LG München I, Endurteil v. 23.03.2023 – 26 O 1859/22

Titel:

Schadensersatzbegehren nach unbefugtem Zugriff Dritter auf personenbezogene Daten

Normenketten:

DSGVO Art. 5, Art. 32, Art. 34, Art. 82

ZPO § 256

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. 32 – 36) (redaktioneller Leitsatz)

2. Ein Schaden kann nicht allein wegen des Verstoßes gegen Art. 32 DSGVO mit der Begründung angenommen werden, dass bereits der Verstoß gegen die DSGVO an sich einen Schaden im Sinne von Art. 82 Abs. 1 DSGO begründe. (Rn. 44) (redaktioneller Leitsatz)

3. 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. 50 – 51) (redaktioneller Leitsatz)

Schlagworte:

Vermögensverwaltung, personenbezogene Daten, Cloud, immaterieller Schaden

Rechtsmittelinstanzen:

OLG München, Beschluss vom 16.08.2023 – 31 U 1786/23 e

OLG München, Beschluss vom 13.12.2023 – 31 U 1786/23 e

Fundstellen:

ZD 2024, 50

LSK 2023, 20935

Tenor

1. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle materiellen künftigen Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten am 05./06.08.2020 und am 10./11.10.2020 entstanden sind.

2. Im Übrigen wird die Klage abgewiesen.

3. Die Kosten des Rechtsstreits trägt der Kläger.

4. Das Urteil ist für die Beklagte – hinsichtlich der Kosten – gegen Sicherheitsleistung in Höhe von 110 % des zu vollstreckenden Betrages vorläufig vollstreckbar.

Tatbestand

1

Der Kläger begehrt von der Beklagten immateriellen Schadensersatz aus Art. 82 I DSGVO und Feststellung der Haftung bezüglich künftiger Schäden aufgrund eines sog. Datenvorfalls.

2

Die Beklagte ist ein Wertpapierinstitut mit Sitz in München und bietet u.a. als sog. „Robo-Advisor“ ihrer Kundschaft eine digitale Vermögensverwaltung an. Der Kläger ist seit dem 19.06.2020 Kunde der Beklagten und hat ihr im Rahmen der Vertragsbeziehungen folgende personenbezogene Daten anvertraut: Vor- und Nachname, Anrede, Anschrift, E-Mail-Adresse, Handynummer, Geburtsdatum, Geburtsort und Geburtsland, Staatsangehörigkeit, Familienstand, steuerliche Ansässigkeit und Steuer-ID, IBAN, Ausweiskopie sowie Portraitfoto.

3
Am 15./16.04.2020, 05./06.08.2020 und am 10./11.10.2020 kam es bei der Beklagten jeweils zu einem unbefugten Zugriff Dritter auf elektronisch gespeicherte, personenbezogene Daten im digitalen Dokumentenarchiv; insgesamt wurden aus einem Teil des Dokumentenarchivs 389.000 Datensätze von 33.200 Kunden kopiert und entwendet. Der Zugriff erfolgte mittels Zugangsdaten zum System der Beklagten, die die Angreifer im Rahmen eines Angriffs auf einen ehemaligen Vertragspartner der Beklagten, die Firma … (im Folgenden: …), erlangt hatten.

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 Beklagte hatte diese Zugangsdaten nach Ende der Vertragsbeziehungen im Jahr 2015 bis zum streitgegenständlichen Datenvorfall nicht geändert. 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. Nach dem streitgegenständlichen Datenvorfall änderte die Beklagte die Zugangsinformationen.

5
Am 19.10.2020 wurde der Kläger durch die Beklagte informiert, dass er von dem Datenvorfall betroffen ist. Dabei wurde ihm mitgeteilt, dass Vor- und Nachname, Anrede, Anschrift, E-Mail-Adresse, Handynummer, Geburtsdatum, Geburtsort und Geburtsland, Staatsangehörigkeit, Familienstand, steuerliche Ansässigkeit, IBAN, Ausweiskopie sowie ein Portraitfoto des Klägers entwendet wurden.

