LG Köln

28 O 328/21

vom 18.05.2022

1.200 € Schadensersatz wegen Verstoß gegen die DSGVO. Hier: Unberechtigter Zugriff auf Nutzerdaten eines Online Finanzdienstleisters; Art. 82 DSGVO.

28 O 328/21 vom 18.05.2022

Urteil | LG Köln | 28. Zivilkammer

Leitsatz der Redaktion

1. Ein Unternehmen, das nach Beendigung der Zusammenarbeit mit einem IT-Dienstleister nicht die diesem überlassenen Zugangsdaten zu seinen IT-Systemen austauscht, verstößt gegen die Pflichten aus Art. 32 und 5 DSGVO.

2. Gerade bei Zugang zu sensiblen Kundendaten darf sich der Verantwortliche nicht darauf verlassen, dass der ehemalige Dienstleister die Zugangsdaten von sich aus löschen wird

3. Für einen Schadensersatzanspruch aus Art. 82 DSGVO genügt es, wenn dieses Versäumnis für einen unberechtigten Zugriff auf Nutzerdaten mitursächlich war

4. Dass das Versäumnis nur mitursächlich war, ist in die nach § 287 ZPO vorzunehmende Schätzung des Schadens aufzunehmen.

Tenor

Die Beklagte wird verurteilt, an den Kläger 1.200 Euro zzgl. Zinsen in Höhe von fünf Prozentpunkten über dem jeweils geltenden Basiszinssatz seit dem 25.10.2021 zu zahlen.

Die Kosten des Rechtsstreits trägt die Beklagte.

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

Tatbestand

Der Kläger begehrt von der Beklagten Schadensersatz wegen eines angeblichen Verstoßes gegen die Vorschriften der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – sogenannte Datenschutz-Grundverordnung (im Folgenden: DSGVO).

Die Beklagte erbringt Wertpapierdienstleistungen, insbesondere in Form der individuellen Vermögensverwaltung für Privatkunden, sowie finanzdienstleistungsnahe Softwaredienstleistungen. Zusätzlich bietet sie Brokerage-Dienstleistungen an und vermittelt Tages-, Fest- und Flexgeldangebote. Der Kläger ist Kunde der Beklagten und unterhält ein Kundenkonto bei dieser. In diesem Zusammenhang stellte er der Beklagten unter anderem die folgenden personenbezogenen Daten zur Verfügung: Vor- und Nachname, Titel, Anschrift, Geburtsdatum, Geburtsort, Geburtsland, Staatsangehörigkeit, E-Mail-Adresse, Telefon/Mobilfunknummer, Familienstand, Steuerliche Ansässigkeit, Steuer-ID und Bankverbindung. Im Rahmen der Registrierung als Neukunde führte der Kläger ein sogenanntes Post-Ident-Verfahren durch, welches die folgenden personenbezogenen Daten zum Gegenstand hat: Ausweisnummer, Datum der Ausstellung, ausstellende Behörde und Ausstellungsland des Personalausweises oder Reisepasses.

Am 19.10.2020 erhielt der Kläger eine E-Mail von der Beklagten mit dem Hinweis auf eine Benachrichtigung, die er in seinem Postfach im Online-Kundenbereich abrufen könne. In dieser Benachrichtigung informierte die Beklagte den Kläger darüber, dass der Schutz seiner personenbezogenen Daten durch einen unrechtmäßigen Zugriff verletzt worden sei. Der Zugriff auf einen Teilbestand von Dokumenten im digitalen Dokumentenarchiv sei „unter Zuhilfenahme von unternehmensinternem Wissen, das nur über entsprechend gesicherte Zugänge verfügbar ist“ erfolgt, jedoch nicht durch die Ausnutzung einer unmittelbar von außen ausnutzbaren technischen Sicherheitslücke. Die in den Dokumenten enthaltenen personenbezogenen Daten des Klägers seien von dem Vorfall betroffen. Es handle sich um folgende Kategorien personenbezogener Daten: 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 Referenzkontenverbindung, Berichte, Wertpapierabrechnungen, Rechnungen) sowie steuerliche Daten (etwa Steueridentifikationsnummer). Zu den möglichen Folgen des Vorfalls erklärte die Beklagte, mit Hilfe der Daten könne versucht werden, die Betroffenen zu bestimmten Verhaltensweisen zu bewegen, insbesondere zur Preisgabe von weiteren vertraulichen Informationen oder Zahlungen zu veranlassen. Weiterhin könne es mit Hilfe der Daten zu Identitätsmissbrauchsversuchen kommen. Wegen der weiteren Einzelheiten wird auf die Anlage K2, Bl. 24 f. d.A. Bezug genommen.

