LG München I, Endurteil v. 14.03.2024 – 44 O 3464/23

Titel:

Kein Schadensersatz bei Verstoß gegen DS-GVO – Scraping

Normenkette:

DS-GVO, Art. 75, Art. 82 Abs. 1, Art. 85, Art. 146

Leitsätze:

1. Die von der DS-GVO verwandten Begriffe "immaterieller" und "materieller" Schaden sind unionsautonom auszulegen und setzen nach dem Wortlaut der Norm, der Systematik und Telos des Art. 82 Abs. 2, Abs. 1 DS-GVO sowie der Art. 77-84 DS-GVO und den Erwägungsgründen 75, 85 und 146 DS-GVO einen über den schlichten Verstoß gegen die DS-GVO hinausgehenden Schaden voraus. (Rn. 31) (redaktioneller Leitsatz)

2. Ein Kontrollverlust durch Scraping, also bei unbefugter Offenlegung/unbefugtem Zugänglichmachen, betraf als generelles Risiko der (unrechtmäßigen) Verarbeitung alle Personen, deren Daten ohne Rechtfertigungsgrund suchbar waren, gleichermaßen. (Rn. 31) (redaktioneller Leitsatz)

Schlagworte:

Scraping, Kontrollverlust, immaterieller Schaden

Fundstelle:

BeckRS 2024, 5479

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 Juli bis Oktober 2020 entstehen werden.

2. Im Übrigen wird die Klage abgewiesen.

3. Von den Kosten des Rechtsstreits haben der Kläger 6/7 und die Beklagte 1/7 zu tragen.

4. Das Urteil ist vorläufig vollstreckbar. Der Kläger kann die Vollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110% des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110% des zu vollstreckenden Betrags leistet. 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 7.000,00 € festgesetzt.

Tatbestand

1
Der Kläger begehrt von der Beklagten immateriellen Schadensersatz aus Art. 82 Abs. 1 DSGVO, Feststellung der Haftung bezüglich künftiger materieller Schäden, Unterlassung, Auskunft und weiteren Schadensersatz wegen verspäteter Auskunft aufgrund eines Datenvorfalls.

2
Die Beklagte ist ein Wertpapierinstitut mit Sitz in M. und bietet ihren Kunden Konten für eine digitale Vermögensverwaltung bzw. Depots für den Aktienhandel an. Der Kläger registrierte sich im Juli 2020 als Kunde der Beklagten mittels Post-Ident-Verfahren und übermittelte ihr zu diesem Zweck folgende personenbezogenen Daten: Vor- und Nachname, Anschrift, E-Mail-Adresse, Handynummer, Geburtsdatum, Geburtsort und Geburtsland, Staatsangehörigkeit, Familienstand, steuerliche Ansässigkeit und Steuer-ID, IBAN und eine Kopie seines Personalausweises.

3
Am 15./16.04.2020, 05./06.08.2020 sowie am 10./11.10.2020 kam es bei der Beklagten zu einem unbefugten Zugriff Dritter auf elektronisch gespeicherte, personenbezogene Daten im digitalen Dokumentenarchiv; insgesamt wurden bei diesen drei Zugriffen 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 (im Folgenden:), erlangt hatten. ist ein IT-Unternehmen, das Cloud-Dienstleistungen anbietet. Die Beklagte nahm bis Ende 2015 Dienstleistungen von in Anspruch, weshalb dort Zugangsinformationen zum IT-System der Beklagten hinterlegt waren. Die Beklagte hatte diese Zugangsdaten nach Ende der Vertragsbeziehungen im Jahr 2015 bis zu den streitgegenständlichen Datenvorfällen 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.

4
Im Oktober 2020 wurde der Kläger durch die Beklagte informiert, dass er von dem Datenvorfall betroffen ist und dass seine Personalien, Kontakt- und Ausweisdaten sowie auf das Kundenkonto bezogene Daten wie die Referenzkontoverbindung und steuerliche Daten wie die Steuer-ID erlangt wurden. Die Beklagte wies darin auf die Gefahr eines Identitätsmissbrauchs hin und empfahl besonders auf Phishing, ungewöhnliche Kontobewegungen und die Abfrage vertraulicher Zugangsdaten zu achten.

5
Mit Schreiben vom 21.12.2022 forderte der Kläger die Beklagte dazu auf, ihm Datenauskunft zu erteilen (Anlage K1). Die Beklagte antwortete mit Schreiben vom 03.01.2023 (mit Anlage B13 als Anlage) und vom 05.01.2023 (Anlage K2, ebenfalls mit Anlage B13 als Anlage).

6
Der Kläger trägt vor, dass er durch den Datenvorfall einen Kontrollverlust über seine personenbezogenen Daten erlitten; es bestehe die unmittelbare Gefahr eines Identitätsdiebstahls. Das Risiko könne sich jederzeit verwirklichen und werde auch durch Zeitablauf nicht geringer, da der Datensatz im Darknet verfügbar sei und der Kläger einige der betroffenen Daten nicht ändern könne. 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.

