LG Coburg, Endurteil v. 08.02.2023 – 14 O 224/22

Titel:

Keine Haftung des Plattformbetreibers für Scarping (Meta/Facebook)

Normenkette:

DS-GVO Art. 4, Art. 5, Art. 15, Art. 17, Art. 18, Art. 33, Art. 82

Leitsätze:

1. Art. 82 DS-GVO erfasst nicht die behauptete Verletzung von bloßen Benachrichtigungspflichten bzw. Informationsrechten oder Verstöße gegen Art. 34 DS-GVO. (Rn. 31 – 33) (redaktioneller Leitsatz)
2. Meta (Facebook) haftet nicht wegen des Auslesens von auf "öffentlich" gestellten Daten (Scraping) mittels eines "ContactImport-Tools". (Rn. 39 – 46) (Rn. 51) (redaktioneller Leitsatz)
3. 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. (Rn. 60) (redaktioneller Leitsatz)
4. Der klägerseits behauptete „Kontrollverlust über seine Daten“ stellt keine spürbare Beeinträchtigung im Sinne einer Persönlichkeitsverletzung und damit keinen Schaden dar. (Rn. 74) (redaktioneller Leitsatz)

Schlagworte:

Datenschutz, Scraping, Schadensersatz, privacy by default, Kontrollverlust, Persönlichkeitsrechtsverletzung, VO (EU) 2016/679

Fundstellen:

ZD 2023, 308

LSK 2023, 2110

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 11.000,00 € festgesetzt.

Tatbestand

1
Der Kläger macht Ansprüche im Zusammenhang mit der Datenschutzgrundverordnung gegenüber der Beklagten geltend.

2
Der Kläger nutzte im streitgegenständlichen Zeitraum einen Facebook-Account, die Beklagte ist Betreiberin der Facebook-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. Im Jahr 2019 lasen und persistierten unbefugte Dritte Telefonnummern, Facebook-ID, Name, Vorname, Geschlecht und weitere Daten über das Tool „ContactImport“ aus zum Teil öffentlich zugänglichen Daten bei der Beklagten aus (sog. Scraping). Die Beklagte geht davon aus, dass das Contact-Import-Tool zur Bestimmung der Telefonnummern der einzelnen Benutzer genutzt wurde. 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 des ContactImport-Tools fiktive Nummern erzeugt und geprüft und die zugehörigen Nutzer wurden angezeigt. Auf dem Profil des Nutzers wurde dieser dann besucht und von dort wurden die öffentlichen Daten gescrapt („abgeschöpft"). Anfang April 2021 wurden Daten von ca. 533 Millionen Nutzern der Plattform der Beklagten aus 106 Ländern im Internet veröffentlicht.

3
Beim Anlegen eines Profils muss der künftige Nutzer Datenschutz- und CookieRichtlinien zustimmen. 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". Ebenso ist für alle Informationen, die ein Nutzer in sein Profil einträgt, standardmäßig „öffentlich" als Voreinstellung ausehen, wie die Beklagte insbesondere die Mobilfunknummer verwendet. 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. Die Grundeinstellung lautet auch insoweit zunächst „alle".

4
Der Kläger trägt vor, 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. Diese seien zuvor aus dessen Facebook-Account mittels einer Software durch unbefugte Dritte ausgelesen worden (Scraping). Hierfür sei ein Facebook-Tool benutzt worden. Die Beklagte habe keine hinreichenden Sicherheitsvorkehrungen gegen derartige Vorgänge getroffen. Ferner seien ihre Einstellungen bzgl. der Telefonnummer des Klägers so konzipiert, dass keine echte Sicherheit möglich sei.

5
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 April 2021 vermehrt dubiose E-Mails und SMS-Nachrichten von unbekannten Adressen und Nummern erhalten.

6
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. personenbezogene 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.