Der unbefugte Zugriff auf die Daten des Klägers war den Hackern mittels Zugangsdaten möglich, die infolge eines Cyber-Angriffs auf die Fa. C. Inc. erlangt worden waren. Hierbei handle es sich um ein weltweit tätiges Unternehmen, das „Software as a Service“-Lösungen für Unternehmen unterschiedlicher Größen und Branchen anbiete und welches bis 2015 in vertraglichen Beziehungen zu der Beklagten stand. Im Rahmen der Vertragsbeziehung waren der Fa. C. die Zugangsdaten zugänglich gemacht worden. Eine Abänderung der Daten nach Ende der Vertragsbeziehung erfolgte beklagtenseits nicht, ebensowenig eine Überprüfung einer Löschung der Daten bei C. durch die Beklagte.

Die Beklagte richtete nach diesem Vorfall auf ihrer Internetseite eine Sonderseite zu „häufig gestellten Fragen zum Datenschutzvorfall bei S. C." ein, welche unter der URL [xxx]/ datenschutzvorfall abgerufen werden kann.

Dort berichtete sie unter der Frage „Sind meine Daten verwendet worden?“, dass einige Kunden unter Verwendung der Daten von Dritten kontaktiert worden seien und Dritte auch zu Journalisten unter Bezugnahme auf den Vorfall Kontakt aufgenommen hätten. Weiter erklärte die Beklagte auf dieser Seite, dass der unbefugte Zugriff auf ihr digitales Datenarchiv anlässlich einer Kundenanfrage am 16.10.2020 festgestellt worden sei und zu drei Zeitpunkten im Zeitraum von April bis Oktober 2020 stattgefunden habe. Von diesem unbefugten Datenzugriff seien insgesamt etwa 33.200 Kunden der Beklagten betroffen gewesen. Wegen der weiteren Einzelheiten wird auf die Anlage K3, Bl. 26 ff. d.A. Bezug genommen.

Nach Bekanntwerden des Datenvorfalls ergriff die Beklagte umfangreiche IT-technische Sofortmaßnahmen, um weitere unberechtigte Zugriffe zu vermeiden, und wandte sich am 19.10.2020 an die zuständigen Behörden, u.a. erstattete sie Strafanzeige bei der Staatsanwaltschaft München I.

Im November 2020 nahm der Kläger das Angebot der Beklagten an, sich als von dem unbefugten Datenzugriff betroffener Kunde kostenfrei für den Identitätsschutz „meine S. P. zu registrieren. Gegenstand des Angebots war die Kostenübernahme durch die Beklagte für das erste Vertragsjahr sowie die Aktivierungsgebühr in Höhe von 9,95 EUR. Bei Nutzung der Dienste über das erste Vertragsjahr hinaus verlängerte sich der Vertrag automatisch um ein weiteres Jahr zu einem Preis in Höhe von monatlich 4,95 EUR (Anlage K3, Bl. 30 f. d.A.).

Der Kläger behauptet, im Rahmen des bei der Registrierung als Neukunde durchgeführten Post-Ident-Verfahrens werde eine digitale Kopie des Personalausweises oder Reisepasses angefertigt. Angesichts des Missbrauchsrisikos hinsichtlich seiner Daten überprüfe der Kläger seit dem Datenvorfall jeden E-Mail- und Rechnungseingang – insbesondere im Zusammenhang mit Online-Käufen – sowie sämtliche Kontobewegungen auf verdächtige Bewegungen. Ihn begleite seit dem Datendiebstahl ein beständiges Gefühl der Unsicherheit.

