LG Landshut, Endurteil v. 10.01.2025 – 13 O 838/24

Titel:

Reichweite der sekundären Darlegungslast

Normenketten:

DSGVO Art. 82 Abs. 1

ZPO § 138

Leitsätze:

1. Dem Prozessgegner ist eine sekundäre Darlegungslast aufzuerlegen, sofern die primär darlegungsbelastete Partei keine nähere Kenntnis von den maßgeblichen Umständen und auch keine Möglichkeit zur weiteren Sachverhaltsaufklärung hat, während der Prozessgegner die wesentlichen Tatsachen kennt und es ihm unschwer möglich und zumutbar ist, nähere Angaben zu machen. In diesem Rahmen obliegt es dem Prozessgegner auch, zumutbare Nachforschungen zu unternehmen. (Rn. 22) (redaktioneller Leitsatz)

2. Die sekundäre Darlegungslast führt weder zu einer Umkehr der Beweislast noch zu einer über die prozessuale Wahrheitspflicht und Erklärungslast hinausgehenden Verpflichtung der Partei, ihrem primär darlegungs- und beweisbelasteten Gegner alle für seinen Prozesserfolg benötigten Informationen zu verschaffen. (Rn. 22) (redaktioneller Leitsatz)

Schlagworte:

Datenschutz-Grundverordnung, Scraping-Vorfall, Internationale Zuständigkeit, Rügelose Einlassung, Darlegungs- und Beweislast, Sekundäre Darlegungslast, Kostenfolge

Fundstelle:

GRUR-RS 2025, 1283

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 2.500,00 € festgesetzt.

Tatbestand

1
Die Klagepartei macht Ansprüche nach einem behaupteten Datenschutzverstoß der Beklagten geltend.

2
Die Beklagte betreibt das soziale Netzwerk F. , auf welches sowohl über die Internetseite www.f..com als auch über eine gleichnamige App mittels Smartphone oder Tablet im Gebiet der Europäischen Union zugegriffen werden kann. Dieses soziale Netzwerk wird durch die Klagepartei genutzt.

3
Das soziale Netzwerk F. ermöglicht nach Anmeldung die Erstellung von persönlichen Profilen, welche mit Freunden geteilt werden können. Auf diesen Profilen können die Nutzer verschiedene Daten zu Ihrer Person angeben, wobei bestimmte Informationen wie Name, Geschlecht und Nutzer-ID stets öffentlich sind.

4
Anfang April 2021 wurde durch die Medien öffentlich berichtet, dass von Unbekannten Daten von ca. 533 Millionen F. Nutzern im Internet öffentlich verbreitet werden. Die Unbekannten hatten durch sogenanntes „Scraping“ diese Daten aus öffentlich zugänglichen Dateien der Beklagten ausgelesen. Zu diesem Zweck

erzeugten die Unbekannten künstliche Telefonnummern, welche anschließend in das von F. bereitgestellte Contact-Import-Tool eingegeben wurden. Der Contact-Importer überprüfte sodann, ob diese Telefonnummer zu einem Profil bei F. passt. Sofern beim jeweiligen F. -Profil die Standardeinstellung „Finden über die Telefonnummer“ auf „Alle“ eingestellt war, konnte über den Contact-Importer der vorhandene Datensatz ausgelesen werden.

