LG München I, Endurteil v. 09.02.2023 – 5 O 5853/22

Titel:

Umfang der Schutzmaßnahmen bei Datenverarbeitung

Normenkette:

DS-GVO Art. 5 Abs. 1 lit. f

Leitsatz:

Art. 5 Abs. 1 lit. f DS-GVO ergänzt den Aspekt der Vertraulichkeit, dass die Daten vor unbefugter und unrechtmäßiger Verarbeitung zu schützen sind durch geeignete technische und organisatorische Maßnahmen. Die konkret zu ergreifenden Schutzmaßnahmen hängen von der Bedeutung der Daten für die Rechte und Interessen der betroffenen Personen ab. (Rn. 39) (redaktioneller Leitsatz)

Schlagworte:

Datenschutz, Verarbeitung, Schutzmaßnahmen, VO (EU) 2016/679

Rechtsmittelinstanz:

LG München I, Berichtigungsbeschluss vom 14.03.2023 – 5 O 5853/22

Fundstellen:

LSK 2023, 20930

ZD 2024, 52

Tenor

1. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle materiellen künftigen Schäden zu ersetzen, die dem Kläger durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten im Zeitraum von April bis Oktober 2020 entstanden sind.

Im Übrigen wird die Klage abgewiesen.

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

3. Das Urteil ist vorläufig vollstreckbar. Der Kläger kann die Vollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110% des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110% des zu vollstreckenden Betrags leistet.

4. Der Streitwert wird auf 5.400,00 € festgesetzt.

Tatbestand

1
Die Parteien streiten über Schadensersatzansprüche aufgrund eines Datenlecks bei einem Finanzdienstleistungsunternehmen.

2
Die Beklagte ist ein 2014 gegründetes Wertpapierinstitut, das als sogenannter Robo-Advisor digitale Vermögensverwaltung anbietet. Der Kläger war bis November 2020 Kunde der Beklagten und unterhielt dort seit 09.08.2020 ein Wertpapierdepot. Im Rahmen der Authentifizierung und Anmeldung musste der Kläger gegenüber der Beklagten folgende personenbezogene Daten angeben: Vor- und Nachname, Anrede, Anschrift, E-Mail-Adresse, Handynummer, Geburtsdatum, Geburtsort, Geburtsland, Staatsangehörigkeit, Familienstand, Steuerliche Ansässigkeit, IBAN, Ausweiskopie, und ein im Post-Ident-Verfahren angefertigtes Portraitfoto (Anlage B7).

3
Am 15./16.04.2020, 05./06.08.2020 und 10./11.10.2020 ist es bei der Beklagten zu einem Zugriff auf personenbezogene Daten im digitalen Dokumentenarchiv gekommen, insgesamt wurden 389.000 Datensätze von 33.200 Kunden der Beklagten kopiert und entwendet. Der Zugriff auf die

personenbezogenen Daten erfolgte im Rahmen eines Hacker-Angriffs auf das Unternehmen (im Folgenden:)

4
Die Fa. ist ein IT-Unternehmen, das Cloud-Dienstleistungen anbietet. Die Beklagte nahm bis Ende 2015 Dienstleitungen von in Anspruch, daher waren bei Zugangsinformationen zum IT-System der Beklagten hinterlegt. Die Angreifer verschafften sich mithilfe dieser Zugangsdaten Zugriff auf einen Teil des Dokumentenarchivs der Beklagten und die darin befindlichen Kundendaten. Die Angreifer sind unbekannt, die Generalstaatsanwaltschaft Bamberg führt unter dem Az. ein Ermittlungsverfahren.

5
Die Beklagte hat die Zugangsdaten nach der Beendigung der Vertragsbeziehungen mit Ende 2015 bis zum streitgegenständlichen Vorfall nicht geändert.

6
Die Beklagte informierte den Kläger am 19.10.2020 von dem Vorfall und darüber, dass er von dem Datenleck betroffen ist (Anlage K2).

7
Die Prozessbevollmächtigten des Klägers forderten die Beklagte mit Schreiben vom 26.04.2022 auf, mitzuteilen, ob sie bereit sei, den dem Kläger durch den Zugriff auf seine Daten entstandenen immateriellen Schaden zu ersetzen (Anlage K4), was die Beklagte mit Schreiben ihrer Prozessbevollmächtigten vom 05.05.2020 ablehnte.

