LG Kempten, Endurteil v. 23.06.2023 – 13 O 293/23

Titel:

Notwendigkeit der Darlegung eines konkreten Schadens bei Datenschutzverstößen

Normenkette:

DSGVO Art. 5 Abs. 1, Art. 15, Art. 24, Art. 25 Abs. 2, Art. 32, Art. 33, Art. 82

Leitsätze:

1. Zur Notwendigkeit der Darlegung eines konkreten Schadens bei Geltendmachung eines Schadensersatzanspruchs wegen Verstoßes gegen die DSGVO in einem Scraping-Fall bei einem sozialen Netzwerk. (Rn. 47 – 50) (redaktioneller Leitsatz)

2. Zu Verstößen gegen die DSGVO durch einen "Scraping"-Vorfall bei einem sozialen Netzwerk. (Rn. 31 – 46) (redaktioneller Leitsatz)

Schlagworte:

Schadensersatz, Schadensersatzanspruch, Verletzung, Unterlassungsanspruch, Streitwert, Technik, Ermessen, Daten, Software, Internet, Schaden, Form, Wiederholungsgefahr, Auskunft, personenbezogene Daten, Stand der Technik, Kosten des Rechtsstreits

Rechtsmittelinstanzen:

OLG München, Verfügung vom 14.09.2023 – 14 U 3190/23 e

OLG München, Berichtigungsbeschluss vom 12.10.2023 – 14 U 3190/23 e

OLG München, Beschluss vom 23.11.2023 – 14 U 3190/23

Fundstelle:

GRUR-RS 2023, 27346

Tenor

1. Die Klage wird abgewiesen.

2. Der Kläger hat die Kosten des Rechtsstreits zu tragen.

3. Das Urteil ist gegen Sicherheitsleistung in Höhe von 110% des jeweils zu vollstreckenden Betrags vorläufig vollstreckbar.

Beschluss

Der Streitwert wird auf 6.200,00 € festgesetzt.

Tatbestand

1

Der Kläger macht Ansprüche im Zusammenhang mit der Datenschutzgrundverordnung gegenüber der Beklagten geltend.

2

Der Kläger nutzte im streitgegenständlichen Zeitraum einen ...-Account, die Beklagte ist Betreiberin der ...-Plattform. Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Die Nutzer können auf den persönlichen Profilen Angaben zu verschiedenen Daten zu ihrer Person einstellen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können.

3

Im Zeitraum Januar 2018 bis September 2019 wurden durch unbekannte Dritte Telefonnummern, ...-ID, Name, Vorname, Geschlecht und weitere Daten über das Tool „Contact-Import“ – sofern öffentlich zugänglichen – abgeschöpft („Scraping“). Indem eine Vielzahl von Kontakten in ein virtuelles Adressbuch eingegeben wurde, gelang es Unbekannten, die Telefonnummern konkreten Profilen zuzuordnen, ohne dass in den entsprechenden Profilen die hinterlegten Telefonnummern öffentlich freigegeben waren. Um die

Telefonnummer jeweils zu korrelieren, wurden mit Hilfe eine Contact-Import-Tools Nummern geprüft, um zu sehen, ob diese mit einem ...-Account verbunden waren. Auf dem Profil des Nutzers wurde dieser dann besucht und von dort wurden die öffentlichen Daten gescrapt („abgeschöpft"). Anfang April 2021 wurde durch die Medien bzw Presse berichtet, dass Daten von ca. 533 Millionen Nutzern der Plattform der Beklagten aus 106 Ländern im Internet veröffentlicht wurden.

4
Beim Anlegen eines ...-Accounts wird der künftige Nutzer auf Datenschutz- und Cookie-Richtlinien hingewiesen. Diese sind durch eine Verlinkung getrennt abrufbar. Nach der Anmeldung sind zunächst die Vor- bzw. Standardeinstellungen aktiviert. Demnach können „alle" Personen sehen, welche Seiten der Nutzer abonniert oder mit wem er befreundet ist. Ebenso können „alle" den neuen Nutzer über seine E-Mail-Adresse „finden". Die Angabe der Mobilfunknummer ist nicht grundsätzlich zwingend. Wenn der Nutzer die Zweifaktor-Authentifizierung nutzen möchte, ist die Angabe einer Mobilfunknummer jedoch zwingend. Entscheidet sich ein Nutzer diese anzugeben, kann er in den Suchfunktionen einstellen, in welchem Umfang er über diese gefunden werden will. Der Nutzer kann die Einstellungen individuell verändern und im Hilfebereich einlesen, wie die Beklagte insbesondere die Mobilfunknummer verwendet.