7
Der Kläger ist der Auffassung, dass es einen Verstoß gegen Art. 5 Abs. 1 lit. f) DSGVO i.V.m. Art. 32 DSGVO darstelle, dass die Beklagte nach Beendigung der Vertragsbeziehungen zu die Zugangsdaten zu ihrem Dokumentenarchiv nicht geändert habe bzw. nicht überprüft habe, ob die an überlassenen Zugangsdaten noch aktiv genutzt werden könnten. Es sei zudem mindestens grob fahrlässig, dass die Beklagte ihr System auch nach der Information von über den Angriff nicht überprüft habe. Der Kläger 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 3.000,00 € erforderlich sei.

8
Der Kläger beantragt zuletzt,

1. Die Beklagte wird verurteilt, an den Kläger als Ausgleich für Datenschutzverstöße einen immateriellen Schadenersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von € 3.000,00 jedoch nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über dem jeweiligen Basiszinssatz seit Rechtshängigkeit zu zahlen.

2. 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 Juli bis Oktober 2020 noch entstehen werden.

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu € 250.000,00, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckenden Ordnungshaft bis zu 6 Monaten, im Wiederholungsfall bis zu 2 Jahren, zu unterlassen, personenbezogene Daten der Klägerseite, nämlich Vor- und Nachname, Titel, Anschrift, Geburtsdatum, Geburtsort, Geburtsland, Staatsangehörigkeit, E-Mail-Adresse, Telefon, Mobilfunknummer, Familienstand, steuerliche Ansässigkeit, Steuer-ID, Bankverbindung, Ausweiskopie, Portraitfoto, Dritten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzunehmen und ohne, dass eine Einwilligung des Klägers vorliegt oder ein Rechtfertigungsgrund nach der DSGVO.

4. Die Beklagte wird verurteilt, dem Kläger Auskunft über die personenbezogenen Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten erlangt werden konnten.

5. Die Beklagte wird verurteilt, an die Klägerin für die Nichterteilung einer den gesetzlichen Anforderungen entsprechenden außergerichtlichen Datenauskunft i.A.d. Art. 15 DSGVO einen weiteren immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von € 2000,00 aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über den jeweiligen Basiszinssatz zu zahlen.

6. Die Beklagte wird verurteilt, die Klägerseite von den außergerichtlichen entstandenen Kosten für die anwaltliche Rechtsverfolgung in Höhe von € 1.390,87 nebst Zinsen in Höhe von 5%-Punkten über dem jeweiligen Basiszinssatz der EZB ab Rechtshängigkeit freizuhalten.

9
Die Beklagte beantragt,

die Klage abzuweisen.

10
Die Beklagte trägt vor, der Datenvorfall sei nicht etwa durch Lücken oder Mängel in den Sicherheitssystemen der Beklagten selbst erfolgt. Vielmehr seien die eigenen technischen und organisatorischen Maßnahmen zur Datensicherheit angemessen und ausreichend gewesen. Gegen die Beklagte habe die Datenschutzbehörde kein Bußgeldverfahren aufgrund des Vorfalls eingeleitet.

11
Die Beklagte nutze für die Abwicklung des gesamten Kundengeschäfts insbesondere eine sichere standardisierte IT-Infrastruktur mit Applikations- und Datenbankservern, Speicherkapazitäten, Redundanzsystemen und Backup-Lösungen. Die Kundendaten seien segmentiert gespeichert, das Berechtigungskonzept sehe ausschließlich individuelle nach dem „Need-to-Know“-Prinzip vergebene Zugriffsmöglichkeiten und eine strenge Zugangskontrolle sowie kontinuierliche Überwachung vor.

12
Die Beklagte macht geltend, sie habe davon ausgehen dürfen, dass als führender Dienstleister mit gehobenem Datensicherheitskonzept die Zugangsinformationen vollständig und dauerhaft gelöscht habe, da die Firma zu einer Löschung der zur Ausführung der Softwaredienstleistungen erhaltenen und nach Vertragsbeendigung nicht mehr benötigten Zugangsinformationen vertraglich verpflichtet gewesen sei. Die Zugangsinformationen seien nach Auskunft von in Back-Up-Systemen hinterlegt gewesen und dort abgegriffen worden. Zu dem Zeitpunkt als die Zugangsinformationen erhalten habe, habe das Dokumentenarchiv keinerlei Kundendaten enthalten.

13
Die Beklagte ist Ansicht, die Klage sei unzulässig, weil der Klageantrag zu Ziffer 1 und 3 nicht hinreichend bestimmt sei. Dem Unterlassungsanspruch fehle überdies das Rechtsschutzbedürfnis. Dem Feststellungsanspruch in Ziffer 2) fehle das Feststellungsinteresse.

14
Ein Verstoß der Beklagten gegen Art. 32 DSGVO liege nicht vor. 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. 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 begründen könnte. Eine Verpflichtung jeglichen Datenvorfall zu verhindern, bestehe gerade nicht. Aus einem Datenleck allein könne nicht auf eine Pflichtverletzung der Beklagten geschlossen werden.

15
Eine verbindliche Vorgabe zur regelmäßigen Änderung von Zugangsinformationen bestehe nicht; in bestimmten Fällen werde davon sogar ausdrücklich abgeraten. Die Beklagte habe ihren Pflichten genügt und auf nach der Vertragsbeendigung die Daten vollständig und dauerhaft löschen würde. Da die Mitteilung von vom 30.09.2022 über den Angriff sich nur an aktuelle Kunden gerichtet habe, habe die Beklagte die Relevanz der Information für sie selbst nicht erkennen können.

