könnten aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte. Letzteres wiederum sei u.a. dann anzunehmen, wenn die betroffenen Personen „daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren“. Wenn in der Literatur gegen diese Auslegung eingewendet wird, Erwägungsgrund 75 DSGVO befasse sich mit „Risiken für die Rechte und Freiheiten natürlicher Personen“ und ordne dementsprechend den Verlust der Kontrolle über personenbezogene (nur) als ein entsprechendes „Risiko“ ein, setze ihn also gerade nicht mit einem (immateriellen) Schaden gleich (so *Paal*, NJW 2022, 3673 Rn. 5), so vermag dies bereits grammatikalisch *nicht* zu überzeugen. Der Erwägungsgrund beginnt mit den folgenden Worten: „Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung [*es folgt ein weitgefasste Aufzählung einschließlich des Kontrollverlustfalles*]“. Hier wird deutlich, dass der Verordnungsgeber die „Risiken für die Rechte und Freiheiten natürlicher Personen“ gerade vor der Folie der möglichen *Schadensentstehung* ausdeutet. Anders ausgedrückt sind die hier thematisierten Risiken – nur – solche, die zu einem „physischen, materiellen oder immateriellen Schaden“ führen können. Die folgende Aufzählung macht dann konsequenterweise deutlich, wann dies der Fall ist, sie steckt also den Rahmen für den Schadensbegriff ab, um auf diesem Weg *zugleich* die relevanten Risiken, die an die Möglichkeit eines Schadens anknüpfen, zu beschreiben (i.E. wie hier Kühling/Buchner/*Bergt*, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18b: Den Kontrollverlust nenne Erwägungsgrund 75 ausdrücklich als ‚insbesondere‘ zu erwartenden Schaden). Diese Lesart wird durch Erwägungsgrund 85 gestützt, der sich mit der Meldepflicht von Verletzungen an die Aufsichtsbehörde auseinandersetzt. Dort wird in Satz 1 ausgeführt, eine Verletzung des Schutzes personenbezogener Daten könne „einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten“. Dass hier der Kontrollverlust sogar an erster Stelle der sich anschließenden weiteren Aufzählung von Einzelfällen eines Schadens steht, unterstreicht die Bedeutung dieser Kategorie nach Maßgabe der Verordnung. Dass diese Einordnung in Erwägungsgrund 146, der sich – anders als die Erwägungsgründe 75 und 85 – auch der Überschrift nach explizit mit

dem Schadenersatz befasst, nicht noch einmal wiederholt wird, steht der Annahme einer hinreichend deutlichen Positionierung des Verordnungsgebers zu dieser Rechtsfrage nicht entgegen. Denn Erwägungsgrund 146 zählt auch die übrigen Fallbeispiele aus den Gründen 75 und 85 gerade nicht noch einmal auf, sondern wählt in Satz 3 einen generalisierend-abstrakten Ansatz, wenn es dort heißt, der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen der Verordnung in vollem Umfang entspricht. Dies wiederum kann nur so verstanden werden, dass die „Ziele der Verordnung", wie sich sich u.a. auch in den übrigen Erwägungsgründen ausdrücken, umfänglich in den Blick zu nehmen sind. Daher sind in Ermangelung erneuter oder ggf. gar abweichender Konkretisierung des Schadensbegriffs durch Beispiele in Erwägungsgrund 146 selbst gerade diejenigen Gründe auszuwerten, die solche Konkretisierungen enthalten (ähnlich i.E. *Hellgardt*, ZEuP 2022, 7, 18, der meint, welche Arten von Nachteilen durch einen DSGVO-Verstoß „*dem Normgeber vor Augen standen*", werde in Erwägungsgrund. 85 S. 1 DSGVO „*konkretisiert*"). Die in Erwägungsgrund 146 enthaltene „Anweisung", den Schadensbegriff „weit" auszulegen, rechtfertigt die Heranziehung der in den Erwägungsgründen 75 und 85 enthaltenen, einer weiten Auslegung entsprechenden Einzelausprägungen wie u.a. Diskriminierung, Identitätsdiebstahl oder -betrug, Rufschädigung, Verlust der Vertraulichkeit des Berufsgeheimnisses oder eben des Kontrollverlusts über die Daten zusätzlich (entsprechend auch die Auslegung bei BeckOK DatenschutzR/*Quaas*, 44. Ed. 1.5.2023, DS-GVO Art. 82 Rn. 24). Ergänzend ist ferner zu beachten, dass der Verweis auf die „Ziele der Verordnung" in Erwägungsgrund 146 zwingt, auch Erwägungsgrund 7 einzubeziehen, der solche Ziele näher umschreibt. Darin wird als eines der wesentlichen Verordnungsziele definiert: „Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen." Auch dies bestärkt den Ansatz, schon den Kontrollverlust als Schaden anzusehen. Die Kontrolle über die eigenen personenbezogenen Daten wird damit als Ausdruck eines *persönlichkeitsrechtlich fundierten* Anspruchs hervorgehoben, zu jeder Zeit selbst entscheiden zu können, wem die Daten unter welchen Umständen zugänglich gemacht werden. Mit dieser Auslegung werden im Übrigen die Unterschiede zwischen einem bloßen Verstoß gegen die DSGVO und einem daraus hervorgehenden Schaden nicht nivelliert. Denn es sind zahlreiche Verstöße gegen auf die Datenverarbeitung bezogene Vorschriften der DSGVO denkbar, die nicht bzw. noch nicht zu einem konkreten, nicht wieder rückgängig zu machenden „Kontrollverlust" geführt haben. Schließlich ist in teleologischer

Auslegung zu beachten, dass der Kontrollverlust über personenbezogene Daten einen nicht zu unterschätzendem Nachteil für Betroffene mit sich bringt. Schon begrifflich bedeutet „Kontrollverlust“, dass die Daten sich in einem Maße von der berechtigten Person „entfernt“ haben, dass sie nicht mehr bestimmen kann, wer bei welcher Gelegenheit diese zur Kenntnis nehmen und für weitere Zwecke verwerten kann. Genau dies ist hier der Fall, da hinsichtlich der „geleakten“ Datensätze anzunehmen ist, dass jeder Betrachter die Leak-Inhalte kopieren konnte, sodass eine Rückgängigmachung der Verlustfolgen gar nicht möglich ist. Der Kontrollverlust *per se* stellt damit in Ansehung der Ziele der Verordnung einen ernst zu nehmenden, verordnungsrechtlich relevanten Nachteil dar, was seine Einordnung als „Schaden“ auch teleologisch rechtfertigt.

