LG München I, Endurteil v. 09.12.2021 – 31 O 16606/20

Titel:

Schadensersatz bei Datenabfluss aus dem Datenbestand eines Finanzdienstleisters

Normenkette:

DS-GVO Art. 82 Abs. 1

Leitsätze:

4. Die Entwendung von personenbezogenen Daten aus dem Datenbestand eines Finanzdienstleisters rechtfertigt einen Anspruch auf immateriellen Schadensersatz in Höhe von 2.500 €. (Rn. 41) (redaktioneller Leitsatz)

5. Die Darlegungs- und Beweislast für das Vorliegen eines Datenschutzverstoßes liegt beim Anspruchsteller; eine Beweislastumkehr existiert insoweit nur hinsichtlich des Verschuldens. (Rn. 28 – 40) (redaktioneller Leitsatz)

Schlagwort:

Datenschutzverstoß

Rechtsmittelinstanz:

OLG München vom -- – 36 U 138/22

Fundstellen:

RDV 2022, 107
GRUR-RS 2021, 41707
ZD 2022, 242
BKR 2022, 131
LSK 2021, 41707

Tatbestand

1
Der Kläger ist Kunde der Beklagten. Vor dem Eingehen der Geschäftsbeziehung hat der Kläger der Beklagten, ein Finanzdienstleistungsunternehmen, zahlreiche personenbezogene Daten zur Verfügung gestellt. Hinsichtlich der einzelnen Daten wird auf die Klageschrift Seiten 3 und 5 Bezug genommen (vgl. auch Anlage K 2). Außerdem musste er sich mittels Postident-Verfahren legitimieren, wobei sein Personalausweis abfotografiert wurde.

2
In der Folgezeit nutzte der Kläger sein Kundenkonto für die Geldanlage in Aktien und Wertpapiere. Am 19.10.2020 wurde der Kläger von der Beklagten darüber informiert, dass von unbefugten Dritten unrechtmäßig auf einen Teilbestand der in Ihrem Datenarchiv abgelegten Daten zugegriffen wurde. Von Kläger wurden die folgenden Daten entwendet:

Vor- und Nachname, Anrede, Anschrift, E-Mail-Adresse, Handynummer, Geburtsdatum, -ort und -land, Staatsangehörigkeit, Familienstand, Steuerliche Ansässigkeit und Steuer-ID, IBAN, Ausweiskopie, Portraitfoto, welches im Post-Ident-Verfahren angefertigt wurde.

3
Der Kläger trägt weiter vor, dass sich aus der strafrechtlichen Ermittlungsakte der Generalstaatsanwaltschaft Bamberg (Az.: 620 UJs 1244/21) entnehmen lässt, dass der Zugriff auf die Kundendaten der Beklagten zu drei unterschiedlichen Zeitpunkten im Jahr 2020 konkret am 15./16.04.2020, am 05./06.08.2020 sowie am 10./11.10.2020 erfolgt ist. Bei jedem dieser Zugriffe wurde ein Teil der insgesamt 389.000 Datensätze der 33.200 betroffenen Personen kopiert und entwendet. Nach dem Vortrag der Beklagten soll der Zugriff auf die Daten des Klägers hingegen am 06.08.2021 erfolgt sein (Schriftsatz vom 29.11.2021 S. 16, Bl. 170 d.A.), wobei dies aber ein Schreibfehler in der Angabe der Jahreszahl sein dürfe, es aber hierauf auch nicht entscheidungserheblich ankommt.

4
Die Beklagte hatte bei ihrem früheren Dienstleister Zugangsinformationen zu ihrem vollständigen IT-System hinterlegt. Der Angreifer verschaffte sich mithilfe dieser Zugangsdaten Zugriff auf einen Teil des Dokumentenarchivs und die darin befindlichen Kundendaten.

5
Die Vertragsbeziehung zwischen der Beklagten und der Fa. wurde Ende 2015 beendet, wobei die Beklagte die Zugangsdaten zu ihrem IT-System, welche der Fa. ... bekannt waren, jedenfalls bis zum streitgegenständlichen Vorfall nicht geändert hat.