Der Kläger ist der Auffassung, die Beklagte habe seine personenbezogenen Daten nicht in einer Weise verarbeitet, die eine angemessene Sicherheit der Daten gewährleiste. Anderenfalls wäre ein unbefugter Zugriff auf eine so große Anzahl sensibelster personenbezogener Daten mittels unternehmensinterner Zugangsinformationen nicht möglich gewesen. Falls die Beklagte ein Berechtigungskonzept gehabt habe, sei dieses ungenügend und die Daten nicht ausreichend segmentiert gewesen. Auch wäre es bei Implementierung angemessener Sicherheitsmaßnahmen nicht möglich gewesen, dass eine solch große Menge an Daten unbemerkt bewegt wird, ohne dass dies sofort auffalle. Die Beklagte habe selbst angegeben, dass der unbefugte Zugriff erst durch eine Kundenanfrage bemerkt worden sei. Dafür, dass zum Zeitpunkt des unbefugten Zugriffs keine hinreichenden Sicherheitsmaßnahmen implementiert gewesen seien, spreche auch die

Tatsache, dass die Beklagte nach dem Sicherheitsvorfall Maßnahmen ergriffen habe, um die unrechtmäßigen Zugriffe auf die Daten auszuschließen.

Weiter meint der Kläger, er habe aufgrund des unbefugten Zugriffs einen irreversiblen Schaden erlitten. Aufgrund des mit dem Datenschutzvorfall einhergehenden Risikos des Identitätsmissbrauchs stehe fest, dass die betroffenen Daten der Kontrolle des Klägers nunmehr dauerhaft entzogen seien. Insbesondere handle es sich dabei auch um Daten, die im Laufe des Lebens gerade keiner Änderung unterliegen, was bedeute, dass selbst durch einen Umzug oder den Wechsel der E-Mail- Adresse und der Handynummer der Kontrollverlust nicht ausgeglichen werden könne. Der Kläger müsse täglich damit rechnen, dass Dritte in seinem Namen Verträge schließen oder Zahlungen veranlassen. Er müsse damit leben, dass Daten, die typischerweise ausschließlich der Identifikation des Klägers dienen (wie Geburtsdatum und -ort), irgendwo im Darknet kursierten. Die durch den Datenschutzvorfall veranlasste akribische Kontrolle sämtlicher Kontobewegungen und Briefe sowie E-Mails bedeute eine irreversible Einschränkung für die Teilnahme des Klägers am Rechts- und Geschäftsverkehr, die auch durch die Inanspruchnahme von Diensten, wie etwa „meine Schufa plus“ nicht hinreichend ausgeglichen werden könne. Die Gefahr des Identitätsmissbrauchs verringere sich auch nicht im Laufe der Zeit, weil die Daten auch nach Jahrzehnten noch im Darknet kursierten und dort verkauft würden. Daran, dass andere Betroffene bereits Erpresser-E-Mails erhalten hätten, zeige sich, dass die Daten bereits in den Händen Krimineller seien. Der Kläger müsse dauerhaft damit leben, dass sich das Risiko eines Identitätsmissbrauchs realisieren könnte. Die Entwendung seiner Telefonnummer und E-Mailadresse seien per se mit dem Risiko verbunden, dass diese für Spam-Nachrichten genutzt würden. Dem durch einen Wechsel zu begegnen bedeute einen immensen Aufwand und einen teilweisen Verlust der Erreichbarkeit.

Schließlich ist der Kläger der Ansicht, er habe durch den Datenschutzvorfall auch einen Schaden dahingehend erlitten, dass ihm in diesem Zusammenhang ein enormer persönlicher Aufwand entstanden sei, etwa durch die eigene Auseinandersetzung mit der Materie, eigene Recherchen, die Überprüfungsmaßnahmen des eigenen Kontos sowie die Nutzung des Dienstes „meine S[xxx] plus“.