7
Die Beklagte beantragt, die Klage abzuweisen.

8
Die Beklagte trägt vor, es lägen keine Verstöße gegen die DSGVO vor. Zudem sei der Schutzbereich des Art. 82 DSGVO vorliegend durch die von Klägerseite behaupteten Verstöße bereits nicht eröffnet. Dem Kläger sei ferner kein kausaler, der Beklagten zurechenbarer Schaden entstanden.

9
Wegen der weiteren Einzelheiten des Sachvortrags der Parteien wird auf die gewechselten Schriftsätze nebst Anlagen sowie das Protokoll der mündlichen Verhandlung vom 25. Januar 2023 und den sonstigen Akteninhalt Bezug genommen. Das Gericht hat den Kläger im Rahmen der mündlichen Verhandlung informatorisch angehört. Auch diesbezüglich wird auf die Sitzungsniederschrift Bezug genommen.

Entscheidungsgründe

10
Die Klage ist zulässig, jedoch unbegründet.

11
A. Zulässigkeit

12
Die Klage ist zulässig. Sie ist ordnungsgemäß erhoben.

13
Zudem ist das Landgericht Coburg international, sachlich und örtlich zuständig.

14
1. Das Landgericht Coburg ist international zuständig. Gemäß Art. 1 Abs. 1 EuGVVO ist die EuGVVO sachlich anwendbar auf Zivil- und Handelssachen. Vorliegend handelt es sich um eine Zivilsache. Die deutsche Gerichtsbarkeit folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 2. Alt EuGVVO. Ein ausschließlicher Gerichtstand gemäß Art. 24 EuGVVO ist nicht ersichtlich. Gemäß Art. 18 Abs. 1 2. Alt EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat. Der Kläger ist gemäß Art. 17 Abs. 1 EuGVVO unzweifelhaft Verbraucher. Der Kläger hat seinen Wohnort in .

15
Die internationale Zuständigkeit deutscher Gerichte ergibt sich ferner aus Art. 79 Abs. 2 DSGVO. Danach können Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines

Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist. Gemäß Art. 4 Nr. 7, 8 DSGVO sind Verantwortliche natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Auftragverarbeitende sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten.

16
Die Beklagte ist Verantwortliche im Sinne dieser Vorschriften.

17
2. Das Landgericht Coburg ist auch sachlich und örtlich zuständig. 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.

18
3. Der Feststellungsantrag zu Ziffer 2 ist zulässig. Der Kläger hat sein Feststellungsinteresse gemäß § 256 Abs. 2 ZPO hinreichend dargelegt. 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.

19
B. Begründetheit

20
Die Klage hat jedoch in der Sache keinen Erfolg.

21
1. Dem Kläger steht kein Anspruch auf Ersatz immateriellen Schadens aus § 82 Abs. 1 DSGVO zu, weshalb die Klageanträge zu Ziffer 1 und Ziffer 2 abzuweisen waren. a.

22
Es fehlt vorliegend bereits an der Anwendbarkeit dieser Norm.

23
Soweit der Kläger der Beklagten mehrere Verstöße vorwirft, etwa

- ungenügende Information und Aufklärung über die Verarbeitung der ihn betreffenden Daten durch ungenügende Aufklärung zur Verwendung und Geheimhaltung der Telefonnummer (Art. 5 Abs. 1 a DSGVO),

- unmittelbaren Verstoß gegen Art. 13, 14 DSGVO, die Informationspflichten enthielten, die seitens der Beklagten nicht eingehalten worden seien, – ungenügender Schutz der personenbezogenen Daten der Nutzer von F. (Art. 24, 32 DSGVO),

- unvollständig Auskunftserteilung nach Art. 15 DSGVO, da nicht mitgeteilt worden sei, welchen Empfängern die Daten des Klägers durch Ausnutzung des Kontaktimport-Tools zugänglich gemacht worden seien (Art. 33, 34 DSGVO), sind solche Verstöße schon nicht vom Schutzzweck des Art. 82 DSGVO umfasst.