5
Der Kläger trägt im Wesentlichen vor:

6
Die Beklagte habe gegen zahlreiche Vorschriften der Datenschutzgrundverordnung verstoßen. So liege ein Verstoß gegen Art. 4 Nr. 2 DSGVO vor, da Daten des Klägers ohne Rechtsgrundlage und ohne ausreichende Informationen verarbeitet worden seien. Ferner seien entgegen Artt. 5 ff. DSGVO Daten des Klägers unbefugt Dritten zugänglich gemacht worden. Auch lägen Verstöße gegen Artt. 15, 17 und 18 DSGVO vor. Im April 2021 seien Daten auch des Klägers im Internet veröffentlicht worden. Die Beklagte habe keine hinreichenden Sicherheitsvorkehrungen gegen einen unbefugten Zugriff Dritter getroffen. Ferner seien ihre Einstellungen bzgl. der Telefonnummer des Klägers so konzipiert, dass keine echte Sicherheit möglich sei.

7
Von dem Scraping Vorfall seien auch die Daten des Klägers betroffen. Dem Kläger sei durch die unbefugte Veröffentlichung seiner personenbezogenen Daten ein Schaden entstanden, der darin bestehe, dass der Kläger einen erheblichen Kontrollverlust über seine Daten erlitten habe und in einem Zustand großen Unwohlseins und Sorge über möglichen Missbrauch seiner Daten verbleibe. Der Kläger habe seit 2021 vermehrt dubiose E-Mails und SMS-Nachrichten von unbekannten Adressen und Nummern erhalten.

8
Der Kläger beantragt:

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

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

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

a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, ...ID, 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 ...-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.

9
Die Beklagte beantragt

Klageabweisung.

10
Die Beklagte ist der Auffassung, dass kein Verstoß gegen die DSGVO vorliege. Es sei Sache der Klagepartei, welche Daten bei der Beklagten hinterlegt werden und in welchem Umfang diese in den Einstellungen „öffentlich“ oder „privat“ gemacht werden. Es seien lediglich öffentlich einsehbare Daten durch Dritte in Form des Scraping abgerufen worden. Zudem sei unschlüssig und unsubstantiiert, welche Daten der Klagepartei genau gescrapt worden sein sollen.

11
Die Beklagte ist der Ansicht, nicht gegen Art. 24, 32 DSGVO verstoßen zu haben, sondern vielmehr angemessene technische und organisatorische Maßnahmen ergriffen zu haben, das Risiko von „Scraping“ zu unterbinden und Maßnahmen zur Bekämpfung von „Scraping“ zu ergreifen. Es fehle konkreter Vortrag, welche Maßnahmen in welchem Umfang nicht genügen würden. Außerdem müsse eine solche Beurteilung ex ante und nicht ex post erfolgen. Den Anforderungen des Art. 25 DSGVO sei genügt. Es dürfe dabei der zentrale Zweck von ..., mit Freunden, Familien und Gemeinschaften sich zu verbinden nicht außer Betracht bleiben. Es bestehe keine Melde- oder Benachrichtigungspflicht, da es an einer Verletzung der Sicherheit i. S. d. Art. 4 Nr. 12 DSGVO und an einer unbefugten Offenlegung von Daten fehle. Unabhängig davon habe sie – die Beklagte – wegen der Medienberichterstattung freiwillig eine Vielzahl von Maßnahmen ergriffen, über „Scraping“ und Begrenzungsmöglichkeiten einschließlich einer Änderung von Privatsphäre-Einstellungen zu informieren.

