LG München I, Endurteil v. 09.03.2023 – 4 O 6009/22

Titel:

Schadensersatzbegehren nach unbefugtem Zugriff Dritter auf personenbezogene Daten

Normenkette:

DSGVO Art. 32, Art. 82

Leitsätze:

1. Werden die Zugangsdaten zu einem Datenarchiv nach Beendigung der Vertragsbeziehung zu einem IT-Dienstleister (hier: Cloud-Dienstleistungen) nicht geändert, sind die betroffenen Daten nicht angemessen vor einer unbefugten oder unrechtmäßigen Verarbeitung geschützt. (Rn. 40) (redaktioneller Leitsatz)
2. Ein Antrag auf Feststellung einer Ersatzpflicht für etwaige künftige materielle Schäden auf Grund von Daten-Scraping ist begründet, wenn die Möglichkeit des Eintritts materieller Schäden besteht und nicht gänzlich auszuschließen ist, weil die Daten des Betroffenen noch immer „verloren" sind und damit potenziell missbraucht werden können. (Rn. 43) (redaktioneller Leitsatz)

Schlagworte:

Schadensersatz, Schadensersatzanspruch, Schaden, Verletzung, Feststellungsinteresse, Daten, Rechtsanwaltskosten, Beendigung, Klage, Anspruch, Unternehmen, Anlage, Anwaltskosten, Missbrauch, immaterieller Schaden, personenbezogene Daten, vorgerichtliche Anwaltskosten

Fundstelle:

GRUR-RS 2023, 20934

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. Von den Kosten des Rechtsstreits trägt der Kläger 84 %, die Beklagte 16 %.

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

Beschluss

Der Streitwert wird auf 6.100,00 € festgesetzt.

Tatbestand

1
Die Parteien streiten um Schadensersatz nach einem Abgriff von Daten des Klägers (DSGVO-Verstoß).

2
Die Beklagte ist ein 2014 gegründetes Wertpapierinstitut, das als sogenannter Robo-Advisor digitale Vermögensverwaltung anbietet. Der Kläger ist Kunde der Beklagten und unterhält dort seit dem 22.12.2016 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.

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: …). Welche Daten speziell des Klägers hiervon genau betroffen waren, ist zwischen den Parteien streitig.

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 hatte die Zugangsdaten nach der Beendigung der Vertragsbeziehungen mit … Ende 2015 bis zum streitgegenständlichen Vorfall nicht geändert.

6
Die Beklagte informierte den Kläger mit einem Standardanschreiben vom 19.10.2020 von dem Vorfall und darüber, dass er von dem Datenleck betroffen ist (Anlage K 2).

7
Die Prozessbevollmächtigten des Klägers forderten die Beklagte mit Schreiben vom 05.04.2022 auf, mitzuteilen, ob sie bereit sei, den dem Kläger durch den Zugriff auf seine Daten entstandenen immateriellen Schaden zu ersetzen (Anlage K 5), was die Beklagte mit Schreiben ihrer Prozessbevollmächtigten vom 13.04.2022 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. Es sei offenkundig, dass die Täter mit gestohlenen Kundendaten versucht hätten, Kredite zu erlangen. Die Beklagte habe bereits am 15.10.2020 Kenntnis vom Datenvorfall erlangt. Es sei zudem davon auszugehen, dass es bei Einhaltung der als adäquat geltenden Sicherheitsmaßstäbe durch die Beklagte nicht zu dem konkreten Datenvorfall gekommen wäre.

9
Der Kläger bringt vor, ihm sei aufgrund des Umfangs und der Art und Qualität der abgegriffenen personenbezogenen Daten seine Identität gestohlen worden. Ihm drohten daraus materielle Schäden (Verweis des Klägers auf Schreiben der Schufa vom 27.11.2020 Anlage K 4). Er sei seit dem Datenleck vermehrt Opfer von Betrugsversuchen via Phishing-Angriffen und Spam-Mails geworden.