16
Davon unabhängig habe die Beklagte unmittelbar nach Bekanntwerden reagiert, durch Informaton der Betroffenen sowie der Behörden und durch das Angebot für „meinSCHUFA plus“ und die Kostenübernahme für einen neuen Personalausweis. Eine Haftung der Beklagten komme nicht in Betracht, da es an einem Verschulden gem. Art. 82 Abs. 3 DSGVO fehle.

17
Dem Kläger sei tatsächlich weder ein immaterieller noch gar ein materieller Schaden entstanden. Der Vorfall habe sich 2020 zugetragen und bislang sei es nicht zu einem Identitätsdiebstahl gekommen. Ein bloßer Kontrollverlust genüge nicht für die Annahme eines immateriellen Schadens. Etwaige Spam-Nachrichten oder Anrufe ließen sich 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, und seien zudem lediglich als Unannehmlichkeiten zu werten, die die Schwelle zu einem immateriellen Schaden bereits nicht überschreiten würden.

18
Jedenfalls sei die Forderung der Höhe nach deutlich überzogen, da kein Datenmissbrauch stattgefunden habe und Art. 82 DSGVO gerade nicht der Abschreckung diene sondern eine reine Ausgleichsfunktion habe.

19
Das Verlangen nach Auskunft gem. Art. 15 DSGVO sei überobligatorisch durch Schreiben vom 05.01.2023 (Anlage K2), Schreiben vom 03.01.2023 (Anlage B13) und Schreiben vom 08.05.2023 bzw. 09.05.2023 erfüllt worden.

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 08.02.2024 Bezug genommen.

Entscheidungsgründe

21
Die Klage erweist sich als teilweise zulässig und teilweise begründet.

A.

22
Die Klage ist nur zum Teil zulässig.

23
Das LG München 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
Der Kläger hat 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 in juris). Diese Möglichkeit ist vorliegend gegeben, da die Angreifer weiterhin Zugriff auf die Daten des Klägers haben. Dass der Kläger sich einen neuen Ausweis hat ausstellen lassen und somit der vorherige Ausweis, dessen Lichtbild erlangt wurde, ungültig geworden ist, ändert daran nichts, da weiterhin die Möglichkeit eines Schadens aufgrund der erlangten Daten besteht – insbesondere, weil der Kläger einen Teil der Daten nicht bzw. kaum verändern kann (wie sein biometrisches Passbild, die Körpergröße und die Unterschrift). Die bestimmte Wahrscheinlichkeit eines Schadens ist nicht erforderlich, es genügt die weiterhin bestehende Möglichkeit. 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. 4, Rn. 7 bei juris).

25
Die Klageanträge unter Ziffer 3 erweist sich als unzulässig. Der Antrag ist nicht ausreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO. Ein Klageantrag ist dann hinreichend bestimmt, wenn er den erhobenen Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) absteckt, Inhalt und Umfang der materiellen Rechtskraft der gerichtlichen Entscheidung (§ 322 ZPO) erkennen lässt, das Risiko eines Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeiten auf die Beklagte abwälzt, für diesen erkennbar macht, um was es geht, und schließlich eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (Anders/Gehle/Anders, 81. Aufl. 2023, ZPO § 253 Rn. 34 m.w.N.).

26
Hieran fehlt es vorliegend bezüglich des Klageantrags unter Ziffer 3, denn die Klageseite begehrt mit ihrem Antrag eine Unterlassung der Zugänglichmachung von Daten an Dritte „ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzunehmen“. Dies entspricht wortwörtlich dem Wortlaut des Art. 32 DSGVO. Abgesehen davon, dass dies keinen vollstreckungsfähigen Inhalt darstellt, und die Beklagte somit ihr Risiko nicht abschätzen kann und ihr Verhalten nicht darauf einrichten kann, besteht gerade Streit zwischen den Parteien, welche Maßnahmen nach der DSGVO für die Sicherheit der betreffenden Daten erforderlich und geboten sind. Der Streit zwischen den Parteien würde damit ins Vollstreckungsverfahren getragen. Der Begründung ist auch keine bestimmbare einschränkende Auslegung zu entnehmen.

27
Auch die Formulierung „ohne dass eine Einwilligung des Klägers vorliegt“ ist zu unbestimmt, da es einer rechtlichen Bewertung des Vollstreckungsorgans bedarf, ob eine rechtlich wirksame Einwilligung des Klägers vorliegt. Gleiches gilt für die Formulierung „oder ein Rechtfertigungsgrund nach der DSGVO“.

28
Im Übrigen bestehen keine Zweifel an der Zulässigkeit der Klage. Die Zahlungsanträge sind hinreichend bestimmt. Insbesondere kann ein Zahlungsanspruch auf mehrere Sachverhalte gestützt werden.

B.