6
Es sei mit Blick auf den Schaden des Klägers nach Einsicht in die Ermittlungsakte der Generalstaatsanwaltschaft Bamberg offenkundig, dass die Täter versucht haben, mit gestohlenen Kundendaten Kredite zu erlangen. Weiterhin ergibt sich aus der Ermittlungsakte, dass die gestohlenen Daten im Darknet angeboten wurden.

7
Aufgrund dessen ist der Kläger der Ansicht, dass er nunmehr dauerhaft dem Risiko ausgesetzt ist, dass die über ihn erbeuteten Daten für Identitätsdiebstähle, Zugriffsversuche auf von ihm genutzten Online-Dienste oder sonstige Betrugsversuche verwendet werden. So sei es am 27.9.2020 zu insgesamt 10 fehlgeschlagenen Login-Versuchen bei seinem E-Mail-Anbieter gekommen (Anlage K 3).

8
Der Kläger ist daher der Ansicht, dass ihm deshalb Ansprüche gem. § 82 Abs. 1 DSGVO i.V.m. § 253 BGB zustehen, da die Beklagte seine Daten unter Verstoß gegen Art. 32 DSGVO verarbeitet habe.

9
Der Kläger beantragt daher:

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.

2. Die Beklagte wird verurteilt, an den Kläger ein angemessenes Schmerzensgeld, dessen Höhe in das Ermessen des Gerichts gestellt wird nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit Rechtshängigkeit zu zahlen.

10
Die Beklagte beantragt

die Klage abzuweisen.

11
Hierzu weist sie insbesondere darauf hin, dass sie im Nachgang zum Datenvorfall sämtliche in Betracht kommenden Maßnahmen vorgenommen hat, um einem Missbrauch der Daten ihrer Kunden entgegenzuwirken und den Sachverhalt aufzuklären. Sie kooperierte eng mit den zuständigen Behörden und externen Experten.

12
Der Kläger habe infolge des Datenvorfalls keinerlei materielle und immaterielle Nachteile erlitten. Es sei auch nicht bekannt, dass andere Kunden der Beklagten missbrauchsbedingt geschädigt worden sind.

13
Dem Kläger stünden die geltend gemachten Ansprüche aus mehreren Gründen nicht zu.

14
Der Beklagten würde schon kein Verstoß gegen die Datenschutzgrundverordnung zur Last fallen. Der darlegungs- und beweisbelastete Kläger habe insofern unsubstantiiert und unschlüssig vorgetragen. Der Datenvorfall an sich bedeute keinen Verstoß der Beklagten gegen die DSGVO. Die technischen und organisatorischen Maßnahmen der Beklagten seien angemessen gewesen.

15

Die Beklagte nutzt für die Abwicklung des gesamten Kundengeschäfts insbesondere eine sichere standardisierte IT-Infrastruktur mit u.a. Applikations- und Datenbankservern, Speicherkapazitäten, Redundanzsystemen und Backup-Lösungen. Die dem Dokumentenarchiv zu Grunde liegende IT-Infrastruktur ist außerdem nach IEC 27001:2013, 27017:2015, 27018:2019, ISO/IEC 9001:2015 und CSA STAR CCM v3.0.1 zertifiziert.

16
Für den kriminellen Zugriff sei ein von der Beklagten betriebenes Dienstprogramm nicht kompromittiert worden. Man könne daher nicht von einem „Hack“ des Systems der Beklagten sprechen.

17
Der Angreifer, dessen Identität bislang nicht ermittelt werden konnte, erlangte den Zugriff auf die Kundendokumente im Dokumentenarchiv nicht durch Überwindung der von der Beklagten implementierten IT-Sicherheitssysteme. Vielmehr erfolgte der Zugriff unter Ausnutzung rechtswidrig erlangter Zugangsinformationen. Diese waren offenbar zuvor infolge eines Cyber-Angriffs auf das Unternehmen erlangt worden, das mit Softwaredienstleistungen für die Beklagte beauftragt worden war. Die Beklagte sei demnach ein Kollateralopfer jenes Cyber-Angriffs auf das Drittunternehmen gewesen.