24
(1) Der sachliche Anwendungsbereich des Art. 82 DSGVO ist zunächst hinsichtlich der behaupteten, verspäteten Auskunftsansprüche aus Art. 15 DSGVO und Artikel 34 DSGVO nicht eröffnet.

25
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. Nach Art. 82 Abs. 2 S. 1 DSGVO haftet Jeder an einer Verarbeitung beteiligte Verantwortliche für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.

26
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.

27
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.

28
(a) Vorliegend sind personenbezogene Daten des Klägers betroffen.

29
Nach Art. 4 Nr. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

30
Die in jedem Fall veröffentlichten Informationen des Klägers umfassen den Namen, die Nutzer-ID sowie das Geschlecht, ohne die die Nutzung der Plattform der Beklagten nicht möglich ist, worauf direkt bei der Anmeldung hingewiesen wird. Damit ist es möglich, den Kläger zu identifizieren. Es handelt sich mithin um personenbezogene Daten. Die übrigen Daten wie Telefonnummer und E-Mail-Adresse sind ebenfalls personenbezogen. Diese sind jedoch nicht in jedem Fall öffentlich, worauf später noch näher einzugehen ist.

31
(b) Von Art. 82 DSGVO ist jedoch nur die Verarbeitung von personenbezogenen Daten umfasst. 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.

32
Die behauptete Verletzung von bloßen Benachrichtigungspflichten bzw. Informationsrechten ist 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).

33
(2) Der Schutzbereich des Art. 82 DSGVO umfasst ebenso wenig Verstöße gegen Artikel 34 DSGVO (vgl. Landgericht Essen, a.a.O., m.w.N.; Landgericht Heilbronn, a.a.O.).

34
Auch aus Art. 24 und Art. 25 DSGVO lässt sich von vornherein kein subjektives Recht herleiten (vgl. Landgericht Essen a.a.O., m.w.N.).

35
Somit kann dahinstehen, ob die Beklagten überhaupt gegen Artt. 13, 14 und 34 verstoßen hat, da sie jedenfalls nicht unter den Schutzbereich des Art. 82 DSGVO fallen, weil sie „lediglich“ Informationspflichten über die Verarbeitung enthalten, nicht aber die Verarbeitung als solche zum Gegenstand haben.

36
b. Zudem sind vorliegend keine entsprechende Pflichtverstöße der Beklagten gegen Normen der DSGVO nachgewiesen, selbst wenn man den Anwendungsbereich des Art. 82 DSGVO als eröffnet ansehen wollte.

37
(1) Es ist kein Verstoß gegen Art. 5 Abs. 1 DSGVO feststellbar.

38
(a) Es bedarf auch bei Informationspflichten der Rücksichtname auf den Grundsatz des Art. 5 Abs. 1 DSGVO, wonach personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Dieser Grundsatz der Transparenz überträgt sich in die Informations- und Aufklärungspflicht des Art. 13 DSGVO. Die Aufklärung über die Zwecke der Verarbeitung muss insbesondere für den Nutzer klar verständlich und nachvollziehbar sein (vgl. Zu diesen Grundsätzen Landgericht Essen, a.a.O.).

39
(b) Dies ist hier der Fall.

40
Die tatsächlichen Inhalte der Facebookseite sind offenkundige Tatsachen gemäß § 291 ZPO, die keines Beweises bedürfen. Gleichwohl hat die Beklagte zahlreiche Auszüge aus der Facebook-Seite vorgelegt (vgl. Anlage B1 bis B8), die auch die tatsächlichen Inhalte der Seite abbilden. Diese Inhalte der Website der Beklagten, die jedem Nutzer zugänglich sind, enthalten alle relevanten Informationen zu Art und Umfang der Verarbeitung und Hinweise zu Möglichkeiten der Begrenzung. Zwar liegen teilweise mehrschichtige Informationen vor. Dies schließt aber die Übersichtlichkeit und Transparenz nicht aus. Maßgeblich ist einzig, dass sie verständlich sind, was vorliegend der Fall ist.