29
Die Klage ist nur zum Teil begründet.

30
Der Klageantrag zu 1) ist unbegründet.

31
Unabhängig davon, ob seitens der Beklagten überhaupt eine schadenskausale Pflichtverletzung, die in den Anwendungsbereich des Art. 82 DSGVO fiele, angelastet werden kann, hat die Klagepartei jedenfalls das Vorliegen eines Schadens weder ausreichend dargelegt, noch bewiesen. Voraussetzung für sämtliche klägerischen Anspruchsgrundlagen, welche den Schadensersatzanspruch tragen würden, wäre nämlich, dass dem Kläger überhaupt ein kausaler Schaden entstanden ist. Das OLG Hamm führt hierzu in seinem Urteil vom 15.8.2023 – 7 U 19/23 aus:

„(aa) Die von der DSGVO verwandten Begriffe „immaterieller“ und „materieller“ Schaden sind unionsautonom auszulegen und setzen – entgegen dem Ansatz der Klägerin – nach dem Wortlaut der Norm, der Systematik und Telos des Art. 82 Abs. 2, Abs. 1 DSGVO sowie der Art. 77-84 DSGVO und den

Erwägungsgründen 75, 85 und 146 DSGVO einen über den schlichten Verstoß gegen die DSGVO hinausgehenden Schaden voraus (so EuGH Urt. v. 4.5.2023 – C-300/21, GRUR-RS 2023, 8972 Rn. 29-42; GA Campos Sánchez-Bordona Schlussantr. v. 6.10.2022 – C-300/21, GRUR-RS 2022, 26562 Rn. 117).

Das heißt, dass im Rahmen des haftungsbegründenden Tatbestands des Art. 82 Abs. 2, Abs. 1 DSGVO zunächst zwischen einem haftungsrelevanten Datenschutzverstoß einerseits und einem – materiellen oder immateriellen – Schaden andererseits zu differenzieren ist. Beide sind nicht deckungsgleich, sondern selbständige Voraussetzungen im Rahmen des Art. 82 DSGVO, die kumulativ vorliegen müssen.

Ein solcher Schaden setzt jedoch – entgegen möglicherweise bestehendem innerstaatlichen Recht (vgl. für das deutsche Deliktsrecht zuletzt etwa BGH Urt. v. 6.12.2022 – VI ZR 168/21, r+s 2023, 130 Rn. 18 m. w. N.) – nach Wortlaut, Erwägungsgründen 10, 146 DSGVO und Telos nicht voraus, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat (so EuGH Urt. v. 4.5.2023 – C-300/21, GRUR-RS 2023, 8972 Rn. 44-51; vgl. auch BAG Beschluss vom 26.8.2021 – 8 AZR 253/20 (A), NZA 2021, 1713 Rn. 33; offen gelassen BVerfG Beschluss vom 14.1.2021 – 1 BvR 2853/19, NJW 2021, 1005 Rn. 19 ff.; siehe zu Störungen und Belästigungen sowie Zorn und Ärger in Abgrenzung gegenüber Schäden GA Campos Sánchez-Bordona Schlussantr. v. 6.10.2022 C-300/21, GRUR-RS 2022, 26562 Rn. 111 ff.; GA Pitruzzella Schlussanträge v. 27.4.2023 – C-340/21, BeckRS 2023, 8707 Rn. 79 ff. und insbesondere Rn. 83 zur von den nationalen Gerichten zu beantwortenden Frage des Schadens im Einzelfall).Auch wenn es keine Erheblichkeitsschwelle gibt, so bedeutet dies indes nicht, dass die aus dem Datenschutzverstoß resultierenden negativen Folgen per se einen haftungsbegründenden Schaden darstellen; denn der EuGH führt hierzu explizit aus, dass diese Auslegung nicht bedeutet, „dass eine Person, die von einem Verstoß gegen die DSGVO betroffen ist, der für sie negative Folgen gehabt hat, vom Nachweis befreit wäre, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 dieser Verordnung darstellen [Hervorhebungen hinzugefügt]“ (EuGH Urt. v. 4.5.2023 – C-300/21, GRUR-RS 2023, 8972 Rn. 50 und das in dem Bewusstsein der konkret vom ÖOGH zum Kontrollverlust aufgeworfenen Frage, vgl. Rn. 17). Entsprechend stellt der EuGH auch darauf ab, dass die „konkret erlittenen Schäden“ vollständig ausgeglichen werden müssen (vgl. EuGH Urt. v. 4.5.2023 – C-300/21, GRUR-RS 2023, 8972 Rn. 58).

Die Annahme eines solchen konkreten Schadens setzt in unionsautonomer Auslegung nach ständiger Rechtsprechung des EuGH voraus, dass dieser „tatsächlich und sicher“ besteht (vgl. etwa zur Haftung der Union im Sinne von Art. 340 Abs. 2 AEUV jeweils m. w. N. hier nur EuGH Urt. v. 13.12.2018 – C-150/17 P, BeckRS 2018, 31923 Rn. 86; EuGH Urt. v. 30.5.2017 – C-45/15 P, BeckRS 2017, 111224 Rn. 61; EuGH Urt. v. 4.4.2017 – C-337/15 P, BeckRS 2017, 105868 Rn. 91-94; zur Haftung von Privatpersonen im Sinne von Art. 94 VO/2100/94 EuGH Urt. v. 16.3.2023 – C-522/21, GRUR 2023, 713 Rn. 38, 46, 49, wobei unter Rn. 37 dargestellt wird, dass ein pauschal festzusetzender Strafschadensersatz wie bei Art. 82 DSGVO ausscheidet; zur Haftung von Mitgliedstaaten nach nationalem Recht wegen Verstoßes gegen Unionsrecht EuGH Urt. v. 25.3.2021 – C-501/18, BeckRS 2021, 5310 Rn. 112, 122, 127).