18
Der Beauftragung von durch ging ein sorgfältiger Auswahl- und Prüfprozess voraus, der unter anderem eine vertiefte inhaltliche Auseinandersetzung mit den Spezifikationen der angebotenen Dienstleistung und den ITspezifischen Sicherheitsstandards von einschloss. Die Bereitstellung der Zugangsinformationen zur digitalen Umgebung der Beklagten an war für die Ausführung der Softwaredienstleistungen bereits aus technischer Sicht notwendig, um das externe Deployment-Dienstprogramm an die digitale Umgebung von anbinden zu können.

19
Im Übrigen träfe die Beklagte in Bezug auf einen unterstellten DSGVO-Verstoß kein Verschulden. Schließlich bestehe keine Kausalität eines angeblichen DSGVO-Verstoßes für den vermeintlichen Schaden. Hinsichtlich der weiteren Einzelheiten wird auf die Klageerwiderung vom 12.05.2021 Bezug genommen.

20
Der Feststellungsantrag sei mangels Feststellungsinteresses gemäß § 256 Abs. 1 ZPO unzulässig. Der darlegungs- und beweisbelastete Kläger habe keine Umstände vorgetragen, aus denen sich ergibt, dass der Eintritt materieller Schäden infolge des Datenvorfalls wahrscheinlich ist.

21
Zur Ergänzung des Tatbestands wird Bezug genommen auf die gewechselten Schriftsätze nebst Anlagen sowie auf das Sitzungsprotokoll.

22
Die Wiedereröffnung der Verhandlung aufgrund des Schriftsatzes der Beklagten vom 29.11.2021 war nicht veranlasst (§ 156 ZPO). Die darin enthaltenen Ausführungen wurden vom Gericht berücksichtigt, sind aber letztlich nicht entscheidungserheblich.

Entscheidungsgründe

23
Die Klage ist zulässig, wobei sich die örtliche Zuständigkeit des LG München aus §§ 44 Abs. 1 S. 1 DSGVO, § 12 ZPO ergibt.

24
Hinsichtlich des Feststellungsantrages ist auch das gem. § 256 Abs. 1 ZPO erforderliche Feststellungsinteresse zu bejahen, da die Möglichkeit besteht, dass weitere Schäden durch die Verwendung der illegal erlangten Daten entstehen. 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 (vgl. Bacher BeckOK ZPO, Vorwerk/Wolf 42. Edition Stand: 01.09.2021 § 256 Rn. 24). Aber gerade bei einem solch umfangreichen Datenabgriff ist bei lebensnaher Betrachtung davon auszugehen, dass dies nicht ohne eine bestimmte, und zwar illegale Absicht erfolgt ist.

25

Die Klage ist auch begründet.

26
Der Kläger hat gegenüber der Beklagten einen Anspruch auf Zahlung von 2.500, - Euro gem. § 82 Abs. 1 DSGVO als immateriellen Schadensersatz.

27
Nach dieser Vorschrift hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

28
Nach § 82 Abs. 3 DSGVO trägt die Darlegungs- und Beweislast für die haftungsbegründenden Voraussetzungen nach allgemeinen zivilprozessualen Grundsätzen der Anspruchsberechtigte. Eine Beweislastumkehr ist in Art. 82 Abs. 3 ausdrücklich nur bezüglich des Gesichtspunkts des Verschuldens vorgesehen. Dem Verletzten obliegt es daher auch, den Datenschutzverstoß zu beweisen. Die allgemeine Rechenschaftspflicht der Art. 5 Abs. 2, 24 Abs. 1 DS-GVO bezieht sich auf eine Verantwortlichkeit gegenüber der Behörde. Hierauf kann jedoch eine Beweislastumkehr oder Beweiserleichterung nicht gestützt werden (Quaas BeckOK Datenschutzrecht, Wolff/Brink; 36. Edition Stand: 01.05.2021 § 82 Rn. 51; 9 U 34/21 OLG Stuttgart Urteil vom 31.03.2021; LG Frankfurt vom 18.01.2021 - 2-30 O 147/20).