41
Zwar mag es ferner sein, dass die Vielzahl der Einstellungsmöglichkeiten einige Nutzer dazu verleitet, es bei den Voreinstellungen zu belassen. Die internetspezifischen Gepflogenheiten und gerade die DSGVO verlangen jedoch vielfältige Einstellungsmöglichkeiten, damit der jeweilige Nutzer die Einstellungen entsprechend seiner spezifischen Bedürfnisse individuell vornehmen kann. Tut er dies nicht, geht dies zu seinen Lasten.

42
Zu sehen ist auch, dass die Nutzung der Plattform als solche freiwillig ist. Die Preisgabe der Mobilfunknummer ist i. Ü. für die Nutzung der Plattform nicht erforderlich. Vielmehr handelt es sich um ein Zusatzangebot der Beklagten, wodurch der jeweilige Nutzer – so auch der Kläger – auf weitere Funktionen und Informationen nutzen kann, wenn er diese nach Eingabe entsprechender Angaben nutzen will. Dies umfasste u.a. die Möglichkeit, der Zweifaktor-Authentifizierung, auf deren Nutzung es dem Kläger gerade ankam. Im Übrigen wurde über die Nutzung und Nutzungsmöglichkeiten der Mobilfunknummer ausführlich informiert (vgl. Anlagen B5, B6, B7).

43
Abgestellt auf den objektiven Empfängerhorizont gemäß §§ 133, 157 BGB ist es zwar sicherlich mit einem gewissen Aufwand verbunden, sich durch die Seiten und Hinweise zu klicken und sie sorgfältig zu lesen. Ein solcher war dem Kläger jedoch zuzumuten. Die Hinweise sind bei genauem Lesen nämlich verständlich.

44
Die Reichweite des Schutzes der DSGVO ist zudem im Lichte der jeweiligen konkreten Nutzung (beispielsweise des Internets) zu sehen. Mithin ist vorliegend zu berücksichtigen, dass es sich bei der beklagtenseits betriebenen Plattform um ein soziales Netzwerk handelt, das auf Kommunikation, Finden von Personen und Teilen von Informationen angelegt ist. In diesem Lichte sind die von der Beklagten gewählten Voreinstellungen nicht zu beanstanden, da der jeweilige Nutzer umfassend und verständlich über Änderungsmöglichkeiten informiert wird.

45
Die Einstellungsmöglichkeiten sind gesammelt über mehrere Links und Unterlinks zu erreichen, und es wurde seitens der Beklagten über die Nutzungs- und Findungsmöglichkeiten aufgeklärt. Insbesondere wird deutlich, dass man das Profil eines Nutzers über die Mobilfunknummer als solches finden kann, wenn man die Suchbarkeitsfunktion über die Mobilfunknummer überhaupt und überdies für jedermann eröffnet. Dann aber ist es auch im Lichte der internetspezifischen Gepflogenheiten umso wichtiger, dass der Nutzer sich sorgfältig mit den Hinweisen auseinandersetzt, um für sich eine Entscheidung zu treffen, ob und welche

Informationen er in welchem Umfang freigibt und wie weitgehend er die Kommunikationsplattform der Beklagten nutzen will.

46
Schließlich hat sich der Kläger – ohne dass es hierauf vorliegend entscheidungserheblich ankommt – selbst als technikaffin und vor allem bei Anmeldung bei Facebook bereits als problembewusst und sensibel im Hinblick auf mögliche Datenschutzprobleme beschrieben. Das Gericht ist daher davon überzeugt, dass die von der Beklagten zur Verfügung gestellten Informationen für den Kläger hinreichend verständlich waren.

47
(2) Es liegt auch kein Verstoß nach Art. 32 DSGVO vor.

48
(a) Nach Art. 32 DSGVO haben der Verantwortliche und der Auftragsverarbeiter 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. Gemäß Art. 5 Abs. 1 lit. f) DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung, und zwar durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit`).