(b) Ist der Kontrollverlust über die Daten damit dem Grunde nach als Schaden einzuordnen, kommt nicht in Betracht, den Sachverhalt nunmehr noch einer Prüfung anhand einer „Erheblichkeitsschwelle“ zu unterziehen. Weil der Begriff des Schadens in Art. 82 DSGVO ein autonom-europarechtlicher ist, darf im Besonderen nicht auf nationale Erheblichkeitsschwellen oder andere Einschränkungen rekurriert werden (EuGH, Urteil vom 4.5.2023 – C – 300/21 (U I / Österreichische Post AG, NJW 2023, 1930, 1932 f., beck-online; Kühling/Buchner/*Bergt*, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18a). Es ist daher z.B. nicht zu verlangen, dass es durch den Datenrechtsverstoß etwa zu einer ernsthaften Beeinträchtigung für das Selbstbild oder Ansehen einer Person kommt (zutreffend Kühling/Buchner/*Bergt*, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18a). Der Gegenauffassung, die eine solche Erheblichkeitsschwelle implementieren wollte, und u.a. meinte, der Datenverlust stelle ohne ernsthafte Beeinträchtigung für das Selbstbild oder Ansehen einer Person ggf. lediglich einen unbeachtlichen Bagatellschaden dar (so OLG Dresden Hinweisbeschluss v. 11.6.2019 – 4 U 760/19, BeckRS 2019, 12941 Rn. 13), ist der Boden entzogen, seit der EuGH im Urteil vom 04.05.2023 (a.a.O.; Vorlage des OGH Österreich ZD 2021, 631) entschieden hat, dass keine Erheblichkeitsschwelle überschritten werden muss. Damit verbindet sich zudem, dass über den Kontrollverlust hinausreichende spezifische Angaben, wie konkret sich der Kontrollverlust auf die Persönlichkeit und auf das Leben der betroffenen Person ausgewirkt hat, *per se* nicht erforderlich sind; derartige weitergehende Umstände mögen den immateriellen Schaden vertiefen, sind aber in Annahme der eigenständigen Bedeutung der Kontrolle über schützenswerte personenbezogene Daten für den Schadensbegriff nicht

konstitutiv (i.E. zutreffend Kühling/Buchner/*Bergt*, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18b).

e) Die haftungsausfüllende Kausalität ist ebenfalls gegeben.

Dem Sachvortrag des Klägers zu den Pflichtverstößen der Beklagten einerseits und dem Schaden andererseits ist (in interessengerechter Auslegung des Vortrags, §§ 133, 157 BGB analog) ohne Weiteres zu entnehmen, dass auch eine Kausalität behauptet wird, nämlich dahingehend, dass die Klägerseite namentlich bei zutreffender Information und Aufklärung nach Maßgabe von Art. 13 DSGVO bzw. bei Kenntnis der unzureichenden Sicherungsmaßnahmen und der Funktionsweise des CIT sich mit der Suchbarkeit in Bezug auf die Telefonnummer nicht einverstanden erklärt und diese Funktion ggf. deaktiviert hätte.

f) Vorliegend ist ein Betrag in Höhe von 500,- € als immaterieller Schadensersatz angemessen.

aa) Über den – bereits bejahten – Kontrollverlust hinsichtlich der personenbezogenen Daten hinaus, sind hierbei *weitergehende Nachteile* auf Seiten des Klägers zu berücksichtigen: Der Kläger hat im Rahmen der persönlichen Anhörung im Termin vom 4.7.2023 gut nachvollziehbar und glaubhaft angegeben, dass es eine Zeit lang viele Anrufe und SMS-Nachrichten gegeben habe. U.a. habe er Nachrichten von der (angeblichen) BW-Bank mit einem entsprechenden Link bekommen, den er angeklickt habe, bevor er bemerkt habe, auf einen Betrug hereingefallen zu sein. Dieser Umstand deckt sich mit den Angaben Geschädigter aus Parallelverfahren, die ähnliche Nachrichten vermeintlicher Banken bekommen haben. Unter den Anrufen sei auch ein solcher von „Interpol“ gewesen, was sich wiederum mit Erkenntnissen aus Parallelverfahren deckt. Der Kläger gab ferner an, entsprechende Anrufe vor dem „Daten-Leak“ nicht erhalten zu haben; bei den SMS sei er sich diesbezüglich nicht so sicher und könne den Zugang von Spam-Nachrichten auch zu einem früheren Zeitpunkt nicht ausschließen.

Soweit die Beklagte bestritten hat, dass der Kläger Spam-Anrufe und Spam-SMS bekommen habe, ist dies zur Überzeugung der Kammer nachgewiesen durch die glaubhaften Angaben des persönlich angehörten Klägers. Denn der Kläger war bei seiner Anhörung ersichtlich um eine realitätsbasierte Schilderung bemüht, indem er jeweils Details zu den Anrufen und SMS-Anrufen angab, nichts dramatisierte und auch

Umstände einräumte, die seiner Position potentiell nicht förderlich waren (u.a. hätten ihn die SMS – anders als die Anrufe – „nicht so genervt“). Dass der Kläger sich die im Einzelnen doch sehr spezifischen Inhalte jeweils ausgedacht haben könnte, hält die Kammer nach Abwägung sämtlicher Umstände für fernliegend.

Aufgrund der zeitlichen Abläufe sowie inhaltlich äußerst ähnlicher Nachrichten in Parallelverfahren wiederum in engem zeitlichen Zusammenhang mit dem Datenleck ist für die Kammer nach dem Beweismaß des § 287 ZPO zudem auch überwiegend wahrscheinlich, dass jedenfalls die klägerseits angeführten Anrufe ursächlich auf das streitgegenständliche Datenleck zurückzuführen sind.

bb) Bei der Bemessung des Schmerzensgeldes hat die Kammer im Rahmen ihres durch § 287 ZPO eingeräumten Ermessens ein Schmerzensgeld von 500,00 € für erforderlich, aber auch ausreichend erachtet.

Die Kammer hat sich für die Bemessung an den Grundsätzen des § 253 BGB sowie den Kriterien des Art. 83 Abs. 2 DSGVO orientiert. Darunter zählen u. a. die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung, der Grad des Verschuldens, Maßnahmen zur Minderung des entstandenen Schadens, frühere Verstöße sowie die Kategorien der betroffenen personenbezogenen Daten und die betroffenen Kategorien personenbezogener Daten zur Ermittlung (LG Lübeck, CR 2023, 442, 449 mit Verweis auf Quaas in BeckOK/DatenschutzR DS-GVO Art. 82 Rz. 31-36).