5
Die Klagepartei behauptet, der sog. „Scraping-Vorfall“ habe im September 2019 stattgefunden. Ihre Daten seien in dem vorgenannten Datensatz veröffentlicht worden. Aus der von den Unbekannten veröffentlichten Datenbank würden sich die Telefonnummer, die F. -ID und ihr Name ergeben. Die Ausnutzung der beschriebenen Funktion des Contact-Importers sei nur dadurch möglich gewesen, da die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um eine solche Ausnutzung des Contact-Importers zu verhindern. Die ausgelesenen Daten würden für gezielte Phishingattacken genutzt. Durch die datenschutzunfreundlichen Voreinstellungen ihres F. -Accounts sei die Datensicherheit beeinträchtigt worden, da mit hoher Wahrscheinlichkeit zu erwarten sei, dass ein Nutzer die Standardeinstellungen beibehalten würde. Eine Aufklärung, dass die Telefonnummer zur Identifikation des Profils genutzt werden könne, habe es nicht gegeben bzw. diese sei uneindeutig gewesen. Bei einem entsprechenden Hinweis auf das Contact-Import-Tool hätte die Klägerin ihre Daten nicht öffentlich geteilt. Die Zuordnung der Telefonnummer zu weiteren Daten wie Mailadressen oder Anschriften würde sogar den Identitätsdiebstahl zulasten der Klagepartei ermöglichen. Nachdem die Beklagte über die abgegriffenen Daten keine Auskunft erteilen würde, könne die Klagepartei sich nicht sicher sein, dass nicht noch mehr Daten abgegriffen worden seien. Die Klagepartei erleide daher einen Kontrollverlust über ihre Daten.

6
Die Klageseite meint, der zeitliche Anwendungsbereich der DSGVO sei eröffnet. Hinsichtlich des „relevanten Zeitpunkts“ des Datenabgriffs obliege der Beklagten eine sekundäre Darlegungslast, der sie nicht nachgekommen sei.

7
Der Kläger beantragte zuletzt,

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. eine Verarbeitung personenbezogene Daten derKlägerseite, namentlich Telefonnummer, F. -ID,Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt und Beziehungsstatus, über die Eingabe der Telefonnummer der Klägerseite in das Kontakt-Import-Tool und die darüber hergestellt Verknüpfung der eigegebenen Telefonnummer mit weiteren öffentlichen personenbezogenen Daten des Nutzerprofils der Klägerseite zu ermöglichen, ohne dass die Beklagten zum Zeitpunkt der Verwendung des Kontakt-Import-Tools unter Eingabe der Telefonnummer Sicherheitsmaßnahmen in Form einer Implementierung von Sicherheits-CAPTCHAs und der Überprüfung massenhafter IP-Abfragen oder vergleichbaren Sicherheitsmaßnahmen vorgehalten hat.

b. die Telefonnummer der Klägerseite durch Kontaktvorschläge für Dritte, welche diese Telefonnummer abfragen, mit dem F. profil des Klägers zu verknüpfen, solange der Kläger hierzu nicht ausdrücklich einwilligt.

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 538,95 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

8
Die Beklagte beantragte,

Klageabweisung.

9
Die Beklagte behauptet, der „Scraping-Vorfall“ habe sich zwischen Januar 2018 und September 2019 ereignet. Sie sei nicht in der Lage, den genauen Zeitpunkt des Scrapings der Daten der Klagepartei zu bestimmen. Sie sei nicht im Besitz der Rohdaten, welche die durch Scraping abgerufenen Daten enthielten und halte aufgrund der seit dem Scraping-Sachverhalt vergangenen Zeit keine Logdateien vor, die es ihr ermöglichen würden, genau herauszufinden, wie der Scraping-Sachverhalt abgelaufen sei oder wann die Daten der jeweiligen Klagepartei gescraped worden seien. Darüber hinaus wisse die Beklagte weder, wer die Scraper gewesen seien, noch welches F. -Konto sie gegebenenfalls verwendet hätten, um das F. -Profil der Klagepartei einzusehen. Die Nutzer würden darüber hinaus auf der F. -Plattform umfangreich über ihre Privatsphäreeinstellungen informiert. Die Beklagte habe ausreichende Sicherheitsvorkehrungen gegen Missbrauch des Contact-Importers vorgenommen, auch Maßnahmen gegen Scraping habe die Beklagte in ausreichendem Maße eingeführt.

10
Die Beklagte meint, der zeitliche Anwendungsbreich der DSGVO sei nicht eröffnet. Das Risiko der Nichterweislichkeit des genauen Zeitpunkts des Abrufens der Daten der Klagepartei gehe zu Lasten der beweisbelasteten Klagepartei.