8
Der Kläger behauptet, dass auch Kontodaten und/oder Wertpapierdepotdaten sowie steuerliche Daten abgegriffen worden seien und die abgegriffenen Kundendaten, auch die des Klägers, im Darknet kursieren würden. Die Beklagte habe bereits am 15.10.2020 Kenntnis vom Datenvorfall erlangt.

9
Der Kläger ist der Ansicht, dass ihm gegen die Beklagte ein Anspruch auf immateriellen Schadensersatz zustehe, da die Beklagte gegen mehrere Vorschriften der DSGVO verstoßen habe. So habe es die Beklagte unterlassen, geeignete organisatorische Schutzmaßnahmen zu treffen, um einen Zugriff Dritter auf die Daten des Klägers zu verhindern, da sie die Zugangsdaten zu ihrem IT-System nach Beendigung der Vertragsbeziehungen mit der Fa. Ende 2015 nicht geändert und daher grob fahrlässig gegen Art. 32 Absatz 1 lit. b DSGVO verstoßen habe.

10
Zudem sei er nicht unverzüglich im Sinne des Art. 34 Abs. 1 DSGVO über die Verletzung seiner Datenschutzrechte informiert worden und die Mitteilung vom 19.10.2020 habe nicht die inhaltlichen Mindestangaben des Art. 33 Abs. 3 lit. b, c, d DSGVO erfüllt.

11
Dem Kläger sei aufgrund des Umfangs und der Art und Qualität der abgegriffenen personenbezogenen Daten seine Identität gestohlen worden, dieser Identitätsdiebstahl begründe bereits einen immateriellen Schaden. Ein immaterieller Schaden sei zudem eingetreten, weil der Kläger die Kontrolle darüber verloren habe, was zukünftig mit seinen Daten geschehe und zu welchem Zweck sie verwendet würden.

12
Es sei zudem davon auszugehen, dass es bei Einhaltung der als adäquat geltenden Sicherheitsmaßstäbe durch die Beklagte nicht zu dem konkreten Datenvorfall gekommen wäre.

13
Die Beklagte befinde sich seit dem 05.05.2020 in Verzug, weswegen sie die dem Kläger entstandenen außergerichtlichen Rechtsverfolgungskosten zu tragen habe.

14
Ein Feststellungsinteresse läge vor, da die Möglichkeit bestehe, dass weitere Schäden durch die Verwendung der illegal erlangten Daten entstehen würden.

15

Der Kläger beantragt,

1. Die Beklagte wird verurteilt, an die Klagepartei einen Betrag in Höhe von mindestens € 5.100,00 nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit Rechtshängigkeit zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klagepartei alle materiellen künftigen Schäden zu ersetzen, die der Klagepartei durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten im Zeitraum von April bis Oktober 2020 entstanden sind.

3. Die Beklagte wird verurteilt, der Klagepartei vorgerichtliche Anwaltskosten in Höhe von € 859,18 zu erstatten.

16
Die Beklagte beantragt,

die Klage abzuweisen Die Beklagte behauptet, sie habe nicht bereits am 15.10.2020, sondern erst am 16.10.2020 Kenntnis von dem Datenvorfall erlangt. Die Steueridentifikationsnummer des Klägers sei von dem Datenvorfall nicht betroffen gewesen, da der Kläger bei seiner Registrierung seine Steueridentifikationsnummer nicht angegeben habe. Ebenso wenig vom Datenvorfall betroffen seien die im Rahmen der Geeignetheitsprüfung erfassten Informationen des Klägers. Eine solche Geeignetheitsprüfung sei bei Registrierung des Klägers nicht erfolgt, weil diese für die vom Kläger in Anspruch genommene Dienstleistung des Brokerage nicht durchzuführen war.

17
Der Datenvorfall habe sich bereits 2020 zugetragen und die Daten des Klägers seien seitdem nicht missbraucht worden. Der Kläger trage auch nicht vor, dass er selbst Opfer etwaiger Betrugsversuche durch Cyberkriminelle im Nachgang zu dem Datenvorfall geworden sei, insbesondere habe er nach eigenen Angaben weder selbst Spamanrufe noch erpresserischen E-Mails erhalten.