Entsprechend sieht der die Frage des Schadensersatzes allein betreffende Erwägungsgrund 75 DSGVO auch nur vor, dass ein Schaden entstehen „könnte“, nicht aber in jedem Fall eintritt, „wenn“ u. a. „die betroffene Person um ihre Rechte und Freiheiten gebracht oder daran gehindert wird, die sie betreffenden personenbezogenen Daten zu kontrollieren“. In Erwägungsgrund 85 DSGVO hingegen geht es im Kern um die Informationspflichten und nicht um den Schadensersatzanspruch.

Etwas anderes gebietet auch Erwägungsgrund 146 Satz 6 DSGVO nicht, der „nur“ einen vollständigen und wirksamen Schadensersatz für den – konkret-individuell -„erlittenen“ Schaden fordert, während Art. 83 Abs. 1 und Art. 84 Abs. 1 Satz 2 DSGVO aus generell-abstrakter Perspektive nicht nur eine wirksame und verhältnismäßige, sondern auch abschreckende Maßnahmen einfordern.

Ein Kontrollverlust durch Scraping, also bei unbefugter Offenlegung / unbefugtem Zugänglichmachen, betraf als generelles Risiko der (unrechtmäßigen) Verarbeitung alle Personen, deren Daten ohne Rechtfertigungsgrund suchbar waren, gleichermaßen (vgl. allgemein Erwägungsgrund 7 Satz 2 DSGVO).

Einem solchen generellen Risiko soll im Hinblick auf die Zielsetzung der DSGVO, den unionsweiten Schutz personenbezogener Daten sicherzustellen (vgl. Erwägungsgrund 10 DSGVO), durch die Minimierung der Verarbeitungsrisiken entgegengewirkt werden, um ein möglichst hohes Schutzniveau zu erreichen. Dem Einzelnen die Kontrolle über seine Daten möglichst umfassend zu belassen bzw. dies zu gewährleisten, ist

hierfür von grundlegender Bedeutung. Realisiert sich das generelle Risi ko, dessen Eintritt verhindert werden soll, kommt es zwangsläufig zum Kontrollver lust. Daraus allein resultiert aber deshalb noch kein tatsächlicher Schaden im konkreten Einzelfall, wenn bzw. – hier eben – weil dieser automatisch bei jedem vom festgestellten Verstoß gegen die DSGVO Betroffenen in Form der Offenlegung / Zugänglichmachung von Daten eintritt (vgl. EuGH Urt. v. 4.4.2017 – C-337/15 P, BeckRS 2017, 105868 Rn. 91-94, zur mangelnden Schadensqualität eines Vertrauensverlustes, der generell mit der Sorgfaltspflichtverletzung eines Amtsträgers einhergeht). Der Kontrollverlust in Form des unkontrollierten Abrufs der Daten durch die Scraper und der anschließenden Veröffentlichung des Leak-Datensatzes im Darknet waren lediglich die zwangsläufige und generelle Folge der unrechtmäßigenbzw. unzureichend geschützten Datenverarbeitung durch die Beklagte. Daraus folgt, dass es über den Kontrollverlust als Realisierung des generellen Risikos hinaus eines tatsächlichen materiellen oder immateriellen Schadens im konkreten Einzelfall bedarf. Damit deckt sich, dass der völlige Kontrollverlust als solcher nicht per se ein immaterieller Schaden ist; denn stellt ein unkontrollierter Datenverlust im konkreten Einzelfall wegen des Werts der Daten eine in Geld messbare Einbuße dar, so ist dies unzweifelhaft ein Vermögensschaden.“

32
Dem schließt sich das Gericht vollumfänglich an.

33
Das Vorhandensein eines tatsächlichen Schadens wurde durch die Klagepartei indes weder ausreichend dargetan, noch bewiesen. In den Schriftsätzen der Klagepartei wird lediglich berichtet, die Klägerin mache sich „Sorgen über den Verbleib“ der Daten. Die Klagepartei habe „berechtigte Sorge, dass es zu einem Missbrauch“ komme. Der Datenklau stelle ein „hohes Risiko und eine erhebliche Unsicherheit“ dar. Ferner habe der Kläger Spam- und Phishinganrufe sowie SMS erhalten. Dieser Vortrag kann einen immateriellen Schaden nicht begründen. Bei einem immateriellen Schaden handelt es sich um einen inneren Vorgang, auf welchen durch die Aussage des Betroffenen und durch objektive Beweisanzeichen geschlossen werden muss. Es sind vorliegend indes nicht genug Beweisanzeichen objektiver Art vorgetragen sind, in denen sich die vorgetragenen Gefühle bzw. der Aufwand widerspiegeln, und zwar bezogen auf den konkreten Einzelfall (vgl. OLG Hamm, a.a.O.).

34
Das Gericht hat diesbezüglich den Kläger im Termin vom 08.02.2024 persönlich angehört. Der Kläger berichtete, dass er sehr selten Spam-Anrufe bzw Spammails bekommen habe.