10
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. 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
Der Kläger ist der Ansicht, der 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
Der Kläger ist ferner der Rechtsauffassung, ein Feststellungsinteresse läge vor, da die Möglichkeit bestehe, dass weitere Schäden durch die Verwendung der illegal erlangten Daten entstehen würden.

13
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 € 719,95 zu erstatten.

14
Die Beklagte beantragt,

die Klage abzuweisen

15
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. Der Datenvorfall habe sich bereits 2020 zugetragen und die Daten des Klägers seien seitdem nicht missbraucht worden. Der Kläger trage auch nicht konkret 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. Daten des Klägers seien zudem auch an anderer Stelle abgegriffen worden (Verweis der Beklagten auf Internetauskunft Anlage B 7).

16
Die Beklagte bringt weiter vor, sie habe 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. Eine Pflicht zur regelmäßigen Änderung von Zugangsinformationen bestehe nicht. Eine derartige „Rotation“ sei auch mit Nachteilen behaftet.

17
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 substantiiertem Vortrag. Die Beklagte habe zudem ausreichende technische und organisatorische Maßnahmen zur Gewährleistung einer angemessenen Datensicherheit implementiert.

18
Die Beklagte meint weiter, 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. Es fehle selbst bei Vorliegen eines Schadens am Verschulden der Beklagten sowie der Kausalität.

19
Die Beklagte ist der Rechtsansicht, 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.

20
Zur Ergänzung des Sachverhalts wird Bezug genommen auf die gewechselten Schriftsätze der Parteien nebst Anlagen sowie das Protokoll über die mündliche Verhandlung vom 12.01.2023.

Entscheidungsgründe

21
Die zulässige Klage ist nur teilweise begründet.

22
A. Die Klage ist zulässig.

23
1. Der Klageantrag Ziffer 1 ist hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO.

24
Entgegen der Auffassung der Beklagten ist der Leistungsantrag nicht deswegen zu unbestimmt, da die behaupteten zwei DSGVO-Verstöße unterschiedliche Lebenssachverhalte darstellten und damit unterschiedliche Streitgegenstände und der Kläger daher konkretisieren hätte 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.

25
2. Hinsichtlich des Klageantrags Ziffer 2 ist auch ein Feststellungsinteresse des Klägers gemäß § 256 Abs. 1 ZPO gegeben.

26
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).

27
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.). Eine solche Konstellation liegt hier aber nicht vor.

28
Unerheblich für die Zulässigkeit (und auch die Begründetheit) des Feststellungsantrags ist ferner, ob dem Kläger in einem etwaigen Bezifferungsprozess es tatsächlich gelänge, etwaig eingetretene Schäden als adäquat kausale Folge des Datenabgriffs zu beweisen. Eine solche Frage wäre in einem etwaigen späteren Bezifferungsprozess zu entscheiden.

29
B. Die Klage ist jedoch nur in Teilen begründet.

30
I. Der Kläger hat gegen die Beklagte keinen Anspruch auf Zahlung eines Betrags in Höhe von 5.100 € als Schadensersatz bzw. eines niedrigeren oder höheren Betrags aus demselben Rechtsgrund.

31
Es fehlt jedenfalls an einem nachgewiesenen materiellen oder immateriellen Schaden des Klägers im Sinne von Art. 82 DSGVO. Für den Schadenseintritt ist der Kläger beweisbelastet (OLG Frankfurt a.M., 02.03.2022, 13 U 206/20; LG Köln, 16.02.2022, 28 I 303/20).

32
Hierzu hat die 5. Zivilkammer des Landgerichts München in ihrem Urteil vom 09.02.2023, Az.: 5 O 5853/22, ausgeführt was folgt:

„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.

bb) Damit weicht der vorliegende Sachverhalt von den vom Kläger zitierten Urteilen (z.B. LG München I, Endurteil vom 23.06.2022 – 5 O 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.

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.

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.

(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 überfüssig, dass Art. 82 Abs. 1 DSGVO das Vorliegen eines Schadens als Voraussetzung für den Schadensersatzanspruch 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).