18
Die Beklagte ist der Auffassung, dass dem Kläger weder ein materieller noch ein immaterieller Schaden entstanden sei. Die Daten des Klägers seien weder missbraucht worden noch liege ein Identitätsdiebstahl vor. Es fehle hierzu bereits an einem substantiierten Vortrag.

19
Die Beklagte habe zudem ausreichende technische und organisatorische Maßnahmen zur Gewährleistung einer angemessenen Datensicherheit implementiert, insbesondere sei die dem Dokumentenarchiv zugrundeliegende IT-Infrastruktur nach IEC 27001:2013, 27017:2015, 27018:2019, ISO/IEC 9001:2015 und CSA STAR CCM v3.0.1 zertifiziert.

20
Ein Schadensersatzanspruch könne von vornherein nicht auf eine vermeintliche Verletzung von Art. 34 DSGVO gestützt werden. Denn diese Norm falle nicht in den Schutzbereich des Art. 82 DSGVO.

21
Sie habe zudem davon ausgehen dürfen, dass die Firma die Zugangsinformationen vollständig und dauerhaft gelöscht habe, da die Firma verpflichtet gewesen sei, sich der zur Ausführung der Softwaredienstleistungen erhaltenen und nach Vertragsbeendigung nicht mehr benötigten Zugangsinformationen zu entledigen.

22
Es fehle selbst bei Vorliegen eines Schadens am Verschulden der Beklagten sowie der Kausalität.

23
Der Feststellungsantrag sei unzulässig, da es an einem Feststellungsinteresse fehle, zudem sei die Klage unzulässig, weil der Klageantrag zu Ziffer 1 nicht hinreichend bestimmt sei. Der Kläger mache einen einheitlichen Zahlungsantrag geltend, stütze das Begehren jedoch auf die vermeintliche Verletzung von Art. 34 DSGVO und Art. 32 DSGVO, womit der Klage zwei unterschiedliche Streitgegenstände zugrunde lägen.

24

Beide Parteien haben sich im Termin am 15.11.2022 mit einer Entscheidung im schriftlichen Verfahren einverstanden erklärt. Mit Beschluss vom 15.11.2022 wurde eine Entscheidung im schriftlichen Verfahren gern. § 128 Abs. 2 ZPO angeordnet (BI. 205 d.A.).

25
Zur Ergänzung des Tatbestandes wird auf die wechselseitigen Schriftsätze der Parteien samt Anlagen sowie das Protokoll der mündlichen Verhandlung vom 15.11.2022 (BI. 204/207 d.A.) Bezug genommen.

Entscheidungsgründe

A.

26
Die zulässige Klage ist überwiegend unbegründet.

27
I. Die Klage ist zulässig.

28
1. Das LG München I ist sachlich zuständig gemäß §§ 1 ZPO, 71 Abs. 1, 23 Nr. 1 GVG und örtlich zuständig gemäß §§ 44 Abs. 1 S. 1 BDSG, 12, 17 ZPO.

29
2. Der Klageantrag Ziffer 1 ist hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO.

30
Entgegen der Auffassung der Beklagtenpartei ist der Leistungsantrag nicht zu unbestimmt, da die angeblichen zwei DSGVO-Verstöße unterschiedliche Lebenssachverhalte darstellen und damit unterschiedliche Streitgegenstände und der Kläger daher hätte konkretisieren müssen, in welchem Verhältnis die Verstöße den Mindestbetrag von 5.100 € anteilig tragen sollen. Die geltend gemachten Verstöße, das Unterlassen des Treffens geeigneter Schutzmaßnahmen sowie eine unzureichende Benachrichtigung über den Datenvorfall, unterfallen nämlich dem gleichen Lebenssachverhalt, da jeweils dieselben Daten betroffen sind.

31
3. Hinsichtlich des Klageantrags Ziffer 2 ist auch ein Feststellungsinteresse des Klägers gemäß § 256 Abs. 1 ZPO gegeben.

32
Eine Klage auf Feststellung der deliktischen Verpflichtung eines Schädigers zum Ersatz künftiger Schäden ist zulässig, wenn die Möglichkeit eines Schadenseintritts besteht (OLG München 10 U 707/15, Rn. 4; Bacher, BeckOK ZPO, 47. Edition, Stand 01.12.2022, § 256 Rn. 24).