Der Kläger beantragt,

> die Beklagte zu verurteilen, an den Kläger einen angemessenen immateriellen Schadenersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, jedoch mindestens EUR 5.001,00, zzgl. Zinsen in Höhe von fünf Prozentpunkten über dem jeweils geltenden Basiszinssatz seit Rechtshängigkeit (25.10.2021) zu zahlen.

Die Beklagte beantragt,

> die Klage abzuweisen.

Sie behauptet, die von dem Datenvorfall betroffenen Daten des Klägers seien bereits Gegenstand früherer Datenvorfälle gewesen, die sich bei anderen Unternehmen zugetragen hätten. Der Personalausweis des Klägers sei nicht wegen der Art der

Identifizierung des Klägers über das Post-Ident-Verfahren von dem Datenvorfall betroffen gewesen. Insbesondere sei die Nummer des Personalausweises nicht betroffen gewesen. Die Beklagte habe über keine Kopie des Ausweises verfügt. Weiter behauptet die Beklagte, auch die im Rahmen einer Geeignetheitsprüfung erfassten Informationen sowie – mit Ausnahme der IBAN des Referenzkontos – Daten über das Wertpapierdepot oder Verrechnungskonto seien nicht betroffen gewesen. Der Kläger habe lediglich Brokerage-Dienstleistungen in Anspruch genommen, sodass eine Geeignetheitsprüfung nicht stattgefunden habe. Eine Zugriffsmöglichkeit auf Kundenpasswörter habe zu keinem Zeitpunkt bestanden, sodass das Vermögen des Klägers bei der Depotbank zu keinem Zeitpunkt gefährdet gewesen sei.

Die Beklagte bestreitet mit Nichtwissen, dass der Kläger sämtliche E-Mail- und Rechnungseingänge sowie Kontobewegungen auf verdächtige Bewegungen überprüfe. Weiter bestreitet sie, dass sich Dritte die Identität des Klägers angeeignet hätten, der Kläger seine E-Mail-Adresse und Handynummer nicht von Spam freihalten könne und er im Zusammenhang mit dem Datenvorfall den von ihm vorgetragenen „persönlichen Aufwand“ betrieben habe. Mit Nichtwissen bestreitet die Beklagte zudem, dass andere Betroffene Erpresser-E-Mails erhalten hätten. Nach ihrer Kenntnis habe es lediglich in sehr geringer Anzahl Kontaktaufnahmen zu Kunden gegeben. Hierzu hätten die Ermittlungsbehörden die Vermutung geäußert, dass durch die Kontaktaufnahmen mit den Kunden seitens der Angreifer Druck auf die Beklagte ausgeübt werden sollte.

Die Beklagte ist der Auffassung, ihr falle kein Verstoß gegen die Datenschutz-Grundverordnung zur Last. Ihre technischen und organisatorischen Maßnahmen, zu denen sie im Einzelnen vorträgt, seien zu jeder Zeit und in jeder Hinsicht angemessen. Dies werde zum einen dadurch verdeutlicht, dass sie zum Zeitpunkt des Datenvorfalls hinsichtlich ihres Informationssicherheitsmanagements über eine Zertifizierung durch den TÜV Rheinland nach dem allgemein anerkannten ISO 27001:2013-Standard verfügte. Zum anderen hätten die zuständigen Datenschutzbehörden weder nach dem Datenschutzvorfall noch zu einem anderen Zeitpunkt ein Verfahren oder andere Maßnahmen aufgrund datenschutzrechtlicher Unzulänglichkeiten gegen sie eingeleitet.