12
Es werde bestritten, dass die Klagepartei aufgrund des „Scraping-Vorfalls“ an den genannten Symptomen wie zum Beispiel Stress, Hilflosigkeit oder Gefühl des Beobachtenwerdens leide. Art. 82 DSGVO umfasse auch keine Verstöße gegen Art. 13-15, 24, 25 DSGVO. Mangels Verstoßes gegen die DSGVO sei der (ohnehin unzulässige) Feststellungsantrag unbegründet. Der Unterlassungsanspruch scheitere an einer Erstbegehungs- und einer Wiederholungsgefahr. Anwaltskosten seien mangels Verzuges unbegründet.

13
Das Gericht hat am 19.06.2023 mündlich zur Sache verhandelt und den Kläger informatorisch angehört. Es wird auf das Sitzungsprotokoll vom 19.06.2023 verwiesen.

14
Zur Ergänzung des Tatbestands wird auf das schriftsätzliche Vorbringen der Parteien nebst Anlagen Bezug genommen.

Entscheidungsgründe

15

Die Klage ist zulässig, jedoch unbegründet.

A. Zulässigkeit

16
I. Das Landgericht Kempten ist international, sachlich und örtlich zuständig.

17
Die deutsche Gerichtsbarkeit folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 2. Alt EuGVVO. Gemäß Art. 18 Abs. 1 2. Alt EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat. Der Kläger ist gemäß Art. 17 Abs. 1 EuGVVO unzweifelhaft Verbraucher. Der Kläger hat seinen Wohnort im Bezirk des Landgerichts Kempten .

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

19
Die sachliche Zuständigkeit ergibt sich aus § 39 ZPO.

20
II. Der Feststellungsantrag zu Ziffer 2 ist zulässig.

21
Ein Feststellungsantrag ist schon zulässig, wenn die Schadensentwicklung noch nicht abgeschlossen ist und der Kläger seinen Anspruch deshalb ganz oder teilweise nicht beziffern kann (vgl. OLG Hamm, Urteil vom 21. Mai 2019 – 9 U 56/18 –, Rn. 22, juris). Ein Feststellungsinteresse ist nur zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (vgl. BGH, Beschluss vom 09. Januar 2007 – VI ZR 133/06 –, juris; BGH, Urteil vom 16. Januar 2001 – VI ZR 381/99 –, juris; Saarländisches Oberlandesgericht Saarbrücken, Urteil vom 20. Februar 2014 – 4 U 411/12, Rn. 46, juris, m.w.N.).

22
Bei den behaupteten Verstößen gegen die DSGVO mit der behauptet dargelegten unkontrollierten Nutzung gescrapter Daten ist bei verständiger Würdigung zumindest nicht ausgeschlossen, dass irgendein materieller oder immaterieller Schaden entstehen könnte. Es ist nicht völlig ausgeschlossen, dass der Kläger infolge der Veröffentlichung seiner Telefonnummer in Verbindung mit seinem Namen sowie weiteren persönlichen Daten einen irgendwie gearteten Schaden erleidet.

B. Begründetheit

23
Die Klage ist unbegründet.

24
I. Der Klagepartei stehen keine Ansprüche auf Ersatz immateriellen Schadens aus § 82 Abs. 1 DSGVO zu (Klageantrag Ziff. 1).

25
1. Der Schutzbereich des Art. 82 DSGVO ist vorliegend hinsichtlich behaupteter Verstöße gegen Artt. 13, 14, 15, 24, 25 und Art. 34 DSGVO bereits nicht eröffnet.

26
a) Nach Art. 82 Abs. 1 DSGVO hat jede 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.

27

Gemäß Art. 2 DSGVO umfasst der sachliche Anwendungsbereich der DSGVO die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

28
Anknüpfungspunkt für eine Haftung ist also eine der Verordnung nicht entsprechende Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO. Dies steht im Einklang mit Erwägungsgrund 146, wonach der Verantwortliche oder der Auftragsverarbeiter Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit der DSGVO nicht im Einklang stehen, ersetzen sollte.