33
Diese Möglichkeit ist vorliegend gegeben, da die Angreifer immer noch Zugriff auf die Daten des Klägers haben. Dass dem Kläger seit dem Datenvorfall 2020 keine materiellen Schäden entstanden sind, vermag daran nichts zu ändern, da keine hinreichende Wahrscheinlichkeit eines Schadens erforderlich ist, sondern die immer noch bestehende Möglichkeit ausreicht. Dies wäre nur dann nicht gegeben, wenn aus Sicht des Klägers bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (BeckOK ZPO a.a.O.).

34
II. Die Klage ist jedoch nur teilweise begründet.

35
1. Der als Klageantrag 1 geltend gemachte Leistungsantrag steht dem Kläger nicht zu. Der Kläger hat gegen die Beklagte keinen Anspruch auf Zahlung von mindestens € 5.100,00 nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit Rechtshängigkeit. Ein solcher ergibt sich nicht aus Art. 82 Abs. 1 DSGVO, weitere Anspruchsgrundlagen sind vorliegend nicht ersichtlich.

36

Ein Anspruch auf immateriellen Schadensersatz gemäß Art. 82 Abs. 1 DSGVO scheidet aus. Die Beklagte hat zwar gegen die DSGVO verstoßen, dem Kläger ist dadurch jedoch kein Schaden entstanden.

37
a) Die Beklagte ist Verantwortliche im Sinne von Art. 82 Abs. 1,4 Nr. 7 DSGVO, da sie Kundendaten im Rahmen des Anmeldeprozesses abfragt und in einem Datenarchiv abspeichert.

38
b) Die Beklagte hat gegen Art. 32 Abs. 1 DSGVO verstoßen.

39
Art. 32 Abs. 1 DSGVO verpflichtet Verantwortliche, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten der von der Datenverarbeitung betroffenen Personen angemessenes Schutzniveau zu garantieren. Art. 5 Abs. 1 (f) DSGVO ergänzt den Aspekt der Vertraulichkeit, dass die Daten vor unbefugter und unrechtmäßiger Verarbeitung zu schützen sind durch geeignete technische und organisatorische Maßnahmen. Die konkret zu ergreifenden Schutzmaßnahmen hängen von der Bedeutung der Daten für die Rechte und Interessen der betroffenen Personen ab (Schantz in: BeckOK Datenschutzrecht, 42. Edition, 01.11.2021, Art. 5 Rn. 35).

40
(1) Dies hat die Beklagte unterlassen, indem sie die Zugangsdaten zu ihrem IT-System nach Beendigung der Vertragsbeziehungen mit der Fa. nicht geändert hat.

41
Die Beklagte hatte den Zugangsschlüssel zu ihrem Datenarchiv bei der Fa. gespei chert. Die gespeicherten personenbezogenen Daten, mithin auch die Daten des Klägers lagen und liegen in einem Dokumentenarchiv bei der Fa in Frankfurt a.M.. Die Vertragsbeziehung zur Fa. beendete die Beklagte Ende 2015. Die beim Kläger im Jahr 2020, d.h. über 4

42
Jahre nach Beendigung der Vertragsbeziehung Beklagte – erhobenen Daten wurden im Datenerarchiv gespeichert und dort mittels des bei der Fa. erlangten Zugangsschlüssels ausgelesen. Nach Beendigung der Vertragsbeziehung mit der Fa. hat die Beklagte den Zugangsschlüssel nicht geändert noch andere Schritte unternommen, dass der Zugangsschlüssel nicht mehr verwendet werden kann.

43
(2) Dadurch hat sie das Risiko aufrechterhalten, dass durch einen Hacker-Angriff auf die Fa. auch Daten ihrer Kunden abgegriffen werden können. Dieses Risiko hätte durch eine Abänderung der Zugangsdaten minimiert oder gar ausgeschlossen werden können.

44
(3) Da die Beklagte Verantwortliche im Sinne von Art. 32 Abs. 1,4 Nr. 7 DSGVO ist, hat sie sich nicht darauf verlassen dürfen, dass die Fa. die Zugangsinformationen löscht, unab hängig davon, ob diese dazu vertraglich verpflichtet war oder nicht.