11
Das Gericht hat am 04.12.2024 mündlich verhandelt und den Kläger informatorisch angehört. Eine Beweisaufnahme hat nicht stattgefunden.

12
Zur Ergänzung des Tatbestands wird auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen Bezug genommen.

Entscheidungsgründe

13
Die zulässige Klage ist unbegründet.

A.

14
Das Landgericht Landshut ist zuständig, insbesondere folgt die internationale Zuständigkeit deutscher Gerichte aus Art. 6 Abs. 1, Art. 18 Abs. 1 Alt. 2 EuGVVO. Die örtliche und sachliche Zuständigkeit ergibt sich jedenfalls infolge rügeloser Einlassung der Parteien nach § 39 ZPO.

B.

15
Die Klage ist unbegründet.

16
Der Klagepartei stehen keinerlei Ansprüche aus der Datenschutz-Grundverordnung zu.

17
I. Es ist nicht festzustellen, dass der streitgegenständliche Scraping-Vorfall in den zeitlichen Anwendungsbereich der DSGVO fällt.

18
Hinsichtlich der zeitlichen Anwendbarkeit ist nicht der Zeitpunkt der Registrierung eines Nutzerkontos im sozialen Netzwerk der Beklagten maßgeblich, sondern der Zeitpunkt des Scraping-Vorfalls (BGH, Urteil vom 18. November 2024 – VI ZR 10/24 –, Rn. 19, juris).

19
II. Die Klagepartei ist beweisfällig geblieben für ihre Behauptung, der Abgriff der klägerischen Daten sei nach dem Inkrafttreten der DSGVO am 25.05.2018 erfolgt.

20
1. Nach allgemeinen Grundsätzen trägt die Klagepartei die Darlegungs- und Beweislast dafür, dass der zeitliche Anwendungsbereich der DSGVO eröffnet ist.

21
Zweifelhaft ist bereits, ob der Vortrag der Klagepartei, sie stelle auf den Abgriffszeitpunkt September 2019 ab, den Anforderungen an substantiierten Tatsachenvortrag genügt oder nicht vielmehr eine Behauptung ins Blaue hinein darstellt. Denn es erschließt sich nicht, wie die Klagepartei auf diesen (konkreten) Zeitpunkt kommt. Darüber hinaus ist die Behauptung der Klagepartei beweisbedürftig, weil die Beklagte abweichend vorträgt, der Vorfall habe zwischen Januar 2018 und September 2019 stattgefunden. Beweis für ihre Behauptung hat die Klagepartei nicht angeboten.

22
2. Die Behauptung der Klagepartei, die Daten seien im September 2019 abgegriffen worden, ist auch nicht deshalb als zugestanden zu behandeln, weil die Beklagtenseite ihrer sekundären Darlegungslast nicht genügt hätte. Dem Prozessgegner ist eine sekundäre Darlegungslast aufzuerlegen, sofern die primär darlegungsbelastete Partei keine nähere Kenntnis von den maßgeblichen Umständen und auch keine Möglichkeit zur weiteren Sachverhaltsaufklärung hat, während der Prozessgegner die wesentlichen Tatsachen kennt und es ihm unschwer möglich und zumutbar ist, nähere Angaben zu machen. In diesem Rahmen obliegt es dem Prozessgegner auch, zumutbare Nachforschungen zu unternehmen (vgl. etwa BGH, Versäumnisurteil vom 4.2.2021 – III ZR 7/20). Die sekundäre Darlegungslast führt aber weder zu einer Umkehr der Beweislast noch zu einer über die prozessuale Wahrheitspflicht und Erklärungslast hinausgehenden Verpflichtung der Partei, ihrem primär darlegungs- und beweisbelasteten Gegner alle für seinen Prozesserfolg benötigten Informationen zu verschaffen (BeckOK ZPO/von Selle, 54. Ed. 1.9.2024, ZPO § 138 Rn. 20, beck-online).