29
Gemäß Art. 4 Nr. 2 DSGVO ist Verarbeitung jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, durch den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

30
b) Die behauptete Verletzung von bloßen Benachrichtigungspflichten bzw. Informationsrechten ist unter Zugrundelegung dieses Maßstabs hingegen nicht erfasst (vgl. Landgericht Essen, Urteil vom 10. November 2022, Az. 6 O 111/22, GRUR-RS 2022, 34818; Amtsgericht Strausberg, BeckRS 2022, 27811; Landgericht Heilbronn, Urteil vom 13. Januar 2023, Az. Bu 8 O 131/22). Folglich sind mögliche Verstöße gegen Artt. 13, 14, 15, 24, 25 und Art. 34 DSGVO, die lediglich Informationspflichten begründen, nicht vom Schutzzweck der Norm erfasst.

31
2. Es fehlt darüber hinaus an entsprechenden Pflichtverstößen der Beklagten gegen Normen der DSGVO.

(1) Kein Verstoß gegen Art. 32 DSGVO

32
Nach Art. 32 DSGVO haben der Verantwortliche und der Auftragverarbeiter geeignete technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

33
Dies zu Grunde gelegt hat die Beklagte gegen ihre Verpflichtung, die Sicherheit der Datenverarbeitung zu gewährleisten, nicht verstoßen. Insbesondere war die Beklagte nicht verpflichtet, Schutzmaßnahmen zu treffen, um die Erhebung der immer öffentlich zugänglichen Informationen des Profils der Klagepartei aufgrund seiner selbst gewählten Einstellung zu verhindern. Diese lautete, dass ihn alle („everyone“) über seine Telefonnummer („by phone number“) finden können. Diese Einstellung beinhaltet dann aber auch das Finden der Klagepartei durch Dritte über ihre Mobilfunknummer, die Dritte etwaig auch unter Zuhilfenahme elektronischer Möglichkeiten zufällig erzeugt haben und so einen Abgleich von in den Kontaktimporter der Plattform von ... hochgeladenen und etwaig generierten Telefonnummern mit der mit dem dort eingerichteten Konto der Klagepartei verknüpften Telefonnummer vornehmen. Denn auch Dritte fallen unter den Begriff „everyone“. Unstreitig sind die Daten der Klagepartei von Dritten gescrapt, mithin verarbeitet worden iSd Art. 4 Nr. 2 DSGVO. Es handelt sich bei den unstreitig gescrapten personenbezogenen Daten der Klagepartei um Daten, die für jedermann ohne Zugangskontrolle oder Überwindung technischer Zugangsbeschränkungen wie Logins oder ähnliches abrufbar sind, was dem Kläger bereits durch die Anmeldung bekannt war.

34
Angesichts des Umstandes, dass die Klagepartei sich selbst dazu entschlossen hat, sich öffentlich durch jedermann über seine Telefonnummer suchen zu lassen, auch wenn diese nur ihm selbst angezeigt wird, besteht keine Verpflichtung der Beklagten diese insoweit vertraulich zu behandeln und entgegen dem erklärten Willen der Klagepartei nicht technisch durch eine Suchfunktion auffinden zu lassen.

(2) Kein Verstoß gegen Art. 33 DSGVO

35
Die Beklagte hat ihre Pflicht gemäß Art. 33 DSGVO, der zuständigen Aufsichtsbehörde den Datenschutzverstoß zu melden, ebenfalls nicht verletzt. Gemäß Art. 33 DSGVO meldet der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die Meldung gegenüber der Aufsichtsbehörde ermöglicht es dieser über Maßnahmen zur Eindämmung und Ahndung der Rechtsverletzung zu entscheiden.

36
Der Beklagten wurde der Datenschutzvorfall spätestens am 03.04.2021 bekannt, denn zu diesem Zeitpunkt schilderte sie Ihr Vorgehen zu dem Scraping-Vorfall auf Ihrer Website. Der zuständigen Aufsichtsbehörde, Irish Data Protection Commission (IDPC, gem. Art. 55 DSGVO) wurde unstreitig allerdings kein solcher Vorfall gemeldet. Da hierin aber der Beklagten kein Datenschutzverstoß anzulasten ist (s. o.), musste sie diesen auch nicht melden.