Die Beklagte behauptet, sie nutze für die Abwicklung des gesamten Kundengeschäfts eine sichere standardisierte IT-Infrastruktur mit u.a. Applikations- und Datenbankservern, Speicherkapazitäten, Redundanzsystemen und Backup-Lösungen. Das von dem unbefugten Zugriff betroffene Dokumentenarchiv, in dem ein Teil der Kundendaten in getrennten Ordnern gespeichert gewesen sei, sei mittels des hochwirksamen Verschlüsselungsverfahrens AES-256 (sog. Advanced Encryption Standard, also symmetrisches Verschlüsselungsverfahren) verschlüsselt. Damit seien Kundendaten im sog. „Ruhezustand“ permanent verschlüsselt. Diese dem Dokumentenarchiv zu Grunde liegende IT-Infrastruktur sei nach IEC 27001:2013, 27017:2015, 27018:2019, ISO/IEC 9001:2015 und CSA STAR CCM v3.0.1 zertifiziert. Die Beklagte verwalte Daten (einschließlich Kundendaten) entsprechend einer systemseitigen Vorgabe in separaten Sub-Umgebungen, welche vollständig eigenständige Umgebungen mit jeweils eigenen Infrastruktur-Ressourcen darstellten. Auch die Verarbeitung der Kundendaten im betroffenen Dokumentenarchiv

geschehe mit einer entsprechenden Segmentierung, also mittels getrennter Ordner, für die die Zugriffsrechte entsprechend eingeschränkt seien. Der Zugang durch einen Anwender erfordere stets die Eingabe der individuellen Zugangsdaten sowie aufgrund der vorgeschriebenen „Mehr-Faktor-Authentifizierung“ die Eingabe eines weiteren Berechtigungsmerkmals. Der Zugriff auf die Daten selbst sei ferner ausschließlich im Umfang der dem jeweiligen Benutzer zuvor verliehenen Berechtigungen möglich. Die konkreten Berechtigungen eines Benutzers würden nach dem strikten „Need-to-Know“-Prinzip (Erforderlichkeitsgrundsatz) vergeben, also in Abhängigkeit davon, welche Berechtigungen der Anwender angesichts seiner Funktion tatsächlich benötigt. Das digitale Benutzermanagement wiederum, also die Einrichtung und Löschung von Benutzern sowie die Zuweisung individueller Zugriffsmöglichkeiten sei nur mit spezifischen, eingeschränkt vergebenen Berechtigungen möglich.

Die Beklagte behauptet weiter, sie habe im Übrigen weitere Sicherungsmechanismen, etwa in Form von gesicherten/verschlüsselten VPN-Verbindungen und „IP-Whitelisting“ (Beschränkung des Zugangs auf bestimmte Endgeräte) vorgegeben.

Zudem verfüge die Beklagte über ein umfassendes, schriftlich fixiertes Informationsrisiko- und Informationssicherheitsmanagement. Es sei in zahlreichen Regelwerken detailliert niedergelegt und regele insbesondere die Zugangs- und Zugriffskontrolle sowie die Verarbeitung von und den Umgang mit Kundendaten. Die Beklagte habe eine strenge Zugangs- und Zugriffskontrolle implementiert, welche eine Mehr-Faktor-Authentifizierung, detaillierte Regelungen zur Passwortvergabe und zum Umgang mit Passwörtern sowie ein granulares Rechte- und Rollenkonzept beinhalte, wonach Kundendaten die höchste verfügbare Sicherheitsstufe „Strictly Confidential“ zugewiesen sei. Die genannten Maßnahmen zur Zugangs- und Zugriffskontrolle würden regelmäßig auf Aktualität und Wirksamkeit geprüft. Der Zugriff u.a. auf das Dokumentenarchiv werde zudem durch Maßnahmen zur Erkennung, Überwachung und zeitnahen Reaktion kontrolliert. Insbesondere würden Zugriffe von Benutzern durch digitale Sicherheitsdienste geloggt und dokumentiert.