35
Das Gericht geht aufgrund der Aussage der Klagepartei nicht von einem eingetretenen immateriellen Schaden aus. Der Kläger berichtete von den Anrufen ganz sachlich. Den neuen Ausweis habe er nicht aus Furcht vor Identitätsklau ausstellen lassen, sondern weil er abgelaufen war. Sein Handy habe er so eingestellt, dass Anrufe mit unterdrückter Rufnummer nicht durchgestellt würden. Eine darüber hinausgehende subjektive Beeinträchtigung war der Aussage nicht zu entnehmen. Anhaltspunkte für das starke Gefühl eines Kontrollverlustes oder anderweitige psychische Beeinträchtigungen ergaben sich aus der Aussage nicht im Ansatz.

36
Unstreitig kam es bis dato zu keinem Identitätsklau. Auch die sensiblen Bankdaten wurden bis dato nicht unzulässig verwendet.

37
Die Klagepartei ist daher darlegungs- und beweisfällig für das Vorhandensein eines Schadens geblieben.

38
Selbst wenn ein Schaden vorliegen würde und das Vorhandensein unerwünschter Kontaktversuche nachgewiesen wäre, würde es auch an einer Kausalität zwischen dem Datenschutzvorfall und dem Schaden fehlen. Ob etwaige Kontaktversuche auf Daten beruhen, die aus dem vorstehenden Vorfall bei der Beklagten erlangt wurden oder auf Daten beruhen, die aus anderen Wegen beschafft wurden, ist nicht nachweisbar.

39
Der Kläger erklärte in seiner Anhörung vom 08.02.2024, dass er auch auf anderen Plattformen wie Twitter, Kleinanzeigen, Amazon, Ebay Kleinanzeigen und Ebay angemeldet sei bzw war und dort seine Daten

eingegeben habe. Außerdem benutze er Bank-Apps, Shopping-Apps und Socialmedia-Apps. Der Kläger erklärte, dass er schon in früheren Jahren – also auch vor dem fraglichen Vorfall – derartige Spamanrufe und Spamemails erhalten habe.

40
Vor diesem Hintergrund – gerade weil der Kläger mit seinen persönlichen Daten im Internet recht freigiebig umgeht – kann nicht nachgewiesen werden, ob die von der Klageseite vorgetragenen Kontaktaufnahmen auf den streitgegenständlichen Vorfall zurückzuführen sind.

41
Der Klageantrag Ziffer 2) ist begründet.

42
Der Kläger hat gegen die Beklagte einen Anspruch auf Feststellung der Ersatzpflicht künftiger materieller Schäden aufgrund des Datenschutzvorfalls im Oktober 2020 gem. Art. 82 Abs. 1 DSGVO.

43
Der Antrag auf Feststellung einer Ersatzpflicht für etwaige künftige materielle Schäden auf Grund des Zugriffs auf die Daten im Oktober 2020 erweist sich gem. Art. 82 Abs. 1 DSGVO als begründet.

44
1. Die Beklagte hat als Verantwortliche schuldhaft gegen Art. 32 Abs. 1 DSGVO verstoßen.

45
1.1. Art. 82 DSVGO ist auf die Beklagte anwendbar.

46
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.

47
Die Beklagte ist Verantwortliche im Sinne von Art. 82 Abs. 1, 4 Nr. 7 DSGVO, weil sie als Finanzdienstleistungsunternehmen (teilweise bereits aufgrund entsprechender gesetzlicher Verpflichtungen) Kundendaten im Rahmen des Anmeldeprozesses abfragt und in einem Datenarchiv abspeichert. Auch sind die von den streitgegenständlichen Datenvorfällen erfassten Daten personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO.

48
1.2. Die Beklagte hat gegen Art. 32 DSGVO verstoßen.

49
Der Verstoß gegen die Verordnung ist entsprechend Erwägungsgrund 146 weit zu verstehen (Frenzel in Paal/Paul, DS-VGO BDSG, Art. 82, Rn. 8).

50
Die Beweislast hierfür liegt bei der Klägerseite; Art. 83 Abs. 3 bezieht sich nach dem eindeutigen Wortlaut nur auf die Verantwortlichkeit, nicht auf die Frage der haftungsbegründenden Handlung. Auch Art. 5 Abs. 2, 24 Abs. 1 DSVGO beinhaltet keine generelle Beweislastumkehr (Quaas in: BeckOK Datenschutzrecht, § 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).

51

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, 43. Ed.,01.11.2021, Art. 5 Rn. 36). Ein besonderer Schutz gilt für personenbezogene Daten nach Art. 9 Abs. 1 DSGVO, für die sich, soweit sie überhaupt verarbeitungsfähig sind, ein gesteigertes Schutzniveau ergibt. Zu berücksichtigen ist dabei insbesondere Erwägungsgrund Nr. 39:

„Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können."

52
1.2.1. Indem die Beklagte die Zugangsdaten nach Beendigung der Vertragsbeziehung mit nicht änderte, schützte sie die Daten nicht angemessen vor einer unbefugten oder unrechtmäßigen Verarbeitung.