(3) Kein Verstoß gegen Art. 35 DSGVO

37
Soweit die Klagepartei den geltend gemachten Schadensersatz auf eine Verletzung des Art. 35 DSGVO durch die Beklagte stützt mit der Behauptung, die Beklagte habe keine Datenschutz-Folgeabschätzung im Sinne des Art. 35 DSGVO durchgeführt, verfängt er hiermit nicht. Selbst wenn die irische Datenschutzaufsichtsbehörde Ermittlungen gegen die Beklagte aufgenommen haben sollte, kann hieraus nicht geschlossen werden, dass die Beklagte im maßgeblichen Zeitraum gegen Art. 35 DSGVO verstoßen hat. Selbst wenn man annähme, dass die Beklagte in diesem Zeitraum eine Folgenabschätzung trotz hohen Risikos für die Rechte und Freiheiten der Nutzer der Plattform ... nicht durchgeführt hat, ist nicht ersichtlich, dass die unterlassene Folgeneinschätzung (mit-)ursächlich für den vom Kläger geltend gemachten Schaden war, nämlich den Verlust über die Kontrolle seiner gescrapten Daten. Hiergegen spricht bereits, dass es sich bei den gescrapten Daten um immer öffentlich zugängliche Informationen des Profils des Klägers auf der Plattform ... handelte.

(4) Kein Verstoß gegen Art. 15 DSGVO

38
Schließlich hat die Beklagte nicht gegen Art. 15 DSGVO verstoßen, indem sie der Klagepartei 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 Verarbeitungszwecke und über 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.

39
Da das Schreiben der Beklagten (Anlage B16) 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 unstreitig 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. Die Klagepartei geht selbst von 2019 aus bzw. von der Veröffentlichung dann im April 2021. Dieser Zeitrahmen ist der Klagepartei bekannt; eine genaue Eingrenzung in Bezug auf seine Daten ist nicht möglich. Die Beklagte hat der Klagepartei 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.

(5) Kein Verstoß gegen Art. 5 Abs. 1 DSGVO

40
Nach dem Grundsatz des Art. 5 Abs. 1 DSGVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Das Erfordernis der Transparenz führt Art. 13 DSGVO in Form von Informations- und Aufklärungspflichten fort. Die Aufklärung über die Zwecke der Verarbeitung muss insbesondere für den Nutzer klar verständlich und nachvollziehbar sein. Ähnliche Vorgaben sieht auch Art. 14 DSGVO für den Fall vor, dass der Verantwortliche die Daten nicht direkt bei der betroffenen Person erhebt. Auch Art. 12 DSGVO sieht eine Information in präziser, transparenter und leicht zugänglicher Form vor.

41
Diesem Maßstab wurde die Beklagte gerecht. Sie hat ihren Nutzern – und damit auch der Klägerseite – im streitgegenständlichen Zeitraum im Rahmen ihrer Datenrichtlinie und dem Hilfebereich in Bezug auf die Verwendung der Daten und insbesondere der Verwendung der Telefonnummer sowie der Kontakt-Import-Funktion klare Informationen zur Verfügung gestellt (Anlagen B 1-9). Die Aufklärung über die Verwendung der Daten erfolgte in verständlicher Sprache. Zudem ist sie auch in für den Nutzer zugänglicher Art und Weise erfolgt. Dies gilt vor allem im Hinblick darauf, dass die Beklagte eine sog. Mehrebenen-Datenschutzerklärung verwendet, bei der der Nutzer auf der ersten Ebene einen Überblick über die ihm hinsichtlich der Verarbeitung seiner personenbezogenen Daten zur Verfügung stehenden Informationen erhält und auf der zweiten Ebene die detaillierten Auskünfte durch das Anklicken eines qualifizierten Abschnitts einsehen kann. Dies dient letztlich der Vermeidung einer Überforderung des Nutzers mit einer blockartigen und überfrachteten Datenschutzinformation. Zwar trifft es zu, dass die Einstellungsmöglichkeiten über mehrere Links erreichbar sind. Die Beklagte informiert den Nutzer jedoch über sämtliche Nutzungs- und Suchbarkeitsoptionen, wie bereits aus den durch die Klägerin selbst vorgelegten Screenshots hervorgeht. Der Leser kann dabei auch gleich zu Beginn der Datenschutzrichtlinie feststellen, dass seitens der Beklagten auf die individuelle Anpassung der Privatsphäre-Einstellungen aufmerksam gemacht wird.