29
Im Hinblick auf die Frage des Datenschutzverstoßes verlangt Art. 32 DSGVO (Sicherheit der Verarbeitung) geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zudem können die Anforderungen bzw. Vorgaben für einen ordnungsgemäßen und sicheren Umgang mit den Daten aus Artikel 5 Abs. 1 Lit. f DSGVO (Grundsätze für die Verarbeitung personenbezogener Daten), aus den Erwägungsgründen 39 und 78 Verordnung (EU) 2016/679 S. 12 sowie der Anlage zu § 9 BDSG 2003. (vgl. Kühling/Buchner/Herbst, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 76) entnommen werden.

30
Insbesondere nennt der Erwägungsgrund 39 als geforderte Maßnahmen, dass gewährleistet ist, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können. Die Anlage zu § 9 BDSG 2003 listete technische und organisatorische Maßnahmen auf, die auch zur Erfüllung der Anforderungen des Art. 5 Abs. 1 lit. f eingesetzt werden können.

31
Unter Zugrundelegung dieser Vorgaben hat die Beklagte einen Datenschutzverstoß begangen.

32
Hierbei kann dahingestellt bleiben, ob der Beklagten etwaige Sicherheitsmängel bei dem Drittunternehmen zugerechnet werden können. Denn die Beklagte hat selbst keine ausreichenden organisatorischen Maßnahmen vorgenommen, um den streitgegenständlichen Datenverlust zu verhindern (vgl. auch Art. 82 Abs. 4 DSGVO).

33
So ist unstreitig, dass die Beklagte die Zugangsdaten für das Unternehmen nach Beendigung der Geschäftsbeziehung nicht geändert hat. Darauf, wie die Beklagte vorträgt, dass sie davon ausgehen musste, dass die Zugangsinformationen vollständig und dauerhaft seitens gelöscht werden, durfte sie sich im Hinblick auf den großen Umfang (Zugriff auf das vollständige IT-System) sowie aufgrund der Qualität und Sensibilität der gespeicherten Daten nicht verlassen. Da die Beklagte die Löschung offensichtlich nicht überprüft hat, war es fahrlässig gewesen, die Zugangsdaten seit Beendigung der Geschäftsbeziehung im Jahre 2015 bis zum Zugriff auf die Kundendaten der Beklagten im Jahre 2020 mehrere Jahre lang unverändert zu lassen. Die Beklagte kann sich auch nicht durch die umfangreichen Ausführungen über die technischen und organisatorischen Maßnahmen (TOMs) insoweit entlasten. Unerheblich wäre hierbei im Übrigen, wenn - wie die Beklagte vorträgt, das Dokumentarchiv im Jahr 2015 noch keine Kundendaten enthalten haben sollte. Denn jedenfalls sind diese dann in der Folgezeit in das Archiv aufgenommen worden.

34
Sofern die Beklagte ausweislich Ihres Schreibens vom 19.10.2020 nach dem Vorfall umgehend alle erforderlichen Maßnahmen ergriffen hat, um weitere unrechtmäßige Zugriffe auf das digitale Dokumentenarchiv auszuschließen, so ist es - entgegen der Ansicht des Beklagten - nicht als unzumutbar anzusehen, dass dies bereits unmittelbar nach Beendigung der Geschäftsbeziehung mit dem Unternehmen hätte getan werden können. Auch wenn dies einen gewissen Aufwand erfordert hätte - und jetzt ja auch erfordert hat, kann dies keine Berechtigung dafür sein, die Daten der Kunden in einem bestimmten Bereich der Gefährdung durch einen (möglichen) unerlaubten Zugriff von außen ausgesetzt sein zu lassen.

35
Wenn die Beklagte außerdem betont, dass es sich bei um ein unabhängiges Unternehmen handelt, dessen etwaige Unzulänglichkeiten ihr daher von vornherein nicht zugerechnet werden können, ist dies unerheblich. Denn es lag eben auch eine Unzulänglichkeit auf Seiten der Beklagten bzw. ein eigener DSGVO-Verstoß vor, und gerade die seitens der Beklagten vorgetragene fehlende rechtliche und tatsächliche Möglichkeit, den Löschungsprozess bei zu beaufsichtigen, zu kontrollieren oder anzuweisen erforderte auf Seiten der Beklagten die Vornahme entsprechender eigener Sicherungsmaßnahmen.