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

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.“

33
Dem ist seitens des Unterzeichners beizutreten. Der Sachvortrag des Klägers zu den durch ihn erlittenen Beeinträchtigungen erschöpft sich in Allgemeinplätzen. Diese werden in weitgehend identischer Form durch die Prozessbevollmächtigten des Klägers in einer Vielzahl von Schriftsätzen in gleicher Form vorgetragen. So heißt es in der Klageschrift S. 8, der Kläger sei bereits vermehrt Opfer von Betrugsversuchen geworden. Einen Satz später heißt es weiter, der Kläger sei bereits vermehrt Opfer von Betrugsversuchen via Phishing Angriffen und Spam Mails geworden. Wenn es konkrete Phishing-Angriffe auf den Kläger gegeben hätte, so wäre es dem Kläger möglich gewesen, hierzu konkret vorzutragen, was nicht erfolgt ist. Hierzu angehört werden konnte der Kläger nicht, da er zum Termin zur mündlichen Verhandlung nicht erschienen ist. Zudem würde sich selbst für den Fall tatsächlicher Phishing-Angriffe das Problem stellen, ob diese tatsächlich ursächlich auf den hier gegenständlichen Datenschutzvorfall zurückzuführen sind. Phising-Angriffe kommen mittlerweile häufig vor. Auch der Unterzeichner war bereits mit solchen Angriffen konfrontiert, etwa dass vermeintlich Passwörter oder Accounts bei Paypal oder Amazon „bestätigt“ werden sollten. Vom Datenschutzvorfall bei der Beklagten war der Unterzeichner hingegen schon mangels Konto dort nicht betroffen. Mithin sind die meisten Internetnutzer mit derartigen Angriffen konfrontiert. Gleiches gilt für Spam-Mails, die wohl jeder Nutzer des Internets in großer Zahl erhält. Zudem ist zu berücksichtigen, dass nach der Internet-Auskunft Anlage B 7 persönliche Daten des Klägers auch bei anderen Datenschutzvorfällen abgegriffen wurden.

34
Unabhängig von diesen Erwägungen erachtet es das Gericht auch für äußerst unwahrscheinlich, dass alle Kunden der Beklagten, die von dem Datenschutzvorfall betroffen waren, die genau gleichen Ängste hatten oder in gleicher Weise mit aus dem Vorfall resultierenden Problemen konfrontiert waren. Der identische

Sachvortrag dazu dürfte eher auf einer Arbeitsökonomisierung der Prozessbevollmächtigten des Klägers, die gerichtsbekannt zahlreiche Kläger gegen die Beklagte vertreten, beruhen. Zuletzt gab auch die im Termin für den Kläger anwesende Rechtsanwältin an, ihr seien über die vorgetragenen Beeinträchtigungen hinaus keine konkreten Beeinträchtigungen bekannt.

35
Anzufügen ist noch, dass nach zutreffender Auffassung der bloße DSGVO-Verstoß selber noch nicht zu einem Ersatzanspruch nach Art. 82 DSGVO führt. Eine abweichende Auffassung würde den Begriff des Schadens sowie von „Schadensersatz“ in Art. 82 Abs. 1 DSGVO ad absurdum führen. Auch reicht ein bloßer Kontrollverlust über Daten führt einen Ersatzanspruch nicht aus (Paal, Höhe des Ersatzes immaterieller Schäden nach Art. 82 DSGVO, NJW 2022, 3673).

36
II. Anspruch auf Zinsen aus dem Zahlungsbetrag hat der Kläger mangels Anspruchs in der Hauptsache nicht.

37
III. Hingegen hat der Kläger Anspruch auf Feststellung der grundsätzlichen Ersatzpflicht für zukünftige Schäden, welche aus dem Datenschutzvorfall bei der Beklagten resultieren. Der entsprechende Anspruch ergibt sich aus Art. 82 DSGVO.

38
1. 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.

39
2. Die Beklagte hat gegen Art. 32 Abs. 1 DSGVO verstoßen.

40
Hierzu hat die 5. Zivilkammer des Landgerichts München I in ihrem Urteil vom 09.02.2023, Az.: 5 O 5853/22, ausgeführt:

„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).