6
Die Beklagte bot den betroffenen Kunden – so auch dem Kläger – sowohl ein einjähriges Abonnement „SchufaPlus“ zur Überwachung der eigenen Finanzdaten an als auch die Übernahme der Kosten für einen neuen Personalausweis. Der Kläger nahm das Angebot für „SchufaPlus“ an.

7
Mit anwaltlichem Schreiben vom 17.09.2021 ließ der Kläger die Beklagte u.a. zur Mitteilung auffordern, ob die Beklagte bereit sei, den dem Kläger durch den Zugriff auf seine Daten entstandenen immateriellen Schaden zu ersetzen (Anlage K7). Das lehnte die Beklagte ab.

8
Unstreitig waren personenbezogene Daten des Klägers, u.a. seine E-Mail-Adresse und seine Telefonnummer, auch bei anderen, rechtswidrigen Datenabgriffen betroffen, wie aus der Anlage B8 ersichtlich.

9
Der Kläger trägt vor, dass die Beklagte nach Beendigung der Vertragsbeziehungen zur Fa. … die Zugangsdaten zu ihrem Dokumentenarchiv nicht geändert habe, stelle einen Verstoß gegen Art. 32 I lit. b) DSGVO dar. Außerdem habe die Beklagteb ereits vor dem 16.10.2020 Kenntnis vom Datenleck gehabt, so dass die Benachrichtigung vom 19.10.2020 weder zeitlich noch inhaltlich den Anforderungen an eine Benachrichtigung nach Art. 34 DSGVO entspreche.

10
Nach Einsicht in die Ermittlungsakte der Generalstaatsanwaltschaft Bamberg (Az.: … offenkundig, dass die Täter versucht hätten, mit gestohlenen Kundendaten Kredite zu erlangen. Zudem würden gestohlene Kundendaten, unter anderem die des Klägers, im Darknet zum Kauf angeboten.

11
Von dem Datenvorfall sei auch die Steuer-ID des Klägers betroffen gewesen. Insgesamt habe er durch den Datenvorfall einen Kontrollverlust über seine personenbezogenen Daten erlitten und es bestehe auch die Gefahr eines Identitätsdiebstahls. Das stelle bereits einen immateriellen Schaden dar, der auf die Verstöße der Beklagten gegen die Art. 32, 34 DSGVO zurückzuführen sei, so dass er einen Anspruch auf Schadenersatz gem. Art. 82 Abs. 1 DSGVO habe. Tatsächlich sei er auf Grund des Datenvorfalls vermehrt Opfer von Betrugsversuchen geworden, so habe er seither nämlich über 800 Spam-E-Mails sowie einige Spam-SMS von unbekannten Kriminellen erhalten, auch Telefonanrufe von ihm unbekannten Personen.

12
Der Kläger ist der Auffassung, er habe deshalb einen Anspruch auf Schadenersatz sowohl für den erlittenen immateriellen Schaden, sowie ein Interesse an der Feststellung der Ersatzpflicht für materielle Schäden. Damit der Anspruch auf immateriellen Schadenersatz im unionsrechtlichen Sinne effektiv sei, dürfe es auch keine Bagatellgrenze geben und der Schaden dürfe aus diesem Grunde auch nicht zu gering bemessen sein, so dass ein Betrag von mindestens 5.100,00 € erforderlich sei.

13
Der Kläger beantragt,

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

2. festzustellen, 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, und

3. die Beklagte zu verurteilen, der Klagepartei vorgerichtliche Anwaltskosten in Höhe von € 859,18 zu erstatten.

14
Die Beklagte beantragt,

die Klage abzuweisen.