53
Die Beklagte speicherte die personenbezogenen Daten des Klägers nach dessen Registrierung in einem Datenarchiv. Die Zugangsdaten zu diesem Datenarchiv hatte sie während der Dauer der bestehenden Zusammenarbeit bei gespeichert. Die Vertragsbeziehung mit endete bereits im Jahr 2015 (d.h. fünf Jahre bevor sich der Kläger bei der Beklagten registrierte und dort ein Kundenkonto erstellte). Nach Vertragsende mit änderte die Beklagte den Zugangsschlüssel nicht ab und unternahm auch keine anderen Schritte um sicherzustellen, dass der Zugangsschlüssel nicht mehr verwendet werden kann. Sie vertraute vielmehr darauf, dass die Daten durch vollständig und dauerhaft gelöscht würden. Dadurch hat sie jedenfalls das Risiko aufrechterhalten, dass durch einen Hacker-Angriff auf (im Rahmen einer supply chain attack) auch Daten ihrer Kunden abgegriffen werden können, ein Risiko, dass durch eine Abänderung der Zugangsdaten hätte minimiert oder gar ausgeschlossen werden können. Das Risiko eines mehrstufigen Hacker-Angriffs liegt – inbesondere bei einem Wertpapierinstitut, das hoch sensible Daten verwaltet und seine Leistungen vor allem auf digitalem Wege ermöglicht, auch nicht so außerhalb jeglicher Lebensrealität, dass es für die Beklagte nicht als ernsthaftes Risiko in Erwägung gezogen werden hätte müssen.

54
In den unterbliebenen Maßnahmen der Beklagten als Reaktion auf die Beendigung der Vertragsbeziehung mit liegt ein Verstoß gegen die Art. 32, 5 DSGVO. Als Verantwortliche im Sinne von Art. 32 Abs. 1, 4 Nr. 7 DSGVO durfte sich die Beklagte nicht lediglich darauf verlassen, dass die Zugangsinformationen löschen würde, unabhängig davon, ob diese dazu vertraglich verpflichtet war oder nicht. Insbesondere konnte sie sich auch nicht ohne weiteres darauf verlassen, dass sämtliche Sicherungskopien, Back-Ups und sonstigen weiteren Speichermaßnahmen im Hinblick auf den Zugangsschlüssel vollständig und dauerhaft gelöscht sein würden. Als Anbieterin von digital und online angebotenen Leistungen musste die Beklagte 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 von befinden könnte.

55
Allein das Vertrauen der Beklagten in ausreichende Schutzmaßnahmen auf Seiten von 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 diesbezüglich nichts getan, um nach Vertragsende mit einem Datenmissbrauch vorzubeugen.

56
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 ihr – nach Bekanntwerden der Datenvorfälle – eine solche Maßnahme möglich.

57
Dass die häufige Rotation derartiger Zugangsdaten mit Aufwand und Nachteilen wegen der zeitweisen Nichtverfügbarkeit verbunden gewesen wäre, kann dahinstehen. Jedenfalls nach Ende der Vertragsbeziehung mit einem Dienstleister wäre es – trotz einer etwaigen zeitweisen Einschränkung der Nutzbarkeit – geboten gewesen, die Zugangsdaten zu ändern.

58
Hinzu kommt, dass die Beklagte durch ihr Verhalten die Datenmissbrauchsmöglichkeit erweiterte bzw. erst schaffte, da sie die personenbezogenen Daten von Kunden, die die Beklagte erst nach Beendigung der vertraglichen Beziehungen zu gewinnen konnte, durch Speicherung in dem Datenarchiv dem Risiko eines Zugriffs über den alten Zugangsschlüssel aussetzte.

59
1.2.2. Selbst unterstellt, es hätte unmittelbar nach Vertragsende mit keine Veranlassung für die Beklagte bestanden, die Zugangsschlüssel zu dem Dokumentenarchiv zu ändern, hätte sie jedenfalls nach der Information durcham 30.09.2020 über den Hackerangriff zumindest überprüfen müssen, ob mit den anüberlassenen Daten weiterhin ein Zugriff auf das Archiv und die enthaltenen sensiblen personenbezogene Daten der Kunden der Beklagten möglich war – und die Daten zu diesem Zeitpunkt ändern müssen. Insbesondere vor dem Hintergrund der Qualität und erhöhten Sensibilität der gespeicherten Daten, die Steuer-IDs und Bankverbindung beinhalten und diese jeweils mit Ausweiskopien samt biometrischen Passbildern und Unterschrift verknüpfen, hätten in Anbetracht eines konkreten Risikos gesonderte Schutzmaßnahmen getroffen werden müssen. Es handelt sich – auch ohne Informationen über Kontostände oder spezifische Vermögensdaten – um umfassende personenbezogene Datensätze, für die in besonderem Maße das Risiko eines Identitätsmissbrauch durch unberechtigte Dritte besteht.

60
Eine Änderung der Zugangsdaten zum Zeitpunkt der Information durch hätte den Zugriff auf die Daten des Klägers verhindern können und ist unstreitig nicht erfolgt.

61
Daher 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.

62
1.2.3. 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 – und insbesondere anlässlich der Mitteilung dieses früheren Vertragspartners über einen bereits erfolgten Hackerangriff – 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.1.3. Die Verstöße gegen Art. 32 Abs. 1 DSGVO – das Absehen von einer Änderung der Zugangsdaten nach Vertragsbeendigung mit der sowie insbesondere nach Mitteilung des Hackerangriffs durch – ließ die im Verkehr erforderliche Sorgfalt außer Acht und war damit fahrlässig, so dass auch das erforderliche

Verschulden auf Seiten der Beklagten zu bejahen ist. Jedenfalls als die Beklagte Kenntnis davon erlangte, dass ein erfolgreicher Hackerangriff auf ihre frühere Vertragspartnerin erfolgt war, hätte sie bei pflichtgemäßer Sorgfalt sicherstellen müssen, dass der seit fünf Jahren unveränderte Zugangsschlüssel keiner weiteren Verwendung mehr zugeführt werden konnte, da sie zuvor zu keinem Zeitpunkt überprüft hatte, ob die Zugangsdaten bei weiterhin vorlagen. (so auch LG Köln, Urt. v. 18.5.2022, Az. 28 328/21, LG München Urt. v. 23.06.2022, Az. 5 O 3768/22).