45
Als Anbieterin von Online-Leistungen – der Vertragsabschluss mit dem Kläger erfolgte ausschließlich online – musste die Beklagte zudem wissen, dass Sicherheitskopien regelmäßig angefertigt werden, d.h. dass Daten letztlich nicht nur an einem einzigen Ort gespeichert werden. Ihr war damit bekannt, dass der Zugangsschlüssel sich auch in Sicherheitskopien der Fa. befinden könnte. Die Beklagte hat damit nicht die erforderliche Sorgfalt dafür aufgewendet, um sicherzustellen, dass der Zugangsschlüssel, der bei der Fa. lag, keiner weiteren Verwendung zugeführt wird (so auch LG Köln, 18.5.2022, 28 I 328/21). Allein das Vertrauen der Beklagten, dass sich die Fa. rechtstreu verhalten werde und damit ein Missbrauch des Zugangsschlüssels ausgeschlossen ist, reicht insbesondere vor dem Hintergrund der Sensibilität der erlangten, personenbezogenen Daten nicht aus, um ein ausreichendes Schutzniveau behaupten zu können. Entgegen Art. 5 DSGVO, der ein Ergreifen von Maßnahmen fordert, hat die Beklagte schlichtweg nichts getan, um nach Vertragsende mit der Fa. einem Daten missbrauch vorzubeugen, quasi so als hätte sie nach Beendigung eines Mietverhältnisses der Mieterin den Wohnungsschlüssel überlassen und sich nicht darum gekümmert, was damit passiert.

46

(4) Die Beklagte hat auch nicht hinreichend vorgetragen, warum die Abänderung der Zugangsdaten derart aufwändig gewesen wäre, dass dies im Verhältnis zu dem Risiko für die Rechte und Freiheiten ihrer Kunden nicht mehr angemessen gewesen wäre. Insbesondere wäre eine kurzzeitige Nichtverfügbarkeit der Dienste hinzunehmen gewesen.

47
(5) Hinzu kommt, dass die Beklagte durch ihr Verhalten die Datenmissbrauchsmöglichkeit über die Fa. über den ursprünglich gegebenen Umfang erweitert hat, hat sie doch die personenbezogenen Daten von Kunden, die erst nach Beendigung der Beziehung Beklagte - - akquiriert wurden, gleichfalls der Zugriffsmöglichkeit über den alten Zugangsschlüssel zugeführt. Es fehlt insoweit auch an einer wirksamen Einwilligung in die Datenverarbeitung nach Art. 6 DSVGO, da der Kläger nicht einmal darüber informiert worden war, dass seine Daten über die Fa. als eine Dritte, die in die Vertragsbeziehungen weder mit ihm noch mit der Beklagten eingebunden gewesen war, zugänglich seien. Dass der Zugangsschüssel bei der Fa. noch vorhanden sein könnte, musste der Beklagten bewusst sein (s.o.).

48
(6) Da die Beklagte ihre eigenen Pflichten aus Art. 32 Abs. 1 DSGVO verletzt hat, kann dahinstehen, ob ihr überdies ein etwaiger Verstoß der Fa. zuzurechnen ist.

49
c) Die Beklagte hat hingegen nicht gegen Art. 34 DSGVO verstoßen.

50
aa) Die Beklagte hat den Kläger unverzüglich im Sinne von Art. 34 Abs. 1 DSGVO über den Datenvorfall informiert.

51
(1) Anders als Art. 33 DSGVO, wonach die Meldung an die Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden ab Kenntnisnahme zu erfolgen hat, enthält Art. 34 Abs. 1 DSGVO keine Nennung eines Zeitrahmens, sondern verlangt nur, dass der Verantwortliche die betroffene Person unverzüglich von der Verletzung informiert. Für eine rechtzeitige Information im Sinne von Art. 34 Abs. 1 DSGVO gilt also nicht grundsätzlich, dass diese zwingend innerhalb von 72 Stunden ab Kenntnisnahme zu erfolgen hat.

52
(2) Die Beklagte hat den Kläger am 19.10.2020 ohne schuldhaftes Zögern und damit unverzüglich im Sinne von § 121 Abs. 1 BGB über den Datenvorfall informiert. Dies gilt unabhängig davon, ob die Beklagte bereits am 15.10.2020 oder erst am 16.10.2020 Kenntnis von dem Datenvorfall erlangt hat.