Gemäß den Ausführungen unter dem vorigen Punkt aa) hat die Kammer berücksichtigt, dass der Kläger durch den Verlust der Kontrolle seiner Daten und deren freier Verfügbarkeit im Internet belastet ist. Damit steht in Einklang, dass es sich auch objektiv insoweit um einen schweren Verstoß handelt, als dass es sich bei der Telefonnummer in Verknüpfung mit einem Klarnamen um sensible Daten handelt, die geeignet sind, eine Bekanntheit vorzuspiegeln, was erhebliches Missbrauchsrisiko mit sich bringt. Dies gilt umso mehr, wenn weitere Daten verknüpft werden können. Zu berücksichtigen ist ferner, dass die Beklagte mehrere Verstöße gegen die DSGVO begangen hat. Diese Umstände sprechen für ein höheres Schmerzensgeld.

Das Gericht verkennt dabei nicht, dass sämtliche Daten des Klägers - mit Ausnahme der Mobiltelefonnummer - ohnehin für Dritte öffentlich einsehbar und damit beliebig kopierbar, weiterverwendbar und missbrauchbar gewesen sind. Maßgeblicher

Anknüpfungspunkt für das Schmerzensgeld ist demgemäß nicht eine Beeinträchtigung der Kontrolle über allein diese Daten (der Kontrolle hatte sich der Kläger insoweit bereits freiwillig begeben), sondern die Beeinträchtigung der Kontrolle über die Möglichkeit der Verknüpfung der Daten. Hierfür ist es ohne Belang, dass die Mobiltelefonnummer nicht von der Beklagten "gestellt", sondern von den Unbekannten per Zufallsgenerator "erraten" worden ist. Denn die Beklagte hat die Nummer jedenfalls validiert (so auch: LG Bonn, Urteil vom 7. Juni 2023 – 13 O 126/22 –, Rn. 73 juris).

Schmerzensgeldmindernd ist zu berücksichtigen, dass es sich um Daten aus der - grundsätzlich am wenigsten schutzwürdigen - Sozialsphäre des Klägers nach der Rechtsprechung des Bundesverfassungsgerichts zum allgemeinen Persönlichkeitsrecht handelt. Weiter ist zu berücksichtigen, dass sich der Kläger seiner Daten in Kenntnis des Geschäftsmodells der Beklagten freiwillig begeben hat, wenn auch nicht zu dem Zweck der streitgegenständlichen Verarbeitung (vgl. LG Bonn, aaO, Rn. 74, juris). Ferner war zu berücksichtigen, dass die Beklagte lediglich fahrlässig gehandelt hat und selbst Opfer eines Datendiebstahls durch kriminell handelnde Dritte wurde.

Bei der Bemessung der Schadensersatzhöhe hat die Kammer daneben auch die gesetzgeberisch beabsichtigte abschreckende Wirkung des Schadensersatzes berücksichtigt. Andererseits war aber auch zu berücksichtigen, dass das Allgemeininteresse im Schwerpunkt nach Art. 83 DSGVO durch die Verhängung von Bußgeldern gewahrt wird.

II. Der Kläger hat daneben den beantragten Zinsanspruch gegen die Beklagte.

Dieser ergibt sich aus den §§ 291, 288 Abs. 1, 187 Abs. 1 (entspr.; vgl. BGH, Urteil vom 10.10.2017 – XI ZR 555/16 –, Rn. 21, juris) BGB, §§ 253 Abs. 1, 261 Abs. 1 ZPO ab dem auf die Zustellung der Klageschrift folgenden Tag.

III. Die Klage ist auch hinsichtlich des Antrages zu Ziffer 2) (Feststellungsantrag) begründet.

1) Die Kammer verkennt dabei nicht, dass in einem Teil der Rechtsprechung in vergleichbaren Fällen die Feststellungsansprüche verneint werden mit dem Argument, der Anspruch setze eine gewisse Wahrscheinlichkeit für einen weitergehenden Schaden voraus und dies sei in Fällen dieser Art zu verneinen. Die Veröffentlichung der

— eher wenig sensiblen — Daten sei bereits Anfang April 2021 erfolgt. Dies liege nunmehr mehr als 2 Jahre zurück. Seitdem seien gerade keine materiellen Schäden eingetreten. Bei einer Verbreitung der Daten von ca. 533 Millionen Facebook-Nutzern verliere sich der klägerische Datensatz gleichsam in der Menge. Rückschlüsse etwa auf das Vermögen oder eine besondere Bereitschaft, sich auf bestimmte Geschäfte am Telefon überhaupt einzulassen, seien für die Klägerseite nicht ersichtlich.

2) Andere Teile der Rechtsprechung halten den Feststellungsantrag demgegenüber für begründet:

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

Diese Auffassung hat u.a. das LG Lüneburg näher wie folgt begründet:

> *„Es bedarf im Rahmen der Begründetheit – entgegen der Auffassung der Beklagten – keiner darüberhinausgehender gewissen Wahrscheinlichkeit des Schadenseintritts. An der Erforderlichkeit eines solchen zusätzlichen Begründungselements hat der BGH – jedenfalls für den Fall, dass Gegenstand der Feststellungsklage ein befürchteter Folgeschaden aus der Verletzung eines deliktsrechtlich geschützten absoluten Rechtsguts ist – Zweifel geäußert (vgl. BGH, Urteil vom 16.01.2001 – VI ZR 381/99, VersR 2001, 874). Streitgegenständlich sind die nicht von den Bestimmungen der DS-GVO gedeckten Übermittlungen oder Verarbeitungen personenbezogener Daten, welche eine Verletzung des allgemeinen Persönlichkeitsrechts als sonstiges Recht im Sinne des § 823 Abs. 1 BGB darstellen können (siehe dazu bereits unter I. 2. b). Die erkennende Kammer schließt sich diesbezüglich der vom Bundesgerichtshof vertretenen Ansicht ausdrücklich an. Demnach reicht vorliegend bereits die Möglichkeit eines Schadens aus. Es liegen, wie dargelegt, die Voraussetzungen des Schadensersatzanspruches aus Art. 82 Abs. 1 DS-GVO vor. Auch die Möglichkeit künftiger materieller Schäden ist zu bejahen. Diese Möglichkeit folgt – wie bereits angeführt – daraus, dass nicht absehbar ist, welche Dritte möglicherweise Zugriff auf die Daten erhalten haben und für welche kriminellen Zwecke diese*

möglicherweise missbraucht werden. Es erscheint eben nicht von vorneherein ausgeschlossen, dass die klagende Partei z.B. betrügerische Anrufe erhält, welche sich durch Ausgabe als Bankmitarbeiter Zugriff zu sensiblen Kontodaten der klagenden Partei erschleichen." (LG Lüneburg Urt. v. 24.1.2023 – 3 O 74/22, GRUR-RS 2023, 4813 Rn. 58)

3) Jedenfalls für die Fälle, in denen es – wie vorliegend – um die Verletzung eines deliktsrechtlich geschützten absoluten Rechtsguts, hier um die Verletzung des Datenschutzes als Ausprägung des Allgemeinen Persönlichkeitsrechts, geht, schließt sich die Kammer der zweitgenannten Auffassung mit der vorstehend zitierten Argumentation an (vgl. auch BGH, Urteil vom 17.10.2017 – VI ZR 423/16, juris Rn. 49; OLG Celle, ZfSch 2022, 558, 567).

