

Leitsatz:

Bestreitet der Plattformbetreiber die Behauptung des Nutzers, eine bestimmte E-Mail-Anschrift zur Anlage eines Accounts genutzt zu haben, kann allein mit einem sich auf diese E-Mail beziehenden Ausdruck der Website www.haveibeenpwnd.com nicht der Nachweis der Betroffenheit von einem Datenschutzvorfall geführt werden. Hierfür trägt der Nutzer die Beweislast.

OLG Dresden, 4. Zivilsenat, Beschluss vom 8. Januar 2025, Az.: 4 U 1090/24



Oberlandesgericht

Dresden

Zivilsenat

Aktenzeichen: **4 U 1090/24**
Landgericht Leipzig, 08 O 1782/23

BESCHLUSS

In dem Rechtsstreit

F..... Ö....., ...

- Kläger und Berufungskläger -

Prozessbevollmächtigte:

D..... Rechtsanwaltsgesellschaft mbH, ...

gegen

.....

vertreten durch den Vorstandsvorsitzenden

- Beklagte und Berufungsbeklagte -

Prozessbevollmächtigte:

Rechtsanwälte W..... & C..... LLP, ...

wegen Schadensersatz, Feststellung, Unterlassung und Auskunft

hat der 4. Zivilsenat des Oberlandesgerichts Dresden durch

Vorsitzenden Richter am Oberlandesgericht S.....,

Richterin am Oberlandesgericht Z..... und

Richterin am Oberlandesgericht R.....

ohne mündliche Verhandlung am 08.01.2025

beschlossen:

1. Der Senat beabsichtigt, die Berufung des Klägers ohne mündliche Verhandlung durch Beschluss zurückzuweisen.
2. Der Kläger hat Gelegenheit, innerhalb von zwei Wochen Stellung zu nehmen. Er sollte allerdings auch die Rücknahme der Berufung in Erwägung ziehen.
3. Der Termin zur mündlichen Verhandlung am 14.01.2025 wird aufgehoben.
4. Der Senat beabsichtigt, den Streitwert für beide Instanzen auf 6.500 € festzusetzen.

Gründe:

I.

Der Senat beabsichtigt, die zulässige Berufung nach § 522 Abs. 2 ZPO ohne mündliche Verhandlung durch - einstimmig gefassten - Beschluss zurückzuweisen. Die zulässige Berufung des Klägers bietet in der Sache offensichtlich keine Aussicht auf Erfolg. Die Rechtssache hat auch weder grundsätzliche Bedeutung noch erfordert die Fortbildung des Rechts oder die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Berufungsgerichts durch Urteil. Auch andere Gründe gebieten eine mündliche Verhandlung nicht.

Zu Recht hat das Landgericht die Klage zurückgewiesen. Die hiergegen gerichteten Einwendungen des Klägers greifen nicht durch.

1. Den geltend gemachten Ansprüchen steht entgegen, dass der nach allgemeinen Grundsätzen darlegungs- und beweisbelastete Kläger (vgl. EuGH, Urte. v. 14.12.2023 - C-340/21, juris Rn. 84; v. 21.12.2023 - C-667/21, juris Rn. 99) nicht substantiiert vorgetragen und unter Beweis gestellt hat, dass er sich bei der Beklagten registriert und zwischen ihm und der Beklagten ein Nutzungsvertragsverhältnis im relevanten Zeitraum bestanden hat. Ferner fehlt die schlüssige Darlegung, welche seiner Daten und ggfls. in welchem Umfang diese von einem Datenleck bei der Beklagten betroffen sein sollen.

a) Der Kläger hat mit der vorliegenden Klage zunächst behauptet, er sei Nutzer der von der Beklagten betriebenen Plattform X, bei der er sich mit der Email-Anschrift „.....@googlemail.com“ angemeldet habe. Eine Abfrage mittels dieser Email-Anschrift bei der Website „haveibeenpwned.com“ habe ergeben, dass diese Email-Adresse von einem Datenleck bei Twitter betroffen sei (vgl. Anlage DB1). Mit Schreiben vom 11.04.2023 hat der Prozessbevollmächtigte der Beklagten mitgeteilt, dass mit der von der Klagepartei angegebenen Email-Adresse „neindustries1@googlemail.com“ kein Twitter-Account verbunden und es der Beklagten daher nicht möglich sei, die Identität der betroffenen Person zu identifizieren (vgl. Anlage B3).

Dem ist der Kläger nicht substantiiert entgegengetreten. Die alleinige Bezugnahme auf eine Abfrage bei dieser Webseite belegt für sich genommen jedoch nicht, dass der Kläger sich mit der angegebenen Email-Anschrift bei der Beklagten registriert, ein Nutzerkonto im relevanten Zeitraum unterhalten hat und - bezogen darauf - von einem Datenhacking im Jahr 2023 betroffen gewesen ist, das auf Datenschutzverstöße bei der Beklagten zurückzuführen ist.

b) Mit Schriftsatz vom 29.01.2024 hat der Kläger sodann behauptet, er habe zum Zeitpunkt des Datenlecks ein Konto unter dem Aliasnamen „@UltimateReview0“ betrieben. Zu dem Konto sei die Email-Adresse „.....@gmail.com“ hinterlegt gewesen (vgl. Bl. 86 eA LG). Als Nachweis hat er einen Screenshot eines im Jahr 2009 angelegten Twitter-Accounts „ProjectCancer“ mit dem Nutzernamen @UltimateReview0 und der benannten Email-Adresse vorgelegt. Aus dem Screenshot ergibt sich jedoch auch, dass die Accountinformationen nicht verifiziert sind.