15
Die Beklagte trägt vor, von dem Datenvorfall seien tatsächlich nur als pdf-Dokumente gespeicherte Kundendaten betroffen gewesen, die aufgrund anderweitiger Vorschriften in dieser Form hätten archiviert werden müssen. Der Datenvorfall sei auch nicht etwa durch Lücken oder Mängel in den Sicherheitssystemen der Beklagten selbst erfolgt, vielmehr seien die eigenen technischen und organisatorischen Sicherheitsstandards angemessen und ausreichend gewesen. Das habe auch die Datenschutzbehörde ausdrücklich festgestellt.

16
Die Beklagte habe darauf vertrauen dürfen, dass die Fa. … nach der Vertragsbeendigung die Daten nicht vollständig und dauerhaft löschen würde; das sei auch geschehen, der Hacker-Angriff bei der Fa. … habe tatsächlich einem Back-Up-System gegolten.

17
Bei der Beurteilung des nach Art. 32 Abs. 1 DSGVO erforderlichen Schutzniveaus müsse auf die Gesamtheit der von der Beklagten ergriffenen technischen und organisatorischen Maßnahmen abgestellt werden und diese hätten vorliegend ein dem Risiko angemessenes Schutzniveau erreicht, so dass kein Verstoß gegen Art. 32 Abs. 1 DSGVO vorliege, der einen Anspruch auf Schadenersatz gem. Art. 82 Abs. 1 DSGVO zu begründen geeignet wäre. Auch die Voraussetzungen des Art. 34 DSGVO seien durch die Mitteilung vom 19.10.2020 erfüllt; davon unabhängig falle diese Vorschrift aber selbst unter der Annahme eines Verstoßes nicht in den von Art. 82 DSGVO umfassten Schutzbereich.

18
Davon unabhängig habe die Beklagte unmittelbar nach Bekanntwerden reagiert, nicht nur durch die Information, sondern auch durch die Angebote zu „Schufa-Plus“ und der Kostenübernahme für einen neuen Personalausweis.

19
Schließlich sei dem Kläger tatsächlich weder ein immaterieller noch gar ein materieller Schaden entstanden. Soweit er Spam-Nachrichten oder Anrufe überhaupt erhalten haben sollte, ließen sich diese nicht ursächlich auf die streitgegenständlichen Datenvorfälle zurückführen, sondern entsprächen dem allgemeinen Risiko, Adressat solcher Nachrichten zu werden, das bereits durch die Nutzung einer E-Mail-Adresse begründet werde. Solche Nachrichten seien auch lediglich als Unannehmlichkeiten zu werten, die die Schwelle zu einem immateriellen Schaden bereits nicht zu überschreiten vermöchten.

20
Für die weiteren Einzelheiten des Sachverhalts und des Parteivorbringens wird auf die gewechselten Schriftsätze mit Anlagen und auf das Protokoll der mündlichen Verhandlung vom 12.01.2023 (Bl. 215/216 d.A.) Bezug genommen.

Entscheidungsgründe

21
Die zulässige Klage erweist sich in nur geringem Umfang als begründet. Der Kläger hat einen Anspruch auf Schadenersatz dem Grunde nach für ihm künftig aus den beiden Datenvorfällen vom August und Oktober 2020 entstehende materielle Schäden gem. Art. 82 Abs. 1 DSGVO. Ein weitergehender Anspruch besteht demgegenüber nicht.

I)

22
Die Klage ist zulässig.

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

24
2. Der Klageantrag zu Ziffer 1 ist hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO, weil die geltend gemachten Verstöße gegen Art. 32, 34 DSGVO und die geltend gemachten Folgen demselben Lebenssachverhalt unterfallen und dieselben Daten betroffen sind, so dass sie auch im Lichte des Antrags auf Zahlung von 5.100,00 € zuzüglich Zinsen einen einheitlichen Streitgegenstand darstellen, der damit hinreichend bestimmt ist.