4) Die Kammer hat den Klagantrag sachgerecht dahingehend ausgelegt und entsprechend tenoriert, dass anstelle der Formulierung *„der nach Aussage der Beklagten im Jahr 2019 erfolgte"* der – unstreitige - Zeitraum des Scraping-Vorfalls „Januar 2018 bis September 2019" gemeint war.

IV. Der Klagantrag zu Ziffer 3 (Unterlassung) ist teilweise begründet.

Die Beklagte hat gegen Art. 13 und Art. 25 Abs. 1 und 2 DSGVO verstoßen. Diese Rechtsverstöße geben dem Kläger dem Grunde nach einen darauf bezogenen Anspruch auf Beseitigung und künftige Unterlassung.###

1) Zum mit dem Antrag zu 3.a) geltend gemachten Anspruch werden unterschiedliche Auffassungen vertreten:

a) Nach einer Ansicht kann der Facebook-Nutzer verlangen, dass die Beklagte es unterlässt, personenbezogenen Daten (Telefonnummer, Facebook-ID, Familienname, Vorname, Geschlecht, Stadt, Beziehungsstatus) unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen.

b) Nach anderer Ansicht sind Unterlassungsansprüche im Geltungsbereich der DSGVO ganz abzulehnen:

„Ein Anspruch scheitert bereits an der Sperrwirkung der DS-GVO. Die DS-GVO sieht individualrechtliche Ansprüche in Art. 17 mit einem Löschungsanspruch und in Art. 82 mit einem Schadensersatzanspruch sowie in Art. 77 und 78 mit

Ansprüchen gegen Aufsichtsbehörden vor, nicht aber einen Unterlassungsanspruch gegen den sog. Auftragsverarbeiter oder Verantwortlichen bei einem Datenschutzrechtsverstoß. Zugleich ist die DS-GVO angesichts des Anwendungsvorrangs des hierdurch unionsweit vereinheitlichten Datenschutzrechts als abschließend anzusehen (vgl. BGH, Urteil vom 3. Mai 2022 – VI ZR 832/20 –, Rn. 10, juris zum Auslistungsbegehren nach Art. 17 DS-GVO). Die klagende Partei kann ihren Anspruch nicht auf sonstige Vorschriften des nationalen deutschen Rechts stützen (vgl. aaO; LG Wiesbaden, Urteil vom 20. Januar 2022 – 10 O 14/21 –, Rn. 39, juris). Wie Art. 17 enthält auch Art. 32 DS-GVO, der die Sicherheit der Verarbeitung regelt, eine ausdifferenzierte Güterabwägung und unbestimmte Rechtsbegriffe wie „nach dem Stand der Technik mögliche Sicherheitsmaßnahmen“ und „ein dem Risiko angemessenes Schutzniveau“, deren Prüfung nicht sinnvoll in das Vollstreckungsverfahren verlagert werden kann und nicht durch einen hiervon abweichenden Unterlassungsanspruch unterlaufen werden darf. Das Recht jeder betroffenen Person auf einen wirksamen gerichtlichen Rechtsbehelf nach Art. 79 Abs. 1 DS-GVO bezieht sich ausdrücklich nur auf die ihr aufgrund der DS-GVO zustehenden Rechte.“ (LG Lüneburg Urt. v. 24.1.2023 – 3 O 74/22, GRUR-RS 2023, 4813 Rn. 60)

c) Schließlich wird noch vertreten, dass der Anspruch jedenfalls an der fehlenden Wiederholungsgefahr scheitern müsse:

„Voraussetzung eines jeden vorbeugenden Unterlassungsanspruch ist die Wiederholungsgefahr (vgl. BGH, Urteil vom 19. Oktober 2004 – VI ZR 292/03 –, Rn. 17, juris, m.w.N.), an der es vorliegend fehlt. Zwar begründet eine vorausgegangene, rechtswidrige Beeinträchtigung (Erstbegehung) eine tatsächliche Vermutung für die Wiederholungsgefahr, an deren Widerlegung hohe Anforderungen zu stellen sind (vgl. BGH, Urteil vom 30. Oktober 1998 – V ZR 64/98 –, BGHZ 140, 1-11, Rn. 20). Vorliegend kann die Wiederholungsgefahr aber vollständig dadurch abgewendet werden, dass die klagende Partei die Suchbarkeit ihrer Telefonnummer auf der streitgegenständlichen Plattform der Beklagten auf „privat“ einstellt. Wie oben (unter 1.) ausgeführt, liegt der von der klagenden Partei gerügte und festgestellte Verstoß gegen die DS-GVO durch die Beklagte allein darin, dass es Dritten möglich war, die Telefonnummer der klagenden Partei mit den auf ihrem Profil ohnehin öffentlich zugänglichen Daten durch einen Missbrauch

des Kontakt-Importer-Tools zu verknüpfen, weil die Suchbarkeit der Telefonnummer auf „für alle“ voreingestellt war bzw. die Beklagte hierüber nicht hinreichend informiert hat. Darin kann, wie die klagende Partei selbst vorträgt, nur dann ein Verstoß gegen die Datenschutzrechte gesehen werden, wenn die klagende Partei bei hinreichender Information bzw. anderer Voreinstellung ihre Telefonnummer (auch) hinsichtlich der Suchbarkeit auf „privat“ gestellt hätte bzw. nach Kenntnis von dem datenschutzrechtlichen Vorfall auf „privat“ stellt. Ob sie das vorliegend tatsächlich getan hat oder nicht, ist unerheblich, denn entweder hat sie damit die Wiederholungsgefahr ausgeräumt oder aber sie verstößt gegen den Grundsatz von Treu und Glauben nach § 242 BGB, indem sie sich selbst in einen unauflösbaren Selbstwiderspruch setzt. Eine Rechtsausübung kann dann unzulässig sein, wenn sich objektiv das Gesamtbild eines widersprüchlichen Verhaltens ergibt, weil das frühere Verhalten mit dem späteren sachlich unvereinbar ist und die Interessen der Gegenpartei im Hinblick hierauf vorrangig schutzwürdig erscheinen (vgl. BGH, Urteil vom 15. November 2012 – IX ZR 103/11 –, Rn. 12, juris). Diese engen Voraussetzungen sind vorliegend gegeben. Die klagende Partei kann nämlich nicht einerseits einen Verstoß gegen Art. 25 Abs. 1 u. 2 DS-GVO daraus herleiten, dass sie bei zutreffender Information bzw. richtiger Voreinstellung die Suchbarkeit der Telefonnummer auf „privat“ gestellt hätte, andererseits aber nach entsprechender Kenntnis hierüber die Suchbarkeit auf „für alle“ belassen, obwohl ihr die Umstellung aufgrund der entsprechenden Kenntnis hierüber unproblematisch möglich wäre, und dann darauf einen vorbeugenden Unterlassungsanspruch stützen.“ (so die Alternativbegründung bei LG Lüneburg Urt. v. 24.1.2023 – 3 O 74/22, GRUR-RS 2023, 4813 Rn. 63)

d) Die Auffassung, einen Unterlassungsanspruch gänzlich abzulehnen, überzeugt aus Sicht der Kammer nicht.

aa) Jedenfalls bestimmte Unterlassungsansprüche lassen sich unmittelbar auf Art. 17 DSGVO stützen.