42
Auch aus dem Umfang dieser Datenschutzinformation kann nicht auf eine Unübersichtlichkeit geschlossen werden. In Anbetracht der Vorgaben der DSGVO und der damit verbundenen vielseitigen Informationsverpflichtungen liegt es in der Natur der Sache, dass eine Datenschutzinformation umfangreich ausfällt (LG Kiel, Urteil vom 12. Januar 2023 – 6 O 154/22, juris Rn. 46).

(6) Kein Verstoß gegen Artt. 24, 25 Abs. 2 DSGVO

43
Demnach muss der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

44
Dies soll vor allem den technisch unversierten Nutzer schützen. Die Voreinstellungen sollen möglichst datenschutzfreundlich eingestellt werden, um die Privatsphäre der Nutzer zu gewährleisten. Der Nutzer kann dann individuell Anpassungen nach seinen Wünschen vornehmen. Unstreitig sind für die Registrierung nur der Name, das Geschlecht und die ID sichtbar, die auch stets öffentlich sichtbar sind, wozu jeder User aber durch Akzeptieren der Datenschutzbestimmungen zustimmt. Soweit jemand sich dann noch entschließt seine Telefonnummer zu hinterlegen, was für die Registrierung bei ... gerichtsbekannt nicht erforderlich ist, ist diese Einstellung zwar zunächst unstreitig bei den Suchbarkeitseinstellungen auf „everyone“ „by phone number“ gestellt. Ändert man diese Einstellung nicht, so kann der jeweilige Nutzer über seine E-Mail-Adresse und Mobilnummer gefunden werden und ihm eine Freundschaftsanfrage

geschickt werden. Der technisch unkundige Nutzer wird gleichwohl über die entsprechenden Hinweise hinreichend informiert und über Einstellungsmöglichkeiten und deren Begrenzungsmöglichkeiten in Kenntnis gesetzt. Zudem muss sich jeder Internetnutzer, der insbesondere eine Plattform eines sozialen Netzwerkes wie das der Beklagten nutzt, bewusst sein, dass es Internetgepflogenheiten gibt, mit denen man sich vertraut zu machen hat, will man solche Kommunikationsplattformen gebrauchen. Der Schutz des Art. 25 DSGVO reicht nicht so weit, dass er den jeweiligen Nutzer vor den internetspezifischen Gepflogenheiten vollends schützt; vielmehr muss sich der jeweilige Nutzer, der einer Plattform eines sozialen Netzwerks beitreten will, mit den geltenden Gepflogenheiten vertraut machen. Bei einer Plattform, die auf Kontaktsuche und das Finden von Kontakten ausgerichtet ist und auf der die Beklagte angibt, dass das nicht zwingend erforderliche Hinterlegen der Telefonnummer es ermöglicht, leichter gefunden zu werden und die Zwecke der Plattform besser zu nutzen, muss der jeweilige Nutzer eigenverantwortlich entscheiden, in welchem Umfang er diese Möglichkeiten nutzt und entsprechende Daten freigibt.

45
Überdies würde selbst eine Verletzung dieser Vorschrift einen Schadensersatzanspruch nicht begründen können. Allein aus einem Verstoß gegen Art. 25 DSGVO kann wegen seines organisatorischen Charakters ein Anspruch nach Art. 82 Abs. 1 DSGVO nicht begründet werden (vgl. Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DSGVO Art. 25 Rn. 3, 34; Kühling/Buchner/Hartung, 3. Aufl. 2020, DSGVO Art. 25 Rn. 31). Die Vorschrift entfaltet bereits vor dem eigentlichen Beginn der Datenverarbeitung ihren Regelungscharakter. Zu diesem, einer tatsächlichen Datenverarbeitung vorgelagerten Zeitpunkt entfaltet die DSGVO jedoch nach Art. 2 Abs. 1 DSGVO noch keine Wirkung. Die Anwendbarkeit der DSGVO setzt vielmehr eine tatsächliche Verarbeitung personenbezogener Daten voraus (vgl. Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 7). Ein Anspruch aus Art. 82 DSGVO kommt daher nur in Betracht, wenn weitere Verstöße gegen die DSGVO vorliegen (vgl. Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DSGVO Art. 25 Rn. 3). Das ist hier indes, wie vorstehend ausgeführt, gerade nicht der Fall.