25
3. Der Kläger hat auch ein gem. § 256 Abs. 1 ZPO erforderliches Interesse an der Feststellung einer Ersatzpflicht für künftige materielle Schäden. Eine Klage auf Feststellung der deliktischen Verpflichtung eines Schädigers zum Ersatz künftiger Schäden ist zulässig, wenn die Möglichkeit eines Schadenseintritts besteht (vgl. z.B. OLG München v. 20.11.2015 – Az.: 10 U 707/15 – Rz. 4; alle Entscheidungen, auch im Folgenden und soweit nicht anders gekennzeichnet, zitiert nach juris-Datenbank; vgl. auch Bacher, Beck'scher Online-Kommentar zur ZPO, 47. Edition, Stand 01.12.2022, § 256 Rz. 24). 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. Etwas anderes gälte erst dann, wenn aus Sicht des Klägers bei verständiger Würdigung gar kein Grund mehr bestünde, mit dem Eintritt eines Schadens wenigstens zu rechnen (OLG München v. 20.11.2015 – Az.: 10 U 707/15 – Rz. 7, Rn. 4).

II)

26
Die Klage ist jedoch in nur geringem Umfang begründet.

27
1. Der Kläger hat keinen Anspruch auf einen immateriellen Schadenersatz in Höhe von 5.100,00 € gem. Art. 82 Abs. 1 DSGVO. Denn auch wenn die Beklagte, indem sie die Zugangsinformationen für die Fa. … nach Beendigung der vertraglichen Beziehungen nicht änderte und somit gegen Art. 32 Abs. 1 DSGVO verstieß, so ist dem Kläger doch kein ursächlich auf die streitgegenständlichen Datenvorfälle zurückzuführender, immaterieller Schaden entstanden, der gem. Art. 82 Abs. 1 DSGVO ersatzfähig wäre.

28
1.1 Nach Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadenersatz gegen den Verantwortlichen. Verantwortlicher im Sinne der DSGVO ist gem. Art. 4 Nr. 7 DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Personenbezogene

Daten sind gem. Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen, wobei eine natürliche Person als identifizierbar angesehen wird, wenn sie 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.

29
1.2 Die Beklagte ist Verantwortliche im Sinne von Art. 82 Abs. 1, 4 Nr. 7 DSGVO, weil sie Kundendaten im Rahmen des Anmeldeprozesses abfragt und in einem Datenarchiv abspeichert. Auch sind die von den streitgegenständlichen Daten vorfällen erfassten Daten personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO, weil sie den Kläger identifizierbar machen.

30
1.3 Die Beklagte hat gegen Art. 32 Abs. 1 DSGVO verstoßen.

31
1.3.1 Nach Art. 32 Abs. 1 DSGVO sind Verantwortliche (i.S.v. Art. 4 Nr. 7 DSGVO) verpflichtet, 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 lit. f. DSGVO ergänzt den Aspekt der Vertraulichkeit, dass die Daten vor unbefugter und unrechtmäßiger Verarbeitung durch geeignete technische und organisatorische Maßnahmen zu schützen sind. Dabei hängen die konkret zu ergreifenden Schutzmaßnahmen von der Bedeutung der Daten für die Rechte und Interessen der betroffenen Personen ab (Schantz in Wolff/Brink, Beck'scher Online-Kommentar zum Datenschutzrecht, 42. Edition, 01.11.2021, Art. 5 Rz. 35).

32
1.3.2 Indem die Beklagte die Zugangsdaten nach Beendigung der Vertragsbeziehung mit der Fa. … nicht änderte, schützte sie die Daten nicht angemessen vor einer unbefugten oder unrechtmäßigen Verarbeitung.