„Allerdings kann sich aus Art. 17 DSGVO über den Wortlaut hinaus auch ein Anspruch auf Unterlassung ergeben. Zwar wird in Art. 17 DSGVO nur ein Löschungsrecht normiert; aus diesem iVm Art. 79 DSGVO, der wirksame gerichtliche Rechtsbehelfe bei einer Verletzung der Datenschutzgrundverordnung garantiert, kann jedoch zugleich ein Unterlassungsanspruch hergeleitet werden

(vgl. BGHZ 231, 264 = GRUR 2022, 258 Rn. 10 – Ärztebewertung V; BSGE 127, 181 Rn. 13). Denn aus der Verpflichtung zur Löschung von Daten ergibt sich implizit zugleich die Verpflichtung, diese künftig nicht (wieder) zu speichern. So sieht der BGH in der erstgenannten Entscheidung vom 12.10.2021 im Löschungsanspruch des Art. 17 DSGVO zugleich einen Unterlassungsanspruch (BGHZ 231, 264 = GRUR 2022, 258 Rn. 10 u. 23).

Dieser aus der inneren Logik des Anspruchs auf Löschung hergeleitete Unterlassungsanspruch richtet sich jedoch nur auf die Unterlassung der Speicherung von Daten. Das Gegenstück der Löschung von Daten ist die Speicherung von Daten. Denn unter Löschen versteht man die Unkenntlichmachung gespeicherter Informationen, so dass es niemand mehr ohne unverhältnismäßigen Aufwand möglich ist, die Information wahrzunehmen (vgl. etwa Kühling/Buchner, 3. Aufl., DSGVO Art. 17 Rn. 37). Der Kl. verlangt hier nicht die Unterlassung der Speicherung von Daten über ihn durch die Bekl., sondern die Unterlassung der Übermittlung von Daten durch die Bekl. an Dritte. Wie insbesondere die Definition der Datenverarbeitung in Art. 4 Nr. 1 DSGVO und die Überschriften der Art. 44 bis 46 DSGVO zeigen, unterscheidet die DSGVO klar zwischen der Speicherung von Daten und der Übermittlung von Daten (an Dritte).“
(so OLG Frankfurt, GRUR 2023, 904 Rn. 44, 45).

Die Kammer folgt insoweit der vorgenannten auch höchstrichterlichen Rechtsprechung, dass die betroffene Person nach Art. 17 Abs. 1 DSGVO unter bestimmten Voraussetzungen von dem Verantwortlichen nicht nur verlangen kann, dass sie betreffende personenbezogene Daten unverzüglich löscht, sondern auch Unterlassungsansprüche bestehen. So definiert DSGVO nicht, was unter Löschung zu verstehen ist. Danach lässt sich aus dem in Art. 17 Abs. 1 DSGVO normierten Recht betroffener Personen, unter gewissen Umständen vom Verantwortlichen zu verlangen, sie betreffende personenbezogene Daten unverzüglich zu löschen, auch ein Anspruch auf Unterlassung ihrer Speicherung und Verarbeitung für die Zukunft ableiten (Argumentum a maiore ad minus). Dies folgt grundsätzlich auch aus Art. 79 DSGVO, der der betroffenen Person einen „wirksamen gerichtlichen Rechtsbehelf“ zugesteht (LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 143, beck-online). Der Kläger kann von der Beklagten mithin auch in der vorliegenden Konstellation die begehrte Unterlassung verlangen. Soweit das OLG Frankfurt einen Unterlassungsanspruch im Falle der Datenübermittlung an in im Ausland befindliche

Dritte ablehnt (aaO, Rn. 53), ist eine solche Übermittlung im vorliegenden Fall nicht streitgegenständlich. Vorliegend geht es dem Kläger um die Speicherung seiner Daten bei der Beklagten, nicht um eine Übermittlung an Dritte. Diese Speicherung soll nicht ohne Sicherungsmaßnahmen erfolgen. Es geht somit um eine qualitative Einschränkung der Speicherung als ein Weniger gegenüber einer Löschung.

bb) Wollte man die Anwendung des Art. 17 DSGVO nach dem vorgenannten Argument *a maiore ad minus* auf Unterlassungsansprüche ablehnen, wären nach zutreffender Ansicht die §§ 1004, 823 BGB im Geltungsbereich der DSGVO in der vorliegenden Konstellation anwendbar:

> *„Daneben sind nach richtiger und wohl herrschender Auffassung auch Beseitigungs- und bei Wiederholungsgefahr die allgemeinen Unterlassungsansprüche gem. § 1004 BGB (Übersicht zum Streitstand Halder/Walker ZD 2020, 605), bei einem Eingriff in das Persönlichkeitsrecht analog §§ 823 Abs. 2, 1004 BGB anwendbar. Unterlassungsansprüche sind in der DS-GVO nicht geregelt. In Literatur und Rechtsprechung ist umstritten, ob der DS-GVO insoweit eine Sperrwirkung zukommt. Eine Sperrwirkung würde jedoch dem allgemeinen Ziel der DS-GVO eines effektiven Rechtschutzes entgegenstehen.*
>
> *Zum Teil wird eine Anwendbarkeit des § 1004 BGB mit der Argumentation verneint, die DS-GVO habe abschließende Wirkung. So stützen sich das VG Regensburg (ZD 2020, 601) sowie LG Wiesbaden (ZD 2022, 238) auf Art. 79 Abs. 1 DS-GVO, der weitere gerichtliche Rechtsbehelfe ausschließe. Die DS-GVO sei im Zweifel restriktiv auszulegen (LG Wiesbaden ZD 2022, 238), nationale Unterlassungsansprüche würden gegen Unionsrecht verstoßen. Eine umfassende Harmonisierung der DS-GVO wird selbst vom Generalanwalt bezweifelt (vgl. Schlussanträge des Generalanwalts im Verfahren facebook ./. vzbv, GRUR-RS 2021, 36943). Die DS-GVO bezweckt jedoch grundsätzlich einen umfassenden Schutz hinsichtlich der Verarbeitung personenbezogener Daten von natürlichen Personen. Eine Sperrwirkung würde diesem Ziel entgegenstehen (OLG Dresden ZD 2022, 235) und der Schutz des Persönlichkeitsrechts nur außerhalb der DS-GVO gewährleistet. Zudem sind auch außerhalb des Kapitels III der DS-GVO wie eben in § 82 DS-GVO subjektive Rechte vorgesehen (Halder ZD 2020, 601 (605)).*
>
> *Der Bundesgerichtshof hat jedenfalls ein nationales Löschungsrecht neben Art. 17 DS-GVO wegen des Anwendungsvorrangs des „vorliegend unionsweit*

abschließend vereinheitlichten Datenschutzrechts“ abgelehnt. Diese Rechtsprechung kann nicht auf die Frage des Unterlassungsanspruchs übertragen werden, da anders als der Löschungsanspruch ein Unterlassungsanspruch in der DS-GVO gerade nicht geregelt ist.“