53
(3) Dem Verantwortlichen muss ein Zeitraum eingeräumt werden, indem er die Reich- und Tragweite des Vorfalls ermitteln kann, schließlich bedarf es eines gewissen Kenntnisstands, damit die Benachrichtigung den inhaltlichen Anforderungen des Art. 34 Abs. 2 DSGVO genügen kann. Stellte man zu strenge Anforderungen an die Unverzüglichkeit im Rahmen des Art. 34 Abs. 1 DSGVO, liefe dies dem Ziel einer den vom dem Datenvorfall Betroffenen Aufschluss verschaffenden Information entgegen. Insbesondere ist auch zu berücksichtigen, dass der 17. und 18.10.2020 auf ein Wochenende fielen, was es der Beklagten erschwert haben dürfte, nähere Informationen zu dem Datenvorfall in Erfahrung zu bringen.

54
bb) Die Information genügte auch den inhaltlichen Anforderungen der Art. 34 Abs. 2, Art. 33 Abs. 3 lit. b, c, d DSGVO.

55
(1) Die Benachrichtigung vom 19.10.2020 war zwar recht knapp gehalten, dennoch enthielt sie alle gesetzlich vorgeschriebenen Inhalte.

56
(2) Den sich aus Art. 34 Abs. 2 DSGVO ergebenden inhaltlichen Informationen wurden durch eine kurze Beschreibung des Ablaufs des Datenvorfalls und damit einer Nennung der Art der Verletzung personenbezogener Daten entsprochen.

57

(3) Auch die nach Art. 34 Abs. 2, 33 Abs. 3 lit. b, c, d DSGVO erforderlichen Inhalte waren enthalten.

58
(a) Das Kundenservice-Team der Beklagten wurde unter Nennung der Kontaktdaten als Anlaufstelle für weitere Informationen im Sinne von Art. 33 Abs. 3 lit. b DSGVO benannt.

59
(b) Die Beklagte hat den Kläger auch im Sinne von Art. 33 Abs. 3 lit. c DSGVO über die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten informiert, indem kurz beschrieben wurde, dass Betroffene zur Preisgabe von weiteren vertraulichen Informationen oder Zahlung veranlasst werden könnten und die Möglichkeit eines Indentitätsmissbrauchs angesprochen wurde.

60
(c) Auch hat die Beklagte eine weitere Untersuchung des Sachverhaltes sowie die Hinzuziehung von externen Beratern als von ihr ergriffenen Maßnahmen beschrieben und den Betroffenen geraten, keine persönlichen Zugangsdaten per E-Mail oder Telefon preiszugeben und damit den Anforderungen des Art. 33 Abs. 3 lit. d DSGVO genüge getan.

61
cc) Überdies hat der Kläger nicht substantiiert vorgetragen, inwiefern der von ihm behauptete Schaden durch eine Art. 34 DSGVO in zeitlicher und inhaltlicher Hinsicht entsprechenden Benachrichtigung entfallen wäre. Eine Verletzung von Art. 34 DSGVO wäre damit auch gar nicht kausal für einen etwaigen Schaden gewesen.

62
(d) Dem Kläger ist jedoch durch den Datenvorfall weder ein materieller noch ein immaterieller Schaden im Sinne des Art. 82 Abs. 1 DSGVO entstanden.

63
Für den Schadenseintritt ist die Klägerseite beweisbelastet, die einen konkret erlittenen Schaden im Rahmen des Schadensersatzanspruches darzulegen und zu beweisen hat (OLG Frankfurt a.M., 2.3.2022, 13 U 206/20; LG Köln, 16.2.2022, 28 I 303/20).

64
aa) Der Kläger hat nicht substantiiert vorgetragen, dass er selbst Beeinträchtigungen erlitten habe, die über ein unkonkretes Gefühl des Kontrollverlustes über seine Daten hinausgingen. Insbesondere gelang es ihm nicht substantiiert vorzutragen, dass es zu einem Missbrauch seiner Daten kam oder dass seine Daten im Darknet angeboten worden seien.