23
Sofern man der Beklagten eine sekundäre Darlegungslast auferlegen will, so ist sie dieser nach Maßgabe der vorgenannten Grundsätze hinreichend nachgekommen, indem sie den relevanten Zeitraum auf Januar 2018 bis September 2019 eingegrenzt hat und vorgetragen hat, dass sie nicht in der Lage ist, den genauen Zeitpunkt des Scrapings der Daten der Klagepartei zu bestimmen. Die Beklagte sei nicht im Besitz der Rohdaten, welche die durch Scraping abgerufenen Daten enthalten und halte aufgrund der seit dem Scraping-Sachverhalt vergangenen Zeit keine Logdateien vor, die es ihr ermöglichen würden, genau herauszufinden, wie der Scraping-Sachverhalt abgelaufen sei oder wann die Daten der jeweiligen Klagepartei gescraped worden seien. Darüber hinaus wisse die Beklagte weder, wer die Scraper gewesen seien, noch welches F. -Konto sie gegebenenfalls verwendet hätten, um das F. -Profil der Klagepartei einzusehen (vgl. etwa Bl. 88, 91, 322, 325, 461/462 d.A.).

24
3. Es kann auch nicht von einem Dauerdelikt ausgegangen werden, denn der Abgriff von Daten zu einem bestimmten Profil kann bei einem Treffer bezüglich der Telefonnummer nur zu einem ganz bestimmten Zeitpunkt erfolgen, nämlich dann, wenn der konkrete Datensatz aus dem Tool abgerufen wird. Wurde der Datensatz vor der zeitlichen Geltung des DSGVO abgegriffen, können mögliche Verstöße gegen die Vorschriften der DSGVO dafür nicht ursächlich sei (OLG Stuttgart, Urteil vom 4. Dezember 2024 – 4 U 97/24).

25
4. Soweit die Klagepartei meint, nach Ansicht des Bundesgerichtshofs sei angesichts des von der Beklagten angegebenen Zeitraums davon auszugehen, dass sich der Scraping-Vorfall jedenfalls nach Mai 2018 ereignet habe, so bleibt unklar, auf welche Ausführungen des Bundesgerichtshofs die Klagepartei sich

stützt. Aus der jüngsten Entscheidung des Bundesgerichtshofs vom 18.11.2024 – VI ZR 10/24 ergibt sich dies jedenfalls nicht. Der Bundesgerichtshof war als Revisionsgericht dort an die Feststellungen des Oberlandesgerichts Köln gebunden, wonach der Scraping-Vorfall in Bezug auf den dortigen Kläger nicht vor dem Mai 2018 stattgefunden habe.

26
5. Gesicherte Rückschlüsse auf den Zeitpunkt des Scraping-Vorfalls lassen sich auch nicht aus dem Zeitpunkt des von dem Kläger behaupteten erhöhten Spam-Aufkommens ableiten. Dem Kläger gelingt der Nachweis nicht, dass der erhaltene Spam kausal auf den streitgegenständlichen Scraping-Vorfall zurückzuführen ist. Dies gilt schon deshalb, weil der Kläger seine Telefonnummer nach eigenem Vortrag auch anderweitig nutzt, etwa für die Verifizierung beim Online-Shopping, sodass nicht auszuschließen ist, dass die klägerischen Daten anderweitig abgegriffen wurden.

C.

27
Mangels Anspruch in der Hauptsache besteht auch kein Anspruch Zahlung außergerichtlicher Rechtsanwaltskosten oder Zinsen.

D.

28
Die Kostenfolge ergibt sich aus § 91 ZPO. Die vorläufige Vollstreckbarkeit resultiert aus § 709 ZPO. Der Streitwert wird gemäß § 3 ZPO auf 2.500,00 € (Ziff. 1: 1.000,00 €, Ziff. 2-4 jeweils 500,00 €) geschätzt (vgl. Zur Streitwertbemessung in Scraping-Fällen etwa OLG Hamm (7. Zivilsenat), Hinweisbeschluss vom 22.09.2023 – 7 U 77/23).