(BeckOK DatenschutzR/*Quaas*, 44. Ed. 1.5.2023, DS-GVO Art. 82 Rn. 9-9.2)

Diese Argumentation hält die Kammer für überzeugend. Der Anspruch auf Harmonisierung kann nur so weit reichen, wie der konkrete Regelungsplan des Unionsgesetzgebers reichte. Würden Unterlassungsansprüche durch Art. 17 DSGVO nicht erfasst, läge eine Intention, das Schutzniveau durch eine auch in Bezug auf Unterlassungsansprüche abschließende – und diese somit ausschließende – Regelung unter die jeweiligen nationalen Niveaus abzusenken, jedenfalls fern.

Dies entspricht auch der Rechtsprechung des OLG Dresden, der sich die Kammer nach eigener Überzeugung insoweit anschließt. Die Geltendmachung eines Anspruchs auf Unterlassung aus §§ 823 Abs. 1 i.V.m. 1004 BGB ist neben den Rechten aus der Datenschutzgrundverordnung möglich, wenn nur so ein lückenloser Schutz hinsichtlich der Verarbeitung personenbezogener Daten von natürlichen Personen gewährleistet werden kann (OLG Dresden, Urteil vom 14. Dezember 2021 – 4 U 1278/21 –, Rn. 46, juris; ebenso Schaffland/Wiltfang, DS-GVO/BDSG, 8. Ergänzungslieferung 2023, Art. 17 EUV 2016/679, Rn. 5 f):

„Würde man einen solchen Unterlassungsanspruch verneinen, wäre kein ausreichender Individualrechtsschutz gegeben. Es ist daher nicht davon auszugehen, dass die Datenschutzgrundverordnung, weil sie keinen ausdrücklichen Unterlassungsanspruch enthält, eine Sperrwirkung entfaltet (so auch Landgericht Darmstadt, a.a.O.).“

Die Wiederholungsgefahr entfällt auch nicht deswegen, weil die klagende Partei die Möglichkeit hat, die Einstellungen hinsichtlich der Suchbarkeit der Telefonnummer für die Zukunft zu ändern (auf „privat“ umzustellen); denn die Möglichkeit zuzulassen, dass die betreffende Person nicht nur durch Eingabe einer spezifischen Telefonnummer aufzufinden ist, sondern gerade im Wege des „Suchlaufs“ unter Nutzung der technischen Möglichkeiten des CIT, weist einen eigenständigen Verletzungsgehalt auf, sodass auf dieser Grundlage ein Unterlassungsanspruch nicht zu verneinen ist. Die

Möglichkeit, Rechtsverletzungen durch eigene Handlungen vorzubeugen, lässt im Übrigen Unterlassungsansprüche nicht entfallen.

Ausgenommen von dem Anspruch sind indes die Daten „Land“ und „Bundesland“, die nicht Gegenstand der Angaben auf der Facebook-Plattform sind. Insoweit ist der Unterlassungsanspruch teilweise nicht begründet und daher abzuweisen (so auch LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 113 – 115).

2) Zu dem Antrag zu 3.b. wird vertreten, dass dieser Anspruch abzulehnen sei, weil die betreffende Pflichtverletzung für die Zukunft keine Folgen mehr auszulösen vermöge:

> *„Diese Pflichtverletzung löst aber für die Zukunft keine Folgen mehr aus, da der Kläger zumindest im Verlauf des Rechtsstreits sämtliche Informationen erhalten hat, die die fragliche Art und Weise der Datenverarbeitung betreffen.*
>
> *Unbeschadet des Umstands, dass die ursprünglich erteilten Informationen der Beklagten unübersichtlich und unvollständig gewesen sein mögen, ist ihm die begehrte Information, 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 G-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird“ schon ausweislich seiner Antragstellung bekannt, ohne die Nutzung von G eingestellt zu haben. Damit verhält sich der Kläger in sich widersprüchlich und verstößt gegen die Grundsätze von Treu und Glauben. Denn die geforderte Information, von der er die weitere Datenverarbeitung abhängig machen will, hat er bereits. Überdies ist ihm zumindest anhand der Darstellungen in der Klageerwiderung auch ohne weiteres möglich, die Suchbarkeitsfunktion so zu ändern, dass er nur durch sich selbst aufgefunden werden kann.“* (LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 160, 161)

Diese Auffassung überzeugt aus Sicht der Kammer nicht. Wie gezeigt, begründet der Umstand, eine Vielzahl von Nutzerdaten über fingierte Telefonnummern unter Nutzung des CIT zu „scrapen“, einen eigenständigen Verletzungsgehalt. Da die Nutzung ein Dauerschuldverhältnis ist, müssen für die Zukunft auch vergleichbare Gefährdungen ausgeschlossen werden. Wenn der Anbieter also etwa ein „Reboot“ durchführt oder wesentliche Veränderungen in den Nutzungsoberflächen implementiert, wobei

wiederum neue Zustimmungen unter Verweis auf Datenschutzrichtlinien eingeholt werden müssen, muss der Nutzer jedenfalls dafür sicherstellen können, dass hinreichend über Funktionen, wie sie sich mit einem Kontaktimporttool verbinden, aufgeklärt wird. Andernfalls dürften die betreffenden Daten – namentlich die Telefonnummer – nicht verwertet werden.

3) Ordnungsmittel sind – wie beantragt – nach § 890 Abs. 2 ZPO anzudrohen.

V. Der Klagantrag zu Ziffer 4 (Auskunft) ist unbegründet.

Der Anspruch auf Auskunft gemäß Art. 15 des DSGVO ist auf Grundlage der Informationen in dem Schreiben Anlage K2 durch Erfüllung untergegangen (§ 362 BGB) und, bzw. besteht, soweit er darüber hinaus geht, von vornherein nicht.