33
Die Beklagte speicherte die personenbezogenen Daten des Klägers – als pdf-Dateien verschriftlichter Dokumente – in einem Datenarchiv. Den Zugangsschlüssel zu ihrem Datenarchiv hatte sie zunächst während der Dauer der bestehenden Zusammenarbeit bei der Fa. … gespeichert. Doch auch nach Beendigung der Vertragsbeziehung mit der Fa. … änderte die Beklagte den Zugangsschlüssel nicht ab und unternahm auch keine anderen Schritte um sicherzustellen, dass der Zugangsschlüssel nicht mehr verwendet werden kann. Dadurch hat sie das Risiko aufrechterhalten, dass durch einen Hacker-Angriff auf die Fa. … auch Daten ihrer Kunden abgegriffen werden können, ein Risiko, dass durch eine Abänderung der Zugangsdaten hätte minimiert oder gar ausgeschlossen werden können.

34
Als Verantwortliche im Sinne von Art. 32 Abs. 1, 4 Nr. 7 DSGVO durfte sich die Beklagte auch nicht lediglich darauf verlassen, dass die Fa. … die Zugangsinformationen löschen würde, unabhängig davon, ob diese dazu vertraglich verpflichtet war oder nicht. Vor allem aber durfte sie sich auch nicht ohne weiteres darauf verlassen, dass auch alle Sicherungskopien, Back-Ups und sonstigen weiteren Speichermaßnahmen im Hinblick auf den Zugangsschlüssel vollständig und dauerhaft gelöscht sein würden. Allein das Vertrauen der Beklagten in ausreichende Schutzmaßnahmen auf Seiten der Fa. … 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.

35
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. Tatsächlich war ihre – nach Bekanntwerden der Datenvorfälle – eine solche Maßnahme dann auch möglich. Berücksichtigt man zudem, dass die Beklagte durch ihr Verhalten die

Datenmissbrauchsmöglichkeit über die Fa. … über den ursprünglich gegebenen Umfang erweiterte, indem sie auch die personenbezogenen Daten von Kunden, die die Beklagte erst nach Beendigung der vertraglichen Beziehungen zur Fa. … gewinnen konnte, gleichfalls dem Risiko eines Zugriffs über den alten Zugangsschlüssel aussetzte.

36
Auf Grund hat die Beklagte die grundlegenden, personenbezogenen Daten des Klägers nicht ausreichend durch geeignete technische und organisatorische Maßnahmen vor einem unberechtigten Zugriff gem. Art. 5 Abs. 1 lit. F DSGVO geschützt und damit nicht ausreichend geeignete Maßnahmen für ein angemessenes Schutzniveau im Sinne von Art. 32 Abs. 1 DSGVO ergriffen.

37
1.3.3 Dem steht auch nicht entgegen, dass die Beklagte für ihr Informationssicherheitsmanagement eine Zertifizierung nach ISO 27001:2013 des TÜV Rheinland erhalten hatte, das Bayerische Landesamt für Datenschutzaufsicht (LDA Bayern) keinen Pflichtenverstoß feststellte und daher – wie die Beklagte vorträgt – in einer nach Art. 32 Abs. 1 DSGVO vorzunehmenden Gesamtwürdigung das Schutzniveau in Anbetracht des Zusammenspiels aller ergriffenen Maßnahmen als ausreichend zu werten sei. Denn ungeachtet dessen, dass der konkrete Prüfungsumfang weder des TÜV Rheinland noch des LDA Bayern nicht hinreichend dargetan ist, stellt die Einhaltung eines Zertifizierungsverfahrens (Art. 32 Abs. 3 DSGVO) nur einen Aspekt im Rahmen der Abwägung dar, in die zugleich auch Umfang und Bedeutung der in Frage stehenden personenbezogenen Daten und die Risiken und potenziellen Folgen eines Datenvorfalls einzustellen sind, wie auch Art. 32 Abs. 2 DSGVO deutlich macht. Nach Beendigung der Vertragsbeziehungen die dem früheren Vertragspartner zur Verfügung gestellten Zugangsdaten nicht abzuändern, ist in Anbetracht des Umfangs der dadurch betroffenen Daten und des Umstandes, dass es sich um höchstpersönliche, private Daten einer großen Zahl von Kunden handelt, daher ein wenngleich singulärer, aber doch im konkreten Fall in seinen Auswirkungen so gravierender Verstoß, dass auch in Anbetracht eines ansonsten angemessenen und ausreichenden Schutzkonzeptes eine Verletzung der sich aus Art. 32 Abs. 1, Art. 5 Abs. 1 DSGVO ergebenden Pflichten zu bejahen ist.