49
Art. 32 DSGVO verlangt damit Verarbeitungsprozessen ab, ein angemessenes Schutzniveau für die Sicherheit personenbezogener Daten zu gewährleisten, um damit angemessenen Systemdatenschutz sicherzustellen. Das Gebot soll personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen u.a. davor schützen, dass Dritte diese unbefugt oder unrechtmäßig verarbeiten (vgl. Landgericht Essen, a.a.O.; Amtsgericht Straußberg, a.a.O., Landgericht Heilbronn, a.a.O.).

50
(b) Nach diesen Grundsätzen, denen das Gericht folgt, hat die Beklagte vorliegend nicht gegen ihre Verpflichtung, die Sicherheit der Datenverarbeitung zu gewährleisten, verstoßen.

51
Insbesondere war die Beklagte nicht verpflichtet, Schutzmaßnahmen zu treffen, um die Erhebung der immer öffentlich zugänglichen Informationen des Profils des Klägers aufgrund seiner selbst gewählten Einstellung zu verhindern. Diese lautete unbestritten, dass ihn alle („everyone“) über seine Telefonnummer („by phone number“) finden können. Diese Einstellung enthält dann aber auch die Möglichkeit des Auffindens des Klägers durch Dritte über seine Mobilfunknummer dergestalt, dass Dritte auch unter Zuhilfenahme elektronischer Möglichkeiten seine Mobilfunknummer erzeugt haben und so einen Abgleich von in dem Kontakt-Import-Tool der Plattform hochgeladenen und etwaig generierten Telefonnummern mit der mit dem dort eingerichteten Konto des Klägers verknüpften Telefonnummer vornehmen. Denn auch Dritte fallen unter den Begriff „everyone“.

52
Soweit Daten des Klägers von Dritten unstreitig gescrapt, mithin i.S.d. Art. 4 Nr. 2 DSGVO verarbeitet wurden, war die Beklagte nicht verpflichtet, diese Daten vor der Verarbeitung durch die Scraper zu schützen, da die Daten nicht unbefugt bzw. unrechtmäßig verarbeitet worden sind.

53
Es handelt sich bei den gescrapten personenbezogenen Daten des Klägers, nämlich seinen Namen, sein Geschlecht und seinen Benutzernamen etc., um Daten, die für jedermann ohne Zugangskontrolle oder Überwindung technischer Zugangsbeschränkungen wie Logins oder Ahnliches abrufbar waren, was dem Kläger bereits durch die Anmeldung bekannt war. Die Erhebung dieser Daten als solche erfolgte daher nicht unbefugt bzw. unrechtmäßig. Diese Verarbeitung in Form des Scrapens erfolgt auch durch Dritte und nicht durch die Beklagte.

54

Dass nicht öffentlich zugängliche Informationen von Dritten erhoben worden sind, kann nicht festgestellt werden.

55
Der Kläger hat im Rahmen informatorischer Anhörung bestätigt, dass sämtliche gescrapte Daten - mit Ausnahme der Mobilfunknummer – auf seinem Facebook-Profil öffentlich einsehbar waren (u.a. auch der Arbeitgeber etc.).

56
Zwar muss die Beklagte aufgrund der Fülle an personenbezogener Daten soweit möglich dafür sorgen, dass gerade sensiblere Daten wie E-Mail-Adressen oder Telefonnummern nicht einfach und schnell zu erlangen sind. Dies tut sie aber bereits dadurch, dass die Freigabe der Telefonnummer lediglich eine Komfortfunktion ist. Zudem leitet sich aus der DSGVO kein Anspruch auf bestimmte konkrete Sicherungsmaßnahmen ab, sondern die Beklagte muss allenfalls für ein hinreichendes Schutzniveau sorgen, was vorliegend geschehen ist.