Insofern ist dem Landgericht Essen in seiner Argumentation zu folgen, welches ausgeführt hat:

> *„Schließich hat die Beklagte nicht gegen Art. 15 DSGVO verstoßen, indem sie dem Kläger keine bzw. unvollständige Auskünfte erteilt hat. Der Anspruch auf Auskunftserteilung ergibt sich aus Art 15 Abs. 1 a), c) DSGVO. Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein 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. Da das Schreiben der Beklagten Nutzer ID, Vorname, Nachname, Land und Geschlecht enthält, ist der Anspruch insoweit erfüllt und erloschen (§ 362 Abs. 1 BGB). Nicht beantwortet wird durch die Beklagte in dem außergerichtlichen Schreiben, 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 nicht erkennbar, wer diese Daten gescrapt hat. Die begehrte Auskunftserteilung ist aufgrund des Vorganges des Scrapings unter Ausnutzung von Daten, die auf „öffentlich“ gestellt sind, unmöglich. Ebenso ist im Rechtssinne unmöglich (und es wird auch nicht näher dargelegt, wie die Beklagte mitteilen können soll), zu informieren, wann die Daten*

gescrapt wurden. Der Kläger geht selbst von 2019 aus bzw. von der Veröffentlichung dann im April 2021. Dieser Zeitrahmen ist dem Kläger bekannt; eine genaue Eingrenzung in Bezug auf seine Daten ist nicht möglich. Die Beklagte hat dem Kläger im Ergebnis also alle Informationen mitgeteilt, die ihr im Zuge des Scraping-Vorfalls zur Verfügung standen. Weitere Angaben kann sie nicht machen. Sie ist folglich hierzu auch nicht verpflichtet." (LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 102, juris).

VI. Der Klagantrag zu Ziffer 5 (Anwaltskosten) ist im tenorierten Umfang begründet.

Dieser Anspruch ergibt sich unmittelbar aus Art. 82 Abs. 1 DSGVO (iVm § 249 Abs. 1 BGB) (vgl. OLG Frankfurt, NJW-RR 2022, 1608 Rn. 60). Dabei sind für den Streitwert als Grundlage der vorgerichtlichen Rechtsanwaltskosten auch der Unterlassungs- und der Auskunftsanspruch zu berücksichtigen, obwohl die Verzugsvoraussetzungen hierfür nicht gegeben waren. Die Kammer verkennt dabei nicht, dass vorgerichtliche Rechtsanwaltskosten regelmäßig nur im Verzugsfalle nach den §§ 280 Abs. 1, Abs. 3, 286 BGB gewährt werden (soweit es sich nicht um eine Schadensersatzposition handelt, die als adäquate Rechtsverfolgungskosten erstattungsfähig sind). Insbesondere wenn die betroffene Person zuvor korrekt nach Art. 13 Abs. 2 lit. b bzw. Art. 14 Abs. 2 lit. c DSGVO über das Bestehen des Auskunftsrechts unterrichtet wurde, besteht nach einer insoweit vertretenen Ansicht kein Grund, (jedenfalls) für den initialen Antrag auf Auskunftserteilung einen Rechtsanwalt einzuschalten (vgl. Gola/Heckmann/Franck, 3. Aufl. 2022, DS-GVO Art. 15 Rn. 70). Angesichts des Umstandes, dass es sich jedenfalls in technischer Hinsicht um eine komplizierte Materie handelte, war es vorliegend aus Sicht des Klägers erforderlich und angemessen, direkt einen Rechtsanwalt einzuschalten, ohne die Beklagte selbst vorher in Anspruch zu nehmen. Hierzu wird auch auf den Erwägungsgrund 146 zur DSGVO S. 6 *„Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten."* verwiesen (vgl. BeckOK DatenschutzR/Quaas, 44. Ed. 1.5.2023, DS-GVO Art. 82 Rn. 29-29.1).

Der Anspruch ist auch auf Zahlung, nicht bloß auf Freistellung nach § 257 S. 1 BGB gerichtet. Mit der Ausführung, die Klägerseite unterliege einem „grundlegenden Missverständnis" hinsichtlich des Vorliegens eines Datenschutzverstoßes in dem Schreiben Anlage K2 hat die Beklagtenseite zugleich auch eine Freistellung dem Grunde nach ernsthaft und endgültig verweigert. Diese Pflichtverletzung berechtigt die

klagende Partei, gemäß den §§ 249 Abs. 1 BGB, 250 S. 2 BGB statt der Freistellung Schadensersatz in Geld zu verlangen. Die an sich nach § 250 S. 1 BGB erforderliche Ablehnungsandrohung wird dabei durch die ernsthafte und endgültige Verweigerung (auch) der Freistellung entbehrlich gemacht (vgl. OLG Hamm 3.9.2013 – I-4 U 58/13, GRUR-RR 2014, 133; OLG Frankfurt, NJW-RR 2022, 1608 Rn. 60).

Der Anspruch berechnet sich entsprechend einer 1,3 Geschäftsgebühr aus dem Gegenstandswert der im Rahmen des hiesigen Verfahrens begründeten Ansprüche, die vorgerichtlich geltend gemacht wurden, sowie des vorgerichtlich teilweise berechtigten, aber erfüllten Auskunftsanspruchs:

- Schadensersatzanspruch in Höhe von 500,- € (Klageantrag zu 1);

- Unterlassungsanspruch zu einem Streitwert in Höhe von insgesamt 5.000,- € (Klageantrag zu 3); die insoweit vorgenommene Teil-Abweisung bezüglich der Daten „Land“ und „Bundesland“ ist in ihrem Wert so gering, dass sie für den Streitwert nicht ins Gewicht fällt, so dass es bei dem (vorprozessualen) Streitwert von 5.000,- € bleibt;

- der Auskunftsanspruch war vorgerichtlich geltend gemacht worden und beklagtenseits – soweit möglich – vorprozessual erfüllt worden; in der damals berechtigten Höhe (von der Kammer geschätzt: 300,- €) geht er in den Streitwert für die vorgerichtlichen Rechtsanwaltskosten ein;

- insgesamt: 6.300,- €.

Bei einer 1,3-fachen Geschäftsgebühr zzgl. 20,- € Kostenpauschale sowie 19% Umsatzsteuer ergibt sich ein Anspruch in Höhe von 713,76 €.

VII. Bezogen auf den Ersatzanspruch für die vorgerichtlichen Rechtsanwaltskosten besteht für den Kläger daneben ein Zinsanspruch aus den §§ 291, 288 Abs. 1, 187 Abs. 1 entspr. BGB, §§ 253 Abs. 1, 261 Abs. 1 ZPO ab dem auf die Zustellung der Klageschrift folgenden Tag (12.10.2022).