46
(7) Schließlich ist auch ein Verstoß gegen Art. 6 Abs. 1, 13 Abs. 1 DSGVO nicht feststellbar. Die Beklagte hat den Kläger ausreichend aufgeklärt gemäß Art. 13 Abs. 1 DSGVO, insbesondere über die Zwecke der Verarbeitung sowie deren Rechtsgrundlage und die etwaigen Empfänger oder Kategorien von Empfängern der personenbezogenen Daten. Der Kläger hat zudem mit der Zustimmung zu den Nutzungsbedingungen und der Datenrichtlinie die Einwilligung zu der Verarbeitung der ihn betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben gemäß Art. 6 Abs. 1 S. 1 a) DSGVO. Insbesondere wurden die Datenschutzrichtlinie sowie die Nutzungsbedingungen in einfach verständlicher Sprache abgefasst und sind einfach zugänglich. Die Website der Beklagten weist den Nutzer sogar mehrfach darauf hin, dass man einen „Privatsphärecheck“ durchführen kann. Insoweit entspricht das Ersuchen der Einwilligung auch den Voraussetzungen des Art. 7 Abs. 2 DSGVO.

47
3. Die Klagepartei ist überdies beweisfällig geblieben, dass ihr aufgrund des „Scraping-Vorgangs“ ein Schaden entstanden ist. Jedenfalls fehlt es an einem ersatzfähigen Schaden des Klägers im Sinne des Art. 82 Abs. 1 DSGVO.

48
a) Zwar ist nach Erwägungsgrund 146 S. 3 zur DSGVO der Schadensbegriff weit auszulegen, der wirksame Schadensersatz muss auch Abschreckungscharakter haben. Grundvoraussetzung ist jedoch nach Erwägungsgrund 146 zur DSGVO, dass der immaterielle Schaden „erlitten“, also tatsächlich entstanden sein muss (und nicht lediglich befürchtet werden darf). Daraus folgt auch, dass ein bloßer Verstoß gegen die DSGVO bei der Datenverarbeitung für einen Anspruch auf Ersatz immaterieller Schäden nicht ausreicht. Es muss eine kausal hierauf beruhende spürbare Beeinträchtigung des Geschädigten hinzutreten, um von einem Schaden sprechen zu können, z. B. eine benennbare und nachweisbare Persönlichkeitsverletzung wie etwa eine „Bloßstellung“ (vgl. OLG Brandenburg, Beschluss vom 21.06.2021, 1 U 69/20 = BeckRS 2021).

49
b) Hiervon ist das Gericht nach dem klägerischen Vortrag und dessen Anhörung in der mündlichen Verhandlung nicht überzeugt. Ein bloßer Kontrollverlust über seine Daten stellt keine spürbare

Beeinträchtigung im Sinne einer Persönlichkeitsverletzung und damit keinen Schaden dar. Dasselbe gilt für einen behaupteten Zustand erhöhten Misstrauens. Ein solches ergab die informatorische Anhörung gerade nicht. Der Kläger ist weiterhin bei ... angemeldet und ist auch bei weiteren sozialen Plattformen (XING) angemeldet. Weiter hat er sensible Daten, wie zB seine Handynummer dem Internetversandhändler „Amazon“ hinterlegt. Dies widerspricht gerade der klägerischen Behauptung, man habe durch ein „Scraping-Vorfall“ einen „Schaden“ in Form von Stress, Misstrauen, Angst vor Kontrollverlust etc erlitten.

50
Hinzu kommt, dass eine der Anruf unbekannter Nummern bzw Spamnachrichten nicht kausal auf den „Scraping-Vorfall“ zurückzuführen ist. Der Kläger gab im Rahmen der Anhörung an, dass Spam-Nachrichten im Zusammenhang mit seinem „Amazon-Konto“ erhalte. Genau bei Amazon unterhält der Kläger jedoch ein Kundenkonto mit dort hinterlegter Handynummer. Es drängt sich daher auf, jedenfalls ist daher zwanglos möglich, dass die Spamnachrichten auf das Nutzungsverhalten des Klägers bei „Amazon“ zurückzuführen sind.