57
Die Beklagte beschäftigt gerichtsbekannt ein EDM-Team (External-Data-Misuse-Team) und verfügt nach eigenen Angaben auch über Datenübertragungsbeschränkungen, wenn von einer bestimmten IP-Adresse in einem bestimmten Zeitraum eine bestimmte Anzahl von Anfragen gestellt werden. Schließlich veröffentlichte sie gerichtsbekannt am 15., 16. und 19. April 2019 Artikel zum fraglichen Vorfall. Kriminelles Verhalten wie Scraping lässt sich jedoch nicht immer verhindern, da externe Dritte mitunter gerade bemüht sind, etwa unter Verwendung einer Vielzahl von IP-Adressen und „gestaffelter“ Abfragen, die bestehenden Sicherheitsbarrieren zu überwinden.

58
(3) Verstöße gegen das in Art. 24, 25 Abs. 2 DSGVO verankerte Prinzip „Privacy by default“ sind ebenfalls nicht feststellbar.

59
(a) 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.

60
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 Facebook 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 (so auch Landgericht Essen, a.a.O.; Landgericht Heilbronn, a.a.O.).

61
(4) Es liegt auch kein Verstoß gegen Art. 35 DSGVO vor.

62
Auch wenn die irische Datenschutzaufsichtsbehörde Ermittlungen gegen die Beklagte aufgenommen und zwischenzeitlich eine Geldbuße gegen die Beklagte verhängt hat, kann hieraus nicht geschlossen werden, dass dies zu einem Schadensersatzanspruch des Klägers führt. Selbst wenn man annehmen wollte, dass die Beklagte in hier streitgegenständlichen Zeitraum eine Folgenabschätzung trotz hohen Risikos für die Rechte und Freiheiten der Nutzer der Plattform nicht durchgeführt habe, ist bereits 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.

63
Hiergegen spricht bereits, dass es sich bei den gescrapten Daten um immer öffentlich zugängliche Informationen des Profils des Klägers auf der Plattform handelte (vgl. dazu auch Landgerich Heilbronn, a.a.O.).

64
(5) Auch hat die Beklagte nicht gegen Art. 15 DSGVO verstoßen, indem sie dem Kläger keine bzw. unvollständige Auskünfte erteilt hat.

65
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.

66
Das Schreiben der Beklagten vom 7. Oktober 2021 (vgl. Anklage B15) informiert den Kläger insoweit umfassend. Damit ist der Anspruch insoweit erfüllt und erloschen (§ 362 Abs. 1 BGB).

67
Unstreitig nicht beantwortet wird durch die Beklagte in diesem 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 von der Klagepartei begehrte Auskunftserteilung ist daher aufgrund des Vorganges des Scrapings unter Ausnutzung von Daten, die auf „öffentlich“ gestellt sind, unmöglich. Ebenso ist im Rechtssinne unmöglich zu informieren, wann die Daten gescrapt wurden. 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.

68
(6) Schließlich ist auch ein Verstoß gegen Artt. 6 Abs. 1, 13 Abs. 1 DSGVO nicht ersichtlich.

69
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 Datenlinie sowie die Nutzungsbedingungen in einfach verständlicher Sprache abgefasst und sind einfach zugänglich, wenn auch mehrschichtig (dazu schon oben). 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. Wie bereits ausgeführt, sind bei Auslegung nach dem objektiven Empfängerhorizont gemäß §§ 133, 157 BGB durchaus bei entsprechender Sorgfalt und Inanspruchnahme von Zeit die mehrschichtigen Hinweise nachvollziehbar c.

70
Jedenfalls hinsichtlich der Telefonnummer des Klägers ist zudem eine Kausalität des Scraping-Vorfalls für die klägerseits vorgetragenen dubiosen SMS und Spam-E-Mails nicht nachgewiesen. Zunächst bleibt festzustellen, dass die Klagepartei die angebliche, von der Beklagten jedoch bestrittene Vielzahl dubioser SMS und Spam-E-Mails (bis auf vereinzelte Exemplare im Rahmen der mündlichen Verhandlung sowie durch Anlagenkonvolut K7) nicht nachgewiesen hat. Denn aus Anlage B 16 geht hervor, dass der Kläger im Zeitraum des Scraping-Vorfalls in den Einstellungen seines Facebook Accounts seine Telefonnummer für jedermann („Everyone“) sichtbar gestellt hatte, also nicht lediglich für seine Freunde oder für niemanden („Only me“). Somit konnte in dem genannten Zeitraum jeder, der ebenfalls einen Facebook-Account unterhielt, die Telefonnummer des Klägers legal und ohne Scraping in Erfahrung bringen. Dass die vom Kläger vorgetragenen und vereinzelt bewiesenen Spam-SMS und Spam-Emails kausal auf dem Scraping-Vorfall beruhen, ist damit nicht nachgewiesen.