Ferner behauptet die Beklagte, sie weise ihre Mitarbeiter an, die zahlreichen vorhandenen Sicherheitsfeatures (wie Firewalls, Virenscanner, VPN-Verbindungen und Verschlüsselungsdienste) stets aktiviert zu halten und lediglich freigegebene Hard- und Software zu verwenden. Die Mitarbeiter würden regelmäßig hinsichtlich der Compliance-Vorgaben geschult, was die IT- und Informationssicherheit sowie den Datenschutz umfasse. Auch würden die Mitarbeiter auf Meldepflichten, insbesondere im Hinblick auf Datenvorfälle aufmerksam gemacht. Die Beklagte lasse regelmäßig externe sowie interne Prüfungen und Audits durchführen, wie etwa Penetrations- und Applikationstests und Prüfungen im Rahmen der Re-Zertifizierung nach ISO 27001:2013. Nach Auswertung der Ergebnisse dieser Prüfungen würden etwaige Optimierungsmaßnahmen umgesetzt, was wiederum mittels sogenannter „Re-Tests“ nachvollzogen und bewertet würde. Zum Zeitpunkt des Datenvorfalls habe die Zertifizierung nach ISO 27001:2013 für einen Gültigkeitszeitraum von 12.03.2018 bis 11.03.2021 vorgelegen (Anlage B1, Bl. 98 ff. d.A.). Anfang des Jahres 2021 habe die Beklagte trotz des Datenvorfalls nach erfolgreichem Re-

Zertifizierungs-Audit ein neues Zertifikat erhalten (Anlage B2, Bl. 102 ff. d.A.). Der TÜV Rheinland als unabhängige Prüfstelle habe der Beklagten bescheinigt, dass „das Managementsystem der Organisation die Anforderungen der Norm(en) erfüllt und angemessen aufrechterhalten sowie umgesetzt wird“, „eine ausgereifte Vorgehensweise bei der Softwareentwicklung“ sowie ein „[h]ohes Sicherheitsbewusstsein der Beteiligten“.

Die Beklagte ist der Auffassung, sie sei „Kollateralopfer“ des Cyber-Angriffs auf C. , nicht hingegen eines „Hack“ ihres Systems. Auch seien die unternehmensinternen Informationen nicht von einem (menschlicher) Benutzer, etwa einem Mitarbeiter der Beklagten, zur Verfügung gestellt worden. Das hätten die zuständigen Strafverfolgungsbehörden nach eingehender Ermittlung und Prüfung ausgeschlossen. Der unbefugte Zugriff sei auch trotz angemessener Sicherheitsvorkehrungen für die Beklagte nicht voraussehbar gewesen.

Wegen der näheren Einzelheiten des Sach- und Streitstands wird auf den Inhalt der zwischen den Parteien gewechselten Schriftsätze nebst Anlagen, die Gegenstand der mündlichen Verhandlung waren, Bezug genommen.

I.

1 Die Klage ist zulässig. Das Landgericht Köln ist gemäß §§ 44 Abs. 1 S. 1 DSGVO, 1 2 ZPO örtlich zuständig.

II.

2 Die Klage ist teilweise begründet.

3 1.

4 Der Kläger hat im tenorierten Umfang Anspruch auf Ersatz eines immateriellen Schadens aus Art. 82 Abs. 1 DSGVO. 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.

5 Die Beklagte hat dadurch, dass sie die der Fa. C. zur Verfügung gestellten Zugangsdaten nach Ende der Vertragsbeziehung nicht änderte, gegen ihre Verpflichtung aus Art. 32 DSGVO sowie aus Art. 5 DSGVO verstoßen. Nach Art. 32 DSGVO haben der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und

Freiheiten natürlicher Personen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Gemäß Art. 5 Abs. 1 lit. f) DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

6 Die Kammer nimmt einen Verstoß gegen diese Vorgaben aufgrund des zwischen den Parteien unstreitigen Umstandes an, dass die der Fa. C. zur Verfügung gestellten Zugangsdaten nach Beendigung der vertraglichen Beziehung zu der Vertragspartnerin über mehrere Jahre nicht verändert wurden. Damit schuf die Beklagte das Risiko, dass die Daten der Betroffenen nicht nur im Falle von ihr selbst zu verantwortender Unzulänglichkeiten, sondern auch durch von Seiten von Mitarbeitern der C. vorsätzlich oder fahrlässig ermöglichte Zugriffe einem Missbrauch ausgesetzt waren. Die Beklagte kann sich angesichts der Sensibilität der gespeicherten Kundendaten insbesondere nicht darauf berufen, sie habe davon ausgehen können, dass die Daten seitens C. dauerhaft und vollständig gelöscht werden würden (so auch in einem Parallelfall LG München I, Urt. v. 9.12.2021, 31 O 16606/20, juris, Rn. 36). Jedenfalls wäre eine Überprüfung der Löschung angezeigt gewesen, die die Beklagte aber ebenfalls nicht vorträgt.