63
Der für die Exkulpation gem. § 82 Abs. 3 DSGVO nötige Nachweis, dass die Beklagte „in keinerlei Hinsicht“ für den schadensbegründenden Umstand verantwortlich ist, gelingt damit nicht.

64
2. 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 DS- GVO sind, so steht ihr gegen die Beklagte ein Schadensersatzanspruch gemäß Art. 82 Abs. 1 DSGVO zu.

65
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 in Anbetracht der Qualität der erlangten Daten nicht auszuschließen, dass die erlangten Daten des Klägers in Zukunft für einen Identitätsdiebstahl oder sonstige Zwecke missbraucht werden und so zu einem Schaden bei der Klägerin führen. Der eingetretene Datenverlust betrifft einen verknüpften Datensatz mit sensiblen personenbezogenen Daten des Klägers. Aufgrund der Kombination der Daten besteht auch in Zukunft das Risiko eines Missbrauchs durch Dritte – insbesondere, weil der Kläger einen Teil der Daten nicht bzw. kaum verändern kann (wie sein biometrisches Passbild, die Körpergröße oder seine Unterschrift).

66
Der Kläger hat keinen Anspruch auf Ersatz eines ihm möglicherweise künftig entstehenden materiellen Schadens im Zusammenhang mit Zugriffen auf das Dokumentenarchiv der Beklagten im April 2020, weil er zu diesem Zeitpunkt unstreitig noch nicht Kunde der Beklagten war und entsprechend seine Daten zu diesem Zeitpunkt nicht von dem damaligen Vorfall betroffen gewesen sein können. Insoweit war die Klage abzuweisen.

67
Der Kläger hat gegenüber der Beklagten keinen Auskunftsanspruch (Ziff. 4 des Klageantrags) mehr, da dieser bereits erfüllt worden ist:

68
Erfüllt im Sinne des § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist. Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll. Daran fehlt es beispielsweise dann, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet. Dann kann der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen (OLG Hamm, Urteil vom 15. August 2023 – I-7 U 19/23).

69
Unter Berücksichtigung des Vorstehenden ist daher Erfüllung eingetreten.

70
Die Beklagte hat mit Schreiben vom 03.01.2023 (Anlage B13) bereits vorgerichtlich Auskunft erteilt, insbesondere durch einen im Kundenpostfach hinterlegten Link, der es dem Kläger ermöglichte, verschlüsselte Daten herunter zu laden, die eine Kopie der personenbezogenen Daten enthielt. Ferner wurde Auskunft erteilt mit Schreiben vom 05.01.2023 (Anlage B2).

71
Hiermit ist die Beklagte dem Auskunftsverlangen nachgekommen. Auf die Vorlage der weiteren Schreiben vom 08.05.2023 und 09.06.2023 kam es bereits nicht mehr an. Die Klagepartei hat nicht substantiiert vorgetragen, warum die von der Beklagten erteilten Auskünfte ungenügend seien. Die Klageseite beschränkt sich hier auf die Wiedergabe des Urteils des EuGH vom 12.01.2023 (C-154/21), ohne einen Bezug zu hiesigem Fall herzustellen.

72
IV. Der Klageantrag Ziffer 5) war ebenfalls abzuweisen.

73
Die Beklagtenseite hat – abgesehen vom einheitlichen Schreiben vom 19.10.2020 – auf das Auskunftsverlangen im Schreiben vom 21.12.2022 (Anlage K1) binnen Monatsfrist gem. Art. 12 Abs. 3 S. 1 DSGVO mit Schreiben vom 03.01.2023 und 05.01.2023 Auskunft erteilt. Inwiefern diese Auskünfte nicht ausreichend gewesen wären, trägt die Klagepartei nicht substantiiert vor. Die Klagepartei beschränkt sich erneut auf die auszugsweise Wiedergabe der Entscheidungsgründe dreier Urteile, ohne auf die konkrete Fallgestaltung, insbesondere die Frage, welche Auskünfte fehlen bzw unvollständig seien, und auf die Frage der Verfristung einzugehen.

74
V. 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.

C.

Nebenentscheidungen

75
Die Kostenentscheidung beruht auf § 92 Abs. 1 Alt. 2 ZPO.

76
Der Ausspruch zur vorläufigen Vollstreckbarkeit beruht auf § 709 S. 1, 2 ZPO.

77
Es war ein Streitwert von € 7.000 festzusetzen. Das Gericht geht hinsichtlich Ziffer 1) des Klageantrags von einem Streitwert von € 3.000,00 aus. Hinsichtlich der Ziffern 2) – 5) des Klageantrags geht das Gericht von einem Streitwert von jeweils € 1.000,00 aus.