36
Es liegt auch die erforderliche Kausalität zwischen dem „DSGVO-Verstoß“ und dem „Schaden“ vor. Art. 82 Abs. 1 DSGVO verlangt, dass der Schaden infolge eines konkreten DSGVO-Verstoßes eintritt. Es genügt zwar nicht, dass ein Schaden bloß auf eine Verarbeitung personenbezogener Daten zurückzuführen ist, in deren Rahmen es zu einem Rechtsverstoß gekommen war (OLG Stuttgart, Urteil vom 31. März 2021, Az. 9 U 34/21, S. 8, Anlage B 2; Paal, MMR 2020, 14, 17 m.w.N.), vorliegend beruht der Schaden aber nicht nur auf eine solche Verarbeitung. Es ist davon auszugehen, dass es bei Einhaltung der als adäquat geltenden Sicherheitsmaßstäbe nicht zu dem konkreten Datenvorfall gekommen wäre (vgl. Quaas, in: BeckOK Datenschutzrecht, Wolff/Brink, 33. Ed., 01.08.2020, Art. 82 DSGVO Rn. 51; 26 - Mitursächlichkeit genügt).

37
Sofern die Beklagte das Urteil das LG München I vom 02.09.2021, 23 O 10931/20 angeführt, sprechen dessen Entscheidungsgründe gerade dafür, dass im vorliegenden Fall ein Schaden gegeben ist. So weist das Landgericht zutreffend darauf hin, dass nach Art. 82 DS-GVO auch ein durch einen Verstoß gegen die Verordnung entstandener immaterieller Schaden ersetzt werden kann sowie dass in den Erwägungsgründen (Nr. 75) (insbesondere) auch Nichtvermögensschäden durch Diskriminierung, Indentitätsdiebstahl oder -betrug, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten oder gesellschaftliche Nachteile genannt sind (Vgl. BeckOK Datenschutz/Quaas DSGVO Art. 82 Rz. 23). Im dortigen Verfahren hat das Gericht seine Entscheidung insbesondere darauf gestützt, dass der Kläger sich darauf beschränkt hat, vorzutragen, sein Schaden bestehe im Verlust der Kontrolle über seine Daten (was aber auch im Erwägungsgrund Nr. 75 genannt ist!). Während dort ein Angriff auf den Account der E-Mail-Adresse zugrunde liegt, sind im vorliegenden Fall wesentlich umfangreichere und sensiblere Daten abgegriffen worden. Entgegen der Ansicht des LG Essen, Urteil vom 23.9.2021 - 6 O 190/21 liegt darin eine nicht nur „unbedeutende oder empfundene Verletzung von Persönlichkeitsrechten“. Im Übrigen erwähnt das LG Essen auch, dass ein Schmerzensgeldanspruch nach Art. 82 DS-GVO nicht auf schwere Schäden beschränkt ist, sodass sich ein genereller Ausschluss von Bagatellfällen verbietet. Das Gericht geht zudem offensichtlich (und zutreffend) auch davon aus, dass ein Identitätsdiebstahl für einen Schmerzensgeldanspruch ausreichen würde.

38
Die Erwägungsgründe 75 und 85 DS-GVO zählen beispielhaft auf, welche konkreten Beeinträchtigungen einen „physischen, materiellen oder immateriellen Schaden“ darstellen können, so etwa Diskriminierung, Identitätsdiebstahl oder -betrug, finanzieller Verlust, Rufschädigung, unbefugte Aufhebung einer Pseudonymisierung oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile. Nach Erwägungsgrund 146 DS-GVO muss der Begriff des Schadens zudem „im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht“ und die „betroffenen Personen sollen einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten“. Im Vordergrund steht hier eine abschreckende Wirkung des Schadensersatzes, die insbesondere durch dessen Höhe erreicht werden soll. Dieser Gedanke wird auch aus Art. 4 III EUV abgeleitet. Danach sind die Mitgliedstaaten angehalten, Verstöße wirksam zu sanktionieren. Denn nur so wäre eine effektive Durchsetzung des EU-Rechts - und damit auch

der DS-GVO - gewährleistet (Wybitul/Haß/Albrecht: NJW 2018, 113, beckonline; vgl. auch Korch, NJW 2021, 978 - „Aus Erwägungsgrund 146 S. 3 ergibt sich, dass der Begriff des Schadens weit zu verstehen ist“).