71
d. Jedenfalls fehlt es aber an einem ersatzfähigen Schaden des Klägers im Sinne des Art. 82 Abs. 1 DSGVO.

72
(1) 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“ (Landgericht Essen, a.a.O. m.w.N.)

73
(2) Nach diesen Grundsätzen, denen das Gericht folgt, ist ein Schaden des Klägers weder substantiiert vorgetragen noch ersichtlich.

74
Der klägerseits behauptete „Kontrollverlust über seine Daten“ stellt keine spürbare Beeinträchtigung im Sinne einer Persönlichkeitsverletzung und damit keinen Schaden dar. Dasselbe gilt für einen behaupteten „Zustand großen Unwohlseins und Sorge über möglichen Missbrauch seiner Daten“. Die Behauptung, der Kläger habe seit April 2021 vermehrt dubiose E-Mails und Nachrichten von unbekannten Adressen und Nummern erhalten, genügt ebenfalls nicht. Ferner gehört derartiges in der digitalisierten Welt mittlerweile zum allgemeinen Lebensrisiko, insbesondere dann, wenn man – wie der Kläger – durch Unterhaltung eines Facebook-Accounts oder durch Teilnahme an anderen sog. sozialen Netzwerken wie Instagram seine personenbezogenen Daten ins Internet stellt. Angebliche Spam-E-Mails und -nachrichten können damit genauso von Personen stammen, die legal durch Teilnahme an einem sozialen Netzwerk an E-Mail-Adresse und Telefonnummer des Klägers gelangt sind.

75
2. Aus obigen Gründen scheitern auch die weiteren Klageanträge zu Ziffern 3 bis 5. Etwaige konkurrierende Anspruchsgrundlagen (z.B. §§ 280, 823 Abs. 2, 1004 BGB) kommen nicht in Betracht (vgl. LG Essen, a.a.O.).

76
Der Kläger hat keinen Unterlassungsanspruch gegen die Beklagte gemäß §§ 1004 analog, 823 Abs. 2 BGB iVm Art. 6 I, Art. 17 DSGVO. Eine Zuwiderhandlung der Beklagten liegt nicht vor und ist auch nicht für die Zukunft zu befürchten.

77
Der Kläger hat auch keinen Anspruch auf eine weitergehende Auskunft gemäß Art. 15 DSGVO.

78
Die Beklagte hat dem Kläger Auskunft über die von ihr verarbeiteten Daten in angemessener Weise zur Verfügung gestellt (siehe dazu schon oben). Welche Daten des Klägers gescrapt worden sind, ist dem Kläger bereits bekannt, so dass auch diesbezüglich keine weitergehende Auskunftspflicht bestehen kann. Soweit der Kläger ferner Auskunft über die Empfänger der „Scraping – Daten“ verlangt, scheitert ein Anspruch an der erteilten Auskunft der Beklagten, sie sei zu weiteren Informationen nicht imstande.

79
Mangels Hauptanspruch besteht auch kein Anspruch auf Ersatz etwaiger Nebenforderungen wie die Zahlung von Zinsen oder die Erstattung vorgerichtlicher Rechtsanwaltskosten.

C.

80
Die Kostenentscheidung ergibt sich aus § 91 Abs. 1 Satz 1 ZPO. Der Ausspruch zur vorläufigen Vollstreckbarkeit folgt aus § 709 ZPO.

81
Der Streitwert war gemäß § 3 ZPO festzusetzen.