LG München I, Endurteil v. 19.04.2024 – 31 O 2122/23

Titel:

Erfolglose Klage auf Unterlassung und Schadensersatz nach Datenleck bei Finanzdienstleister

Normenketten:

ZPO § 253, § 256
DSGVO Art. 4, Art. 6, Art. 15, Art. 82
BGB § 133, § 157

Leitsatz:

Allgemeine formelhafte Wendungen dahin, der von einem Datenleck bei einem Finanzdienstleister betroffene Kunde leide seither unter einem erhöhten Spamaufkommen, er lebe seither in Sorge vor einem Missbrauch seiner Daten und habe einen „anhaltenden Kontrollverlust über persönliche und sensible Daten“ erlitten, vermögen für sich genommen keinen konkreten Schaden zu begründen. (Rn. 49) (redaktioneller Leitsatz)

Schlagwort:

Datenschutzverstoß

Fundstellen:

LSK 2024, 8094
ZD 2024, 409
GRUR-RS 2024, 8094

Tenor

1. Die Klage wird abgewiesen-

2. Der Kläger hat die Kosten des Rechtsstreits zu tragen.

3. Das Urteil ist für die Beklagte gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrags vorläufig vollstreckbar.

Beschluss

Der Streitwert wird auf 17.000,00 € festgesetzt.

Tatbestand

1
Der Kläger macht Ansprüche auf Schadensersatz, Unterlassung und Auskunft aus behaupteten Verstößen gegen die Datenschutzgrundverordnung (DSGVO) nach einem Datenleck bei der Beklagten geltend.

2
Die Beklagte erbringt über ihre Website … Wertpapierdienstleistungen, insbesondere in Form der individuellen Vermögensverwaltung für Privatkunden, sowie finanzdienstleistungsnahe Softwaredienstleistungen. Zusätzlich bietet sie Brokerage-Dienstleistungen an und vermittelt Tages-, Fest- und Flexgeldangebote.

3
Der Kläger ist Kunde der Beklagten und unterhält ein Kundenkonto bei dieser. In diesem Zusammenhang stellte der Kläger der Beklagten insbesondere 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

Bankverbindung

4
Im Rahmen der Registrierung als Neukunde führte der Kläger auch ein sogenanntes Post-Ident-Verfahren durch, welches auch die folgenden personenbezogenen Daten des Personalausweises oder Reisepasses des Klägers zum Gegenstand hatte:

Ausweisnummer

Datum der Ausstellung

ausstellende Behörde und Ausstellungsland

Ausweiskopie

Portraitfoto

5
Die Beklagte hatte bei ihrem früheren Dienstleister Zugangsinformationen zu ihrem vollständigen IT-System hinterlegt (ihm also Adminrechte zugewiesen). Nach der Beendigung der Vertragsbeziehung zwischen der Beklagten und dem Dienstleister Ende 2015, erfolgte weder eine Änderung des Admin-Passwortes und der Zugangsdaten, noch eine Überprüfung der Löschung der Zugangsdaten seitens des Dienstleisters durch die Beklagte.

6
Bei dem Dienstleister der Beklagten kam es im Nachgang zu einem „Hackerangriff“. Die Angreifer verschaffte sich in diesem Zusammenhang mithilfe der Zugangsdaten des Dienstleisters zur Beklagten Zugriff auf das Dokumentenarchiv der Beklagten und die darin befindlichen Kundendaten, welche auch die personenbezogenen Daten der Klagepartei enthielten. Der Zugriff auf die Kundendaten der Beklagten erfolgte hierbei zu drei unterschiedlichen Zeitpunkten im Jahr 2020, nämlich am 15./16.04.2020, am 05./06.08.2020 sowie am 10./11.10.2020. Bei jedem dieser Zugriffe wurde ein Teil der insgesamt 389.000 Datensätze der 33.200 betroffenen Personen kopiert und entwendet. Die gestohlenen Daten wurden anschließend im Darknet angeboten.

7
Von dem Datenleck waren auch die persönlichen Daten des Klägers betroffen.

8
Nachdem der Kläger im Oktober 2020 von der Beklagten über den streitgegenständlichen Datenvorfall informiert wurde, hatte er zunächst keinen weiteren Nachfragebedarf. Er vertraute darauf, dass die in der Information enthaltenen Daten korrekt waren, und sah keinen Anlass, von der Beklagten weiteres zu fordern. Sein Kundenverhältnis bei der Beklagten setzte er ohne weitere Bedingungen fort. Erst nach Mandatsübernahme der Klägervertreter im Dezember 2022 schlug die Kanzlei vor, noch weitere Auskunft zu verlangen.

9

Mit Schreiben vom 21.12.2022 (Anlage K 1) verlangten die Klägervertreter demgemäß im Namen des Klägers von der Beklagten Auskunft über die personenbezogenen Daten des Klägers, hierbei u.a. über:

„4. Haben Sie diese Daten an Dritte übermittelt oder planen Sie, diese an Dritte zu übermitteln? Wenn ja, an wen, wann und zu welchem Zweck (welchen Zwecken)?

Teilen Sie insbesondere auch den Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten unsere Mandantschaft – befugt oder unbefugt – offengelegt worden sind.