39
Im vorliegenden Fall muss aufgrund des Umfanges und Art der entwendeten Daten des Klägers ein solcher Identitätsdiebstahl angenommen werden, welcher einen Anspruch auf Schadensersatz begründet.

40
So hat die Beklagte mit Schreiben vom 19.10.2020 (Anlage K 7) den betroffenen Kunden, somit auch dem Kläger mitgeteilt, dass die folgenden Daten von dem Vorfall betroffen sind wie „Personalien und Kontaktdaten, Daten zur gesetzlich erforderlichen Identifizierung des Kunden (etwa Ausweisdaten), die im Rahmen der Geeignetheitsprüfung erfassten Informationen, Daten bezogen auf Konto und/oder Wertpapierdepot (etwa Referenzkontoverbindung, Berichte, Wertpapierabrechnungen, Rechnungen) sowie steuerliche Daten (etwa Steueridentifikationsnummer)“ und dass der Versuch unternommen werden könnte, Dritte mit der Identität des Kunden zu täuschen, um sich Vorteile zu verschaffen (Identitätsmissbrauch).

41
Für die Bemessung der Höhe des Schadensersatzes können die Kriterien des Art. 83 Abs. 2 herangezogen werden, wie etwa die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung, die betroffenen Kategorien personenbezogener Daten (vgl. Quaas BeckOK Datenschutzrecht, Wolff/Brink 37. Edition Stand: 01.08.2021 Rn. 31), wobei die Ermittlung im Übrigen dem Gericht nach § 287 ZPO obliegt (BeckOK DatenschutzR/Quaas, 32. Ed. 1.2.2020, DS-GVO Art. 82 Rn. 31).

42
Allerdings muss bei der Bemessung der Höhe des immateriellen Schadensersatzes berücksichtigt werden, dass die streitgegenständlichen Daten offensichtlich bislang noch nicht, jedenfalls nicht zu Lasten des Klägers missbraucht worden sind und von daher allenfalls eine mehr oder weniger hohe Gefährdung angenommen werden kann. Berücksichtigt werden muss jedoch auch - wie oben angesprochen - die gesetzgeberisch beabsichtigte abschreckende Wirkung des Schadensersatzes. Unter Abwägung dieser gesamten Gesichtspunkte erachtet das Gericht einen (immateriellen) Schadensersatz in Höhe von 2.500, - Euro als angemessen.

43
Sofern die Beklagte meint, es sei eine Vorabentscheidung des EuGH zwingend erforderlich, was jüngst das BVerfG, Beschluss von 14.1.2021 - 1 BvR 2853/19 festgestellt hat, so übersieht sie Art. 267 Abs. 3 AEUV. Während nämlich bei dem, der genannten Entscheidung zugrunde liegenden Sachverhalt weder die Berufungsbeschwer erreicht war, noch das Amtsgericht die Berufung zugelassen hatte, ist diese vorliegend unzweifelhaft gegeben (vgl. § 511 Abs. 1, 2 Ziff. 1 ZPO), so dass keine letztinstanzliche Entscheidung gegeben ist.

44
Der Zinsanspruch ergibt sich aus §§ 291, 288 Abs. 1 BGB.

45
Kosten §§ 91 Abs. 1, 92 Abs. 2 Ziff. 2 ZPO; vorläufige Vollstreckbarkeit § 709 ZPO; Streitwert: §§ 3, 5 ZPO, wobei sich das Gericht an der Streitwertvorgabe des Klägers in der Klageschrift orientiert hat.