51
4. Auch nach nationalem Recht steht dem Kläger der geltend gemachte Zahlungsanspruch nicht zu. Ein vertraglicher Anspruch gemäß §§ 280 Abs. 1, 241 Abs. 2 BGB scheidet aus, weil der Kläger keine Verletzung von vertraglichen Pflichten durch die Beklagte dargelegt hat.

52
Ansprüche gemäß §§ 823 Abs. 1, 253 Abs. 2 BGB i.V.m. dem allgemeinen Persönlichkeitsrecht bzw. mit dem Recht auf informationelle Selbstbestimmung (vgl. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) scheitern mangels Darlegung der Verletzung eines der in § 253 Abs. 2 BGB genannten Rechtsgüter durch den Kläger.

53
Schließlich besteht auch kein Anspruch nach § 823 Abs. 2 BGB i.V.m. den Vorschriften der DSGVO (s.o.)

54
II. Die Klagepartei hat keinen Anspruch auf die begehrte Feststellung (Klageantrag Ziff. 2).

55
Es wird insoweit auf die obigen Ausführungen verwiesen.

56
III. Die Klagepartei hat keinen Unterlassungsanspruch (Klageantrag. Ziff. 3).

57
Der Klagepartei steht nach §§ 1004 analog, 823 Abs. 1 und aus Abs. 2 BGB i.V.m. Art. 6 Abs. 1 DSGVO sowie Art. 17 DSGVO gegen die Beklagte ferner kein Anspruch auf Unterlassung zu, seine personenbezogenen Daten in Zukunft unbefugt, d.h. konkret ohne vorherige ausreichende Belehrung, zu veröffentlichen und diese zukünftig unbefugten Dritten zugänglich zu machen. Denn es fehlt bereits an einem Verstoß der Beklagten, der überhaupt zu einem Unterlassungsanspruch führen könnte, selbst wenn man Art. 6 DSGVO als Schutzgesetz im Sinne des § 823 Abs. 2 BGB ansieht.

58
Es fehlt jedenfalls an einem Verstoß. Die Beklagte hat die Klagepartei ausreichend aufgeklärt gemäß Art. 13 Abs. 1 DSGVO, insbesondere über die Zwecke der Verarbeitung sowie deren Rechtsgrundlage und die etwaigen Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (s.o.). Die Klagepartei hat zudem mit der Zustimmung zu den Nutzungsbedingungen und der Datenrichtlinie die Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben gemäß Art. 6 Abs. 1 S. 1 a.) DSGVO. Insbesondere wurden die Datenlinie sowie die Nutzungsbedingungen in einfach verständlicher Sprache abgefasst und sind einfach zugänglich, wenn auch mehrschichtig. Die Website der Beklagten weist einen sogar mehrfach darauf hin, dass man einen Privatsphärecheck machen kann. Insoweit entspricht das Ersuchen der Einwilligung auch den Voraussetzungen des Art. 7 Abs. 2 DSGVO. Wie ausgeführt, sind bei Auslegung nach dem objektiven Empfängerhorizont gemäß §§ 133, 157 BGB durchaus bei entsprechender Sorgfalt und Inanspruchnahme von Zeit die mehrschichtigen Hinweise nachvollziehbar

59

IV. Der Auskunftsantrag war ebenfalls abzuweisen (Klageantrag Ziff. 4).

60
Der Auskunftsanspruch nach Art. 15 Abs. 1 DSGVO unterliegt der Abweisung, da er durch das außergerichtliche Schreiben (Anlage B16) bereits erfüllt ist. Eine weitergehende Auskunft kann die Klagepartei nicht verlangen (s.o.).

61
V. Mangels Anspruch in der Hauptsache waren auch die Nebenansprüche abzuweisen.

62
VI. Die Kostenentscheidung ergibt sich aus § 91 Abs. 1 Satz 1 ZPO. Der Ausspruch zur vorläufigen Vollstreckbarkeit folgt aus §§ 708 Nr. 11, 711 ZPO.

63
Der Streitwert war gemäß § 3 ZPO festzusetzen (Klage Ziff. 1: 1.000 EUR; Ziff. 2: 2.400 EUR; Ziff. 3. 2.000 EUR; Ziff. 4. 800 EUR).