C. Die Kostenentscheidung beruht auf § 92 Abs. 1 ZPO.

Der Ausspruch zur vorläufigen Vollstreckbarkeit ergibt sich für die Vollstreckung des Klägers aus § 709 S. 1 und 2 ZPO, für die Vollstreckung der Beklagten aus den §§ 708 Nr. 11, 711, 709 S. 2 ZPO entsprechend.

D. Die Wertfestsetzung findet ihre Grundlage in § 3 ZPO, § 63 Abs. 2 Satz 1 GKG.

I. Für den festzusetzenden Streitwert war bezüglich des Klagantrags zu Ziffer 1) der von dem Kläger vorgestellte (Mindest-)Schadenersatzbetrag in Höhe von 1.000,- € anzusetzen.

II. Soweit der Kläger mit dem Klagantrag zu Ziffer 2) die Feststellung begehrt hat, dass die Beklagte verpflichtet ist, ihm (auch) alle künftigen Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten entstanden sind und/oder noch entstehen werden, so kommt diesem Antrag ein eigener wirtschaftlicher Wert zu. Dieser orientiert sich grundsätzlich an den Vorstellungen des Klägers zum Klagantrag zu 1), ist aber nur mit einem Bruchteil zu bemessen, wobei 50% und damit ein Betrag in Höhe von 500,- € angemessen erscheint (vgl. OLG Stuttgart, Beschluss vom 03.01.2023 – 4 AR 4/22 –, Rn. 23, juris).

III. Mit den Klageanträgen zu Ziffer 3.a) und b) hat der Kläger Unterlassung begehrt. Bei diesen nichtvermögensrechtlichen Anträgen ist es ihm darum gegangen, dass seine im Rahmen des Nutzungsverhältnisses mit der Beklagten angegebenen personenbezogenen Daten einschließlich der Telefonnummer künftig nicht in die Hände unbefugter Dritter gelangen, die diese dann ggf. für illegale Aktivitäten nutzen könnten. Der Kläger hat damit effektivere Sicherheitsvorkehrungen bei der Beklagten zu erreichen angestrebt.

Der Streitwert der Unterlassungsanträge ist als nichtvermögensrechtlicher Streitgegenstand anhand des betroffenen Interesses des Klägers unter Berücksichtigung der Umstände des Einzelfalls zu bestimmen (§ 48 Abs. 2 Satz 1 GKG). Dabei ist in Anlehnung an § 23 Abs. 3 Satz 2 RVG bei mangelnden genügenden Anhaltspunkten für ein höheres oder geringeres Interesse von einem Streitwert von 5.000,- € auszugehen und erscheint es unter Berücksichtigung aller Umstände des vorliegenden Einzelfalls angemessen, auf die Gedanken dieser allgemeinen Wertvorschrift zurückzugreifen (vgl. OLG Stuttgart, a.a.O., Rn. 26 f.). So darf bei der Bemessung des Streitwerts das Gesamtgefüge der Bewertung nichtvermögensrechtlicher Streitgegenstände nicht aus den Augen verloren werden

(vgl. BGH, Beschluss vom 26.11.2020, Az.: III ZR 124/20 – juris, Rn. 11), es erscheint unter Berücksichtigung aller Umstände des vorliegenden Einzelfalls (vgl. § 48 Abs. 2 Satz 1 GKG) hier angemessen, auf die Gedanken der allgemeinen Wertvorschrift des § 23 Abs. 3 Satz 2 RVG zurückzugreifen, und – auch mangels genügender Anhaltspunkte für ein höheres oder geringeres Interesse - angemessen, von einem Wert von 5.000,- € für das Unterlassungsbegehren in Summe auszugehen (vgl. OLG Stuttgart, a.a.O., Rn. 28).

IV. Dem Auskunftsanspruch zu Ziffer 4) ist daneben eine eher untergeordnete Bedeutung beizumessen (vgl. OLG Stuttgart, a.a.O., Rn. 29). Dessen Wert beläuft sich auf einen Betrag in Höhe von 500,- € (vgl. LG Osnabrück, Urteil vom 03.03.2023 – 11 O 834/22 –, Rn. 45, juris; LG Itzehoe, Urteil vom 27.02.2023 – 10 O 159/22 –, juris; LG Essen, Urteil vom 10.11.2022 – 6 O 111/22 –, Rn. 44, juris).

V. Insgesamt ergibt sich daraus ein Wert von 7.000,- €.

Rechtsbehelfsbelehrung

Diese Entscheidung kann hinsichtlich der Wertfestsetzung mit der Beschwerde angefochten werden. Sie ist nur zulässig, wenn sie innerhalb von sechs Monaten, nachdem die Entscheidung in der Hauptsache rechtskräftig geworden ist oder das Verfahren sich anderweitig erledigt hat, bei dem Landgericht Hannover, Volgersweg 65, 30175 Hannover, eingeht. Wird der Streitwert später als einen Monat vor Ablauf dieser Frist festgesetzt, kann die Beschwerde innerhalb eines Monats nach Zustellung oder formloser Mitteilung der Festsetzung bei dem Gericht eingelegt werden.
Die Beschwerde ist nur zulässig, wenn der Wert des Beschwerdegegenstandes 200,00 € übersteigt oder das Gericht die Beschwerde in diesem Beschluss zugelassen hat. Beschwerdeberechtigt ist, wer durch diese Entscheidung in seinen Rechten beeinträchtigt ist.

Die Beschwerde wird durch Einreichung einer Beschwerdeschrift oder zur Niederschrift der Geschäftsstelle des genannten Gerichts eingelegt. Sie kann auch zur Niederschrift der Geschäftsstelle eines jeden Amtsgerichts erklärt werden, wobei es für die Einhaltung der Frist auf den Eingang bei dem genannten Gericht ankommt. Sie ist zu unterzeichnen. Die Einlegung kann auch mittels elektronischen Dokuments erfolgen. Informationen zu den weiteren Voraussetzungen zur Signatur und Übermittlung sind auf dem Justizportal des Bundes und der Länder (www.justiz.de) im Themenbereich zur elektronischen Kommunikation zu finden. Eine Einlegung per einfacher E-Mail ist unzulässig. Rechtsanwältinnen, Rechtsanwälte, Behörden und juristische Personen des öffentlichen Rechts einschließlich der zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse sind zur Einlegung mittels elektronischen Dokuments verpflichtet.
Die Beschwerde muss die Bezeichnung des angefochtenen Beschlusses sowie die Erklärung enthalten, dass Beschwerde gegen diesen Beschluss eingelegt wird. Soll die Entscheidung nur zum Teil angefochten werden, so ist der Umfang der Anfechtung zu bezeichnen.

[redacted]
Vorsitzende Richterin am Landgericht

[redacted]
Richter am Landgericht

[redacted]
Richter am Landgericht

Beglaubigt
Hannover, 14.08.2023

[redacted], Justizangestellte
als Urkundsbeamtin der Geschäftsstelle