38
1.4 Der Verstoß gegen Art. 32 Abs. 1 DSGVO – das Absehen von einer Änderung der Zugangsdaten nach Vertragsbeendigung mit der Fa. … – lässt auch die im Verkehr erforderliche Sorgfalt außer acht und war damit fahrlässig, so dass auch das erforderliche Verschulden auf Seiten der Beklagten zu bejahen ist.

39
1.5 Allerdings ist dem Kläger durch die streitgegenständlichen Datenvorfälle weder ein immaterieller noch ein materieller Schaden entstanden, der eine Ersatzpflicht nach Art. 82 Abs. 1 DSGVO auslösen würde.

40
1.5.1 Der Anspruch auf Schadenersatz setzt nach dem ausdrücklichen Wortlaut des Art. 82 Abs. 1 DSGVO voraus, dass dem Betroffenen „wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist“ (Hervorhebung durch das Gericht). Die Darlegungs- und Beweislast dafür tritt – den allgemeinen zivilprozessualen Regeln, dass die klagende Partei grundsätzlich die den Anspruch begründenden Umstände beweisen muss – der Kläger (vgl. OLG Frankfurt a.M. v. 2.3.2022 – Az.: 13 U 206/20 – Rz. 65 f.; LG München I v. 09.02.2023 – Az. 5 O 5853/22 – vorgelegt als Anlage B15).

41
1.5.2 Diesen Maßstab zugrunde gelegt, hat der Kläger nicht ausreichend dargetan, dass bei ihm ein materieller oder immaterieller Schaden eingetreten sei. Einen konkreten materiellen Schaden hat er selbst nicht behauptet. Dass die bei dem Datenvorfall erbeuteten personenbezogenen Daten für einen Identitätsdiebstahl tatsächlich verwendet bzw. missbraucht worden wären, hat er gleichfalls nicht vorgetragen. Und er hat auch nicht subsstantiiert dazu vorgetragen, dass es in sonstiger Weise zu einem konkreten Missbrauch – über den Erhalt von Nachrichten oder Anrufen hinaus – seiner Daten gekommen sei oder seine Daten im Darknet tatsächlich konkret angeboten worden seien.

42
Soweit der Kläger vorgetragen hat, dass er Adressat einer großen Anzahl von E-Mails, Kurznachrichten oder auch Anrufen, z.T. auch mit erpresserischem Inhalt geworden sei, handelt es sich dabei um typische, mit der Nutzung digitaler Kommunikationsmittel verbundener Beeinträchtigungen und Risiken, wie sie

allgemein auftreten und erlitten werden. Der Datenvorfall mag bei dem Kläger ein unkonkretes, wiewohl unangenehmes Gefühl des Kontrollverlustes über die eigenen Daten ausgelöst haben, die Schwelle zur Annahme eines immateriellen Schadens im Sinne einer Beeinträchtigung eines geschützten Rechtsgutes wird dadurch jedoch noch nicht überschritten.