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

Die Beklagte hatte den Zugangsschlüssel zu ihrem Datenarchiv bei der Fa. … gespeichert. 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 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.

(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.

(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, unabhängig davon, ob diese dazu vertraglich verpflichtet war oder nicht.

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 Datenmissbrauch vorzubeugen, quasi so als hätte sie nach Beendigung eines Mietverhältnisses der Mieterin den Wohnungsschlüssel überlassen und sich nicht darum gekümmert, was damit passiert.

(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.

(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. CodeShip 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.).

(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.“

41
Dem ist seitens des Unterzeichners beizutreten. Ergänzend ist seitens des Gerichts anzuführen, dass es für die unterbliebene Änderung der Zugangsdaten auch jeglichen nachvollziehbaren Grundes fehlte. Ganz offensichtlich hat sich die Beklagte darauf verlassen, dass sich die Fa. … vertragsgemäß verhalte. Möglicherweise war dies im Grundsatz auch der Fall, doch wie der vorliegende Fall zeigt, kann es immer Kopien vorhandener Daten auf Sicherungsservern geben. Schon weil die Beklagte hierauf keinerlei Einfluss hatte, hätte sie die Zugangsdaten ändern müssen. Dabei ist auch unerheblich, ob es technische Standards dahingehend gibt, dass Zugangsdaten regelmäßig zu ändern seien. Eine solche Änderung war hier nach der Beendigung der Vertragsbeziehung derart naheliegend, dass sich die Beklagte nicht darauf berufen kann, es gäbe keine Standards, die eine solche Änderung vorschrieben.

42
3. Das Verschulden der Beklagten ist ebenfalls gegeben, weil die Beklagte gehalten gewesen wäre, die Zugangsdaten nach Kündigung der Vertragsbeziehung mit der Fa. … zu verändern, was sie aber bewusst nicht getan hat.

43
4. Die grundsätzliche 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. Für den Feststellungsantrag ist hingegen unerheblich, ob dem Kläger in einem etwaigen späteren Bezifferungsprozess tatsächlich der Nachweis gelingen würde, dass ihm entstandene Schäden gerade auf das Datenleck bei der Beklagten zurückzuführen sind.

C.

44
Anspruch auf vorgerichtliche Rechtsanwaltskosten hat der Kläger nicht. Die Beklagte befand sich nicht im Verzug mit einer Erklärung zu ihrer Haftung, als der Kläger seine nunmehrigen Prozessbevollmächtigten einschaltete. Vielmehr stammte bereits das erste Anschreiben an die Beklagte von den nunmehrigen Prozessbevollmächtigten, so dass die Kosten der Einschaltung der Prozessbevollmächtigten jedenfalls nicht verzugskausal sind.

45
Im Anspruchsschreiben Anlage K5 wird zudem gar kein Feststellungsantrag geltend gemacht, so dass auch unter dem Gesichtspunkt von §§ 280 Abs. 1, 249 BGB auch ein Teilbetrag für die vorgerichtlichen Rechtsanwaltskosten nicht zuzusprechen war.

D.

46
I. Die Entscheidung über die Kosten erfolgte nach § 92 Abs. 1 ZPO.

47
II. Über die vorläufige Vollstreckbarkeit war für beide Parteien nach §§ 708 Nr. 11, 711 ZPO zu entscheiden.

48
III. Der Streitwert wurde auf 6.100 € festgesetzt. Maßgeblich ist insoweit der mit Ziff. 1 der Klageanträge geforderte Betrag von 5.100 €. Hinzu tritt ein Betrag für den Feststellungsantrag hinsichtlich zukünftiger Schäden. Dieser ist auch wirtschaftlich nicht identisch mit dem Zahlungsantrag, weshalb der Streitwertangabe des Klägers nicht gefolgt werden konnte. Mangels näherer Angaben der Parteien sowie Anhaltspunkt für eine konkrete Bemessung geht das Gericht von einem Betrag in Höhe von 1.000 € aus.