7 Das der Beklagten anzulastende Versäumnis war – was ausreichend ist – jedenfalls mitursächlich für den dem Kläger entstandenen Schaden (vgl. LG München I a.a.O. Rn. 39).

8 Dem Kläger entstand auch ein Schaden im Sinne des Art. 82 DSGVO. 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, weil nur so eine effektive Durchsetzung des EU-Rechts – und damit auch der DS-GVO – gewährleistet ist (LG München I a.a.O. Rn. 41 mit w.N.).

9 Aufgrund des dem Kläger mit Schreiben vom 19.10.2020 mitgeteilten Umfangs der entwendeten persönlichen Daten geht die Beklagte ausweislich dieses Schreibens selbst davon aus, dass versucht werden konnte, die Betroffenen zu bestimmten Verhaltensweisen zu bewegen, insbesondere zur Preisgabe von weiteren vertraulichen Informationen oder Zahlungen zu veranlassen, sowie dass die Gefahr bestand, dass es mit Hilfe der Daten zu Identitätsmissbrauchsversuchen kommen würde. Auf die weiteren, teilweise zwischen den Parteien streitigen, Umstände der tatsächlichen oder gefühlten Beeinträchtigung des Klägers durch den Vorfall kommt es nach Auffassung der Kammer vor diesem Hintergrund nicht maßgeblich an.

10 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, wobei die Ermittlung im Übrigen dem Gericht nach § 287 ZPO obliegt (LG München I a.a.O. Rn. 44 m.w.N.).

11 Hier war bei der Bemessung der Höhe zu berücksichtigen, dass ein Missbrauch der Daten zu Lasten des Klägers bislang nicht festgestellt werden musste, und es daher einstweilen bei einer Gefährdung geblieben ist. Wie vom LG München I a.a.O. zutreffend herausgearbeitet, muss allerdings auch die Absicht des EU-Verordnungsgebers berücksichtigt werden, mit Hilfe des Schadensersatzanspruchs eine abschreckende Wirkung zu erzielen. Zu Gunsten der Beklagten fällt allerdings – wie in der mündlichen Verhandlung bereits ausgeführt, ins Gewicht, dass der ihr zuzurechnende Datenschutzverstoß nur eine von mehreren Ursachen war, die erst im Zusammenwirken den Schadenseintritt bewirkten. Denn hinzu kam ein weiterer mindestens fahrlässiger Verstoß bei der Fa. C. sowie nicht zuletzt das vorsätzliche rechtswidrige Vorgehen der Hacker selbst. Zu berücksichtigen ist auch, dass die Beklagte dem Kläger vorübergehend das „meine Schufa Plus“ Angebot finanzierte. Unter Abwägung der maßgeblichen Gesichtspunkte erachtet die Kammer damit eine Schadensersatzzahlung in der tenorierten Höhe für angemessen.

12 Der Zinsanspruch ist aus §§ 291, 288 Abs. 1 BGB gerechtfertigt.

13 2.

14 Da die Kammer nicht letztinstanzlich entscheidet, ist eine Vorabentscheidung des Europäischen Gerichtshofs auch nach Maßgabe des Beschlusses des Bundesverfassungsgerichts vom 14.1.2021 – 1 BvR 2853/19 – nicht erforderlich.

III.

[redacted]

15 Die prozessualen Nebenentscheidungen beruhen auf §§ 92 Abs. 2 Nr. 2, 708 Nr. 11, 711 ZPO.

16 Streitwert 5.001 Euro.