43
Doch selbst wenn man in dem Erhalt der E-Mails, Nachrichten und Anrufe einen ausreichenden immateriellen Schaden im Sinne von Art. 82 Abs. 1 DSGVO erblicken wollte, so hat der Kläger jedenfalls nicht ausreichend substantiiert darzulegen vermocht, dass diese Beeinträchtigungen ursächlich auf die hier streitgegenständlichen Datenvorfälle zurückzuführen wären. Denn die Beklagte hat substantiiert anhand der Anlage B8 vorgetragen, dass der Kläger bei mindestens drei weiteren Gelegenheiten Opfer von Datenvorfällen wurde, bei denen jedenfalls auch seine Telefonnummer und seine E-Mail-Adresse abgegriffen wurden. Das hat der Kläger auch nicht substantiiert bestritten. Dann aber lässt sich der geklagte Erhalt von E-Mails, Nachrichten und Anrufen auch nicht zur Überzeugung des Gerichts (§ 286 ZPO), nicht einmal mit einer überwiegenden Wahrscheinlichkeit (§ 287 ZPO) auf die streitgegenständlichen Datenvorfälle bei der Beklagten zurückführen.

44
1.5.3 Entgegen der Auffassung des Klägers kann ein Schaden auch nicht allein 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.

45
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 DS-GVO an sich bereits einen Schaden und damit einen Anspruch auf Schadensersatz begründen würde, erübrigte sich, dass Art. 82 Abs. 1 DSGVO das Vorliegen eines Schadens ausdrücklich als weitere Voraussetzung für den Schadensersatzanspruch nennt. Der Schaden ist somit nicht mit der zugrundeliegenden Rechtsgutsverletzung gleichzusetzen, sondern Art. 82 Abs. 1 DSGVO trennt zwischen dem Verstoß und dem daraus resultierenden, „entstandenen“ Schaden, woraus folgt, dass dieser tatsächlich entstanden sein muss und nicht lediglich befürchtet wird (OLG Frankfurt v. 02.03.2022 – Az.: 13 U 206/20 – Rz. 70 f.; Generalanwalt Manuel Campos Sánchez-Bordona, Schlussanträge in der Rechtssache C-300/21 Österreichische Post AG vom 06.10.2022, Rz. 27 ff.; Quaas in Wolff/Brink, Beck'scher Online-Kommentar zum Datenschutzrecht, 43. Edition, Stand 01.02.2023, Art. 82 DSGVO, Rz. 23). Daher muss auch ein immaterieller Schaden eingetreten sein und konkret dargelegt werden, wofür sich beispielhafte Aufzählungen in den Erwägungsgründen 75 und 85 der DSGVO finden (Quaas a.a.O., Rz. 24). Weder die vom Kläger geklagten Beeinträchtigungen noch der Umstand, dass es überhaupt zu einem Datenvorfall gekommen ist, erfüllen damit die Voraussetzungen des Art. 82 Abs. 1 DSGVO für einen ersatzfähigen immateriellen Schaden.

46
1.5.4 Auf Grund all dessen hat der Kläger keinen Anspruch auf Ersatz eines immateriellen Schadens gem. Art. 82 Abs. 1 DSGVO. Lediglich ergänzend sei daher darauf hingewiesen, dass die Beklagte ihrerseits – davon abgesehen – aber auch Kompensationsleistungen erbracht hat, etwa durch das Angebot einer kostenlosen Teilnahme am „SchufaPlus“-Programm, was dem Kläger eine Überwachung im Hinblick auf unbefugte finanzielle Aktivitäten ermöglicht und dieser daher auch angenommen hat, oder durch das Angebot der Kostenübernahme für die Ausstellung eines neuen Personalausweises – ein Angebot, dass der Kläger allerdings selbst im Hinblick auf die nur noch kurze Laufzeit des Personalausweises ausschlug.

47
Auch wenn der Kläger – wie von ihm in der mündlichen Verhandlung vorgetragen – dabei auch berücksichtigte, dass während der Corona-Pandemie ein Antrag auf vorgezogene Ausstellung eines neuen Personalausweises mit erheblichem Aufwand verbunden gewesen wäre, so zeigt der Umstand, dass er diesen Aufwand scheute, doch, dass er das Risiko eines Missbrauchs der mit dem Ausweis verbundenen Daten doch als jedenfalls geringer erachtete als die Unannehmlichkeiten des Aufwandes.