Vor diesem Hintergrund hätte es ihm oblegen, mit der Berufungsbegründung seine konkrete Betroffenheit vom Datenleck nachzuweisen, da sich entgegen seiner Ansicht die Betroffenheit nicht bereits aus einer Auskunft der Webseite „haveibeenpwned.com“ ergibt

und infolge der Anmeldung unter einem Aliasnamen bzw. einem Pseudonym nicht ohne weiteren Sachvortrag oder geeignete Nachweise nachvollzogen werden kann. Es ist bereits nicht hinreichend geklärt und kann auch nicht mittels dieser Auskunft geklärt werden, ob die Email-Adresse vom Kläger genutzt wird oder wurde, und mit welchen konkreten Daten der Kläger betroffen sein soll.

2. Der Kläger hat zudem einen auf mögliche Verstöße gegen die DSGVO zurückzuführenden immateriellen Schaden nicht hinreichend dargelegt, so dass ein Schadenersatzanspruch auch vor dem Hintergrund der aktuellen Rechtsprechung des BGH nicht begründet ist (vgl. zu den Anforderungen an die Darlegungslast zuletzt Senat, Urt. v. 10.12.2024 - 4 U 815/23, m.w.N., zur Veröffentlichung bei juris vorgesehen).

a) Die E-Mail-Adresse „.....@googlemail.com“ soll nach der Website „haveibeenpwned.com“ von zwei Datenlecks betroffen gewesen sein. Die Einträge lauten: „Disqus“ - hier soll das Datenleck zeitlich vor 2023 erfolgt sein - und „Twitter (200M)“. Selbst wenn zugunsten des Klägers unterstellt wird, dass die Email-Adresse zu einem vom Kläger geführten Account hinterlegt ist, hat der Kläger auch nicht dargelegt, dass er vor dem API-Bug die Kontrolle über diese streitgegenständliche E-Mail-Adresse innehatte und die Kontrolle erst durch den API-Bug verloren hat.

b) Die Darlegung eines durch den API-Bug verursachten Kontrollverlust fehlt auch hinsichtlich der Email-Adresse „.....@gmail.com“, zu der der Kläger einen Screenshot eines Twitter-Accounts vorgelegt hat. Zwar hat er sich als Nachweis seiner Betroffenheit auf einen Datenabgleich mittels Auskunft der Webseite „haveibeenpwned.com“ berufen. Diese weist aber - nach aktueller Abfrage des Senats - freilich eine weitere Betroffenheit von insgesamt 18 Datenlecks aus den Jahren 2013 bis 2024 aus, darunter u.a. Adobe, Nexus Mods, Bitcoin Talk, bitly, 500px, younow, Appen, 123RF, Teespring, Gravatar, Deezer (aus den Jahren 2013-2022). Daher ist ein Kontrollverlust durch die Abfrage bei „haveibeenpwned.com“ nicht nachgewiesen oder auch nur hinreichend belegt, letztlich vermutet der Kläger lediglich einen solchen. Denn er hat nicht dargelegt, dass er vor dem API-Bug die Kontrolle über die streitgegenständlichen Email-Adressen innehatte und diese erst durch den API-Bug verloren hat.

Der Senat rät daher zur Rücknahme der Berufung, die zwei Gerichtsgebühren spart.

II.

Die beabsichtigte Streitwertfestsetzung beruht auf folgenden Erwägungen:

1. Hinsichtlich der bezifferten Klageanträge ist der Streitwert auf insgesamt 5.000,- € anzusetzen. Hinzu kommen 500,- € für den Auskunfts- und weitere 500,- € für den Feststellungsanspruch.

Für den Unterlassungsantrag ist Streitwert von 500,- EUR anzusetzen. Für die Streitwertfestsetzung bei Unterlassungsansprüchen ist die Schwere des Vorwurfs, die Beeinträchtigung des Klägers, die wirtschaftliche Bedeutung sowie die sonstige Bedeutung der Sache einzubeziehen. Ausgangspunkt für die Bemessung sind die Werte des § 52 Abs. 2 GKG (5.000,00 EUR) und des § 23 Abs. 3 Satz 2 RVG (5.000,00 EUR), die nach Maßgabe des Einzelfalles zu erhöhen oder zu vermindern sind.

Eine Herabsetzung auf 500 EUR ist hier gerechtfertigt. Dem herabgesetzten Ansatz liegt zugrunde, dass sich dem klägerischen Sachvortrag keine Anhaltspunkte entnehmen lassen, welche konkreten Daten des Klägers infolge des behaupteten Datenlecks abhanden gekommen sein sollen. Auch die Email-Adressen des Klägers sind infolge der offenen API-Schnittstelle nicht „abgegriffen“ worden, sondern ermöglichten es vielmehr nur, seine Twitter-ID aufzufinden. Vor diesem Hintergrund ist von einer nur geringen Beeinträchtigung des Klägers auch in wirtschaftlicher Hinsicht auszugehen (vgl. Senat, Beschluss vom 14.05.2024, 4 U 184/24 n.v.).

S.....

Z.....

R.....