65
bb) Damit weicht der vorliegende Sachverhalt von den vom Kläger zitierten Urteilen (z.B. LG München I, Endurteil vom 23.06.2022 -50 3768/22; LG München I, Endurteil vom 09.12.2021 – 31 O 16606/20), die anderen Klägern gegen dieselbe Beklagte – (deutlich) geringere als die vom Kläger beantragten – Schadensersatzzahlungen zusprachen, ab. Bei den zitierten Urteilen lag jeweils ein Sachverhalt zugrunde, bei dem es der klagenden Partei gelungen war, erlittene Beeinträchtigungen vorzutragen und zu beweisen.

66
cc) Dass andere von dem Datenvorfall betroffene Personen einen Schaden erlitten haben, beispielsweise durch das Erhalten von Spam-E-Mails, kann keinen Schaden des Klägers begründen, da es an einem eigenen erlittenen Nachteil fehlt.

67
dd) Entgegen der Auffassung des Klägers kann ein Schaden auch nicht bereits wegen des Verstoßes der Beklagten gegen Art. 32 DSGVO angenommen werden, mit der Begründung, dass bereits der Verstoß gegen die DSGVO an sich einen Schaden im Sinne von Art. 82 Abs. 1 DSGO begründe.

68
(1) Diese Auffassung ist mit dem Wortlaut des Art. 82 Abs. 1 DSGVO nicht vereinbar. Nach dem Wortlaut besteht ein Schadensersatzanspruch, wenn einer Person wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist; das Vorliegen eines Verstoßes gegen die DSGVO und der daraus entstandene Schaden sind folglich zwei unterschiedliche Tatbestandsmerkmale. Wenn jeder

Verstoß gegen die DSGVO an sich bereits einen Schaden und damit einen Anspruch auf Schadensersatz begründen würde, wäre es überflüssig, dass Art. 82 Abs. 1 DSGVO das Vorliegen eines Schadens als Voraussetzung für den Schaderisersatzanspruch nennt. Der Schaden ist somit nicht mit der zugrundeliegenden Rechtsgutsverletzung gleichzusetzen. Denn ausdrücklich muss der Schaden „erlitten“ werden, woraus folgt, dass dieser tatsächlich entstanden sein muss und nicht lediglich befürchtet wird (BeckOK, Datenschutzrecht, 42. Edition, 01.08.22, Art. 82 DSGVO Rn. 23). Es bedarf somit des Nachweises eines konkreten (auch immateriellen) Schadens (OLG Frankfurt a.M., Urt. v. 02.03.2022, 13 U 206/20).

69
(2) Zudem würde diese Auffassung Verantwortliche im Sinne der DSGVO unbillig belasten.

70
Der vorliegende Fall zeigt, dass bei einem Datenleck bei großen Unternehmen eine Vielzahl von Personen – hier 33.200 Kunden – betroffen sein kann. Würde jeder dieser Person bereits wegen eines Verstoßes gegen die DSGVO ein Schadensersatz in fünfstelliger Höhe zustehen, ohne dass die Betroffenen konkrete Beeinträchtigungen erlitten haben müssen, würde dies für Unternehmen möglicherweise existenzbedrohende Zahlungsverpflichtungen nach sich ziehen, obwohl die Beeinträchtigungen der Rechte ihrer Kunden als eher gering einzustufen sind.

71
(3) Das Vorliegen eines konkreten immateriellen Schadens, wozu auch Ängste, Stress sowie Komfort- und Zeiteinbußen zählen (OLG Frankfurt a. M., Urt. v. 02.03.2022, 13 U 206/20 mit Verweis auf Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18 b), hat der Kläger nicht dargetan, obwohl die Beklagte bereits mit Schriftsatz vom 16.09.2022 explizit darauf hinwies, dass es hierzu an einem substantiierten Vortrag des Klägers fehle.

72
Die darauffolgenden Ausführungen der Klagepartei beispielsweise im Schriftsatz vom 08.11.2022 erschöpfen sich in allgemeinen Ausführungen darin, worin unter Umständen ein Schaden zu verstehen wäre. Ein konkreter Vortrag zu konkreten, individuellen Beeinträchtigungen des hiesigen Klägers erfolgten jedoch nicht.

73
Auch in der Klageschrift hatte die Klagepartei nur unsubstantiiert vorgetragen, dass die Daten der Klagepartei dadurch missbraucht worden seien, dass die Klagepartei wiederholt Opfer von Phishing SMSen und betrügerischen Telefonanrufen wurde (Bl. 27 d.A.).