48

1.6 Aus den gleichen Erwägungen kann der Kläger auch keinen Schadenersatz gem. Art. 82 Abs. 1 DSGVO wegen eines Verstoßes gegen Art. 34 Abs. 1 DSGVO geltend machen. Dabei kann es dahingestellt bleiben, ob die von der Beklagten am 19.10.2020 erteilten Informationen unverzüglich im Sinne von Art. 34 DSGVO erfolgt sind und auch den erforderlichen Inhalt hatten. Und es kann auch dahingestellt bleiben, ob Art. 34 DSGVO überhaupt in den Schutzbereich des Art. 82 Abs. 1 DSGVO fällt (was die Beklagte bestreitet). Denn auch insoweit fehlt es jedenfalls an einem ersatzfähigen immateriellen Schaden nach den oben dargelegten Erwägungen. Und das gilt umso mehr, als auch nach dem klägerischen Vortrag nicht ersichtlich ist, inwieweit die von ihm vorgetragenen Beeinträchtigungen ursächlich auf eine unzureichende Information zurückzuführen sein sollten – die Datenvorfälle waren ja zuvor bereits erfolgt.

49
2. Der Kläger hat auch keinen Anspruch auf Ersatz eines ihm möglicherweise künftig entstehenden materiellen Schadens im Zusammenhang mit dem Datenvorfall im April 2020, weil er zu diesem Zeitpunkt nach eigenem Vortrag noch nicht Kunde der Beklagten war (das ist er erst seit Juni 2020) und entsprechend seine Daten zu diesem Zeitpunkt auch noch nicht von dem Vorfall betroffen gewesen sein können.

50
3. Demgegenüber erweist sich der Antrag auf Feststellung einer Ersatzpflicht für etwaige künftige materielle Schäden auf Grund der beiden Datenvorfälle vom August und Oktober 2020 gem. Art. 82 Abs. 1 DSGVO als begründet. Wie oben ausgeführt, hat die Beklagte als Verantwortliche schuldhaft gegen Art. 32 Abs. 1 DSGVO verstoßen. 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.

51
Die Möglichkeit des Eintritts materieller Schäden besteht und ist auch nicht gänzlich auszuschließen, weil die Daten des Klägers noch immer „verloren“ sind und damit potenziell missbraucht werden können. Auch wenn der Datenabgriff bereits im Jahr 2020 stattfand, ist unter dem Gesichtspunkt „Das Internet vergisst nicht“ nicht auszuschließen, dass die personenbezogenen Daten des Klägers, die über den Datenvorfall erlangt wurden, in Zukunft missbraucht werden und so zu einem Schaden bei dem Kläger führen, zumal ein nicht unerheblicher Bestandteil an personenbezogenen Daten des Klägers betroffen ist.

52
Insoweit erweist sich die Klage daher als begründet. 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.

4, Soweit der Kläger schließlich Ersatz der ihm durch die vorgerichtliche anwaltliche Vertretung entstandenen Kosten von 859,28 € für die Geltendmachung immateriellen Schadenersatzes begehrt, ist die Klage demgegenüber wiederum unbegründet, weil ein solcher Anspruch auf immateriellen Schadenersatz nicht besteht, so dass auch seine vorgerichtliche Geltendmachung unberechtigt war. Und eine Erklärung über die Ersatzpflicht für künftige materielle Schäden wurde mit dem als Anlage K7 vorgelegten Schreiben nicht verlangt, war somit nicht Gegenstand der außergerichtlichen Geltendmachung.

III)

53
Die Kostenentscheidung folgt aus § 92 Abs. 2 ZPO, weil die Klage in nur geringem Umfang begründet ist und insoweit auch kein Kostensprung ausgelöst wird.

54
Der Ausspruch zur vorläufigen Vollstreckbarkeit – hinsichtlich der Kosten – beruht auf § 709 ZPO.