74
Das Gericht beabsichtigte zunächst den Kläger hierzu informatorisch anzuhören, wie es auch später klägerseits auf Seite 38 und 39 des Schriftsatzes vom 08.11.2022 (Bl. 157/158 d.A.) beantragt wurde, weshalb mit Terminverfügung vom 20.07.2022 (Bl. 43/44 d.A.) das persönliche Erscheinen des Klägers angeordnet wurde. Aufgrund des Antrags der Klagepartei mit Schriftsatz vom 10.08.2022 (Bl. 45/46 d.A.), wonach der Kläger zu 100% schwerbehindert sei und es ihm deshalb nicht möglich sei, zum Termin zu erscheinen, wurde der Kläger jedoch mit Verfügung vom 11.08.2022 vom persönlichen Erscheinen entbunden, wobei das Erscheinen eines informierten Vertreters weiterhin angeordnet blieb (Bl. 47 d.A.). Nachfragen des Gerichts im Termin unter anderem zu den klägerischen Ausführungen auf Bl. 27 d.A. konnte die erschiene Klägervertreterin nicht beantworten und auch eine Nachfrage bei dem Kläger selbst blieb erfolglos (Bl. 205 d.A.).

75
Auch im Rahmen des nachgelassenen Schriftsatzes vom 06.12.2022 erfolgte kein weiterer substantiierter Vortrag zu individuell durch den Kläger erlittenen Beeinträchtigungen.

76
2. Der Feststellungsantrag ist begründet, Art. 82 Abs. 1 DSGVO.

77
a) Die Beklagte hat gegen Art. 32 DSGVO verstoßen.

78

b) Erleidet der Kläger in Zukunft materielle Schäden durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, die damit kausal zu dem Verstoß der Beklagten gegen Art. 32 DSGVO sind, so steht ihm gegen die Beklagte ein Schadensersatzanspruch gemäß Art. 82 Abs. 1 DSGVO zu.

79
c) Die Möglichkeit des Eintritts materieller Schäden besteht, da die Daten des Klägers noch immer „verloren“ sind und damit potenziell missbraucht werden könnten. Auch wenn der Datenabgriff bereits im Jahr 2020 stattfand, ist unter dem Gesichtspunkt „Das Internet vergisst nicht“ nicht ansatzweise ausgeschlossen, dass die personenbezogenen Daten des Klägers, die über den Datenvorfall erlangt wurden, in Zukunft zu einem Schaden bei diesem führen. Der eingetretene Datenverlust betrifft einen nicht unerheblichen Bestandteil an personenbezogenen Daten des Klägers.

80
3. Der Kläger hat mangels bestehender Zahlungsverpflichtung der Beklagten gegen diese keinen Anspruch auf Erstattung vorgerichtlicher Anwaltskosten in Höhe von € 859,28, da bereits kein Verzug der Beklagten im Sinne von § 286 BGB eingetreten ist. Der Feststellungsantrag wurde in dem Rechtsanwaltsschreiben vom 26.04.2022 (Anlage K4) nicht geltend gemacht, so dass dieses Schreiben nicht bereits dessen Vorbereitung diente.

81
111. Da es sich vorliegend nicht um ein letztinstanzliches Urteil handelt, war eine Vorlage zum Zweck der Vorabentscheidung an den EuGH gemäß Art. 267 Abs. 3 AEUV nicht, wie von der Beklagten beantragt, erforderlich.

B.

82
Die Kostenentscheidung ergibt sich aus § 92 Abs. 2 Nr. 2 ZPO. Der Kläger obsiegt nur hinsichtlich des Feststellungsantrags, welcher mit 300 € bemessen wurde, wohingegen er mit seinem Leistungsantrag i.H.v. 5.100 € nicht durchdringt, so dass er nur in Höhe von 6% obsiegt.

C.

83
Die Entscheidung über die vorläufige Vollstreckbarkeit richtet sich nach §§ 708 Nr.11,711 ZPO.

D.

84
Der Streitwertbeschluss ergibt sich aus § 48 GKG i.V.m. §§ 3, 5 ZPO. Zu dem bezifferten Klageantrag Nr. 1 wurde für den Feststellungsantrag ein Betrag von 300 € addiert, welcher sich im Wege der Schätzung ergab.