…

7. Welche personenbezogenen Daten unserer Mandantschaft wurden durch Unbefugte erlangt?“

10
Mit Schreiben vom 05.01.2023 (Anlage K 2) erteilte die Beklagte dem Kläger Auskunft über seine bei der Beklagten gespeicherten und verarbeiteten Daten (Fragen 1-6) sowie seine personenbezogenen Daten, die von dem Datensicherheitsvorfall betroffen waren (Frage 7). Zudem verwies die Beklagte darauf, dass die Dateien zu der geforderten Auskunft gemäß Art. 15 DSGVO bereits im Rahmen des entsprechenden Standardprozesses der Beklagten am 3. Januar 2023 über seinen passwortgeschützten Kundenbereich an den Kläger übermittelt wurden (Anlage B13). Ferner bot die Beklagte in diesem Schreiben dem Kläger, wie allen ihren betroffenen Kunden, an, die Kosten für die Neuausstellung seines Ausweises zu übernehmen, wenn konkrete Anhaltspunkte für dessen missbräuchliche Verwendung vorlägen, z.B. wenn sich abzeichne, dass die Ausweisdaten für Registrierungsvorgänge verwendet würden oder eine zuständige Behörde einen Austausch für geboten halte. Dieses Angebot hat der Kläger nicht wahrgenommen. Bereits vor dem Schreiben vom 05.01.2023 (Anlage K 2) hatte der Kläger allerdings das Angebot der Beklagten ebenfalls an alle betroffenen Kunden, sich auf Kosten der Beklagten für den Identitätsschutz „meineSCHUFA Plus“ zu registrieren, in Anspruch genommen.

11
Der Kläger trägt vor, zu dem streitgegenständlichen Datenleck sei es aufgrund mangelnder technischer und organisatorischer Sicherheitsvorkehrungen, nämlich unzureichender technischer und organisatorischer Maßnahmen im Sinne eines Verstoßes gegen die Grundsätze „Privacy by Design“ und „Privacy by Default“, gekommen. Die Beklagte hätte insbesondere eine Pseudonymisierung und/oder Verschlüsselung der personenbezogener Daten vornehmen und ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchführen müssen. Wenn die Beklagte diese Schutzmaßnahmen ordnungsgemäß durchgeführt hätte, wäre es nicht zu dem fraglichen Datenleck gekommen und Unbefugte hätten nicht Zugriff auf die Daten des Klägers erhalten. Seit dem Datenleck bei der Beklagten komme es bei ihm insbesondere zu einem erhöhten Aufkommen an Spam-E-Mails. Auch sei davon auszugehen, dass seine Daten bereits im sog. „Darknet“ zum Verkauf angeboten wurden. Nach wie vor müsse damit gerechnet werden, dass die Daten der Klagepartei von Kriminellen dazu verwendet werden könnten, um unbefugt Zugang zu Bankkonten, Online-Diensten etc. zu erhalten, wodurch der Kläger finanziell geschädigt werden würde.

12
Der Kläger ist der Meinung, ihm sei durch das Datenleck und die daraus folgende unbefugte Weitergabe seiner personenbezogenen Daten bereits ein immaterieller Schaden entstanden. Die unbefugte Weitergabe seiner Daten habe zu einem konkreten und emotional spürbaren Nachteil geführt. Seit der Kenntnis über das Datenleck mache sich der Kläger zu Recht Sorgen über den Verbleib aber auch einen möglichen Missbrauch seiner Daten. Er befürchte z.B. Identitätsdiebstahl, Passwortklau durch Phishing, unzulässige Werbeanrufe und Werbemails. Die abgegriffenen Daten stellten für die Klagepartei ein hohes Risiko dar. Die berechtigten Sorgen der Klagepartei führten zu einem verstärkten Misstrauen gegenüber E-Mails und Anrufen von Unbekannten, insbesondere Anrufen mit unterdrückter Rufnummer. Die von ihm vorgetragenen Datenschutzverstöße seien hierfür auch kausal. Die seitens der Beklagten erteilte Auskunft sei unzureichend gewesen.

13
Der Kläger meint, ihm stehe ein Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO zu. Zudem bestehe ein Unterlassungsanspruch nach §§ 1004 BGB analog, 823 Abs. 1 bzw. Abs. 2 BGB i.V.m. Art. 6 Abs. 1 DSGVO, Art. 13 DSGVO, 14 DSGVO und Art. 17 DSGVO. Durch die Rechtsverletzung werde die

Wiederholungsgefahr indiziert. Die Beklagte trage die Darlegungsund Beweislast hinsichtlich der Einhaltung der Vorschriften der DSGVO. Selbst wenn man von einem Erfordernis des Eintritts eines konkreten Schadens auf Seiten des Betroffenen ausgehen würde, wäre in Art. 82 DSGVO eine Beweislastumkehr enthalten. Für den Schadensersatzanspruch nach Art. 82 DSGVO sei ein Verschulden nicht erforderlich.

14
Die Klagepartei beantragte zuletzt,

1. Die Beklagte wird verurteilt, an die Klagepartei als Ausgleich für Datenschutzverstöße einen immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von € 3.000,00 aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über den 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 April bis Oktober 2020 noch entstehen werden.

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 vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu 6 Monaten, im Wiederholungsfall bis zu 2 Jahren, zu unterlassen, personenbezogenen Daten der Klägerseite, namentlich 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.

3. 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.

4. Die Beklagte wird verurteilt, an die Klägerin (sic) für die Nichterteilung einer den gesetzlichen Anforderungen entsprechenden außergerichtlichen Datenauskunft i.S.d. Art. 15 DSGVO einen weiteren immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von € 2.000,00 aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über den jeweiligen Basiszinssatz seit Rechtshängigkeit zu zahlen.

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

15
Die Beklagtenpartei beantragt,

die Klage abzuweisen.

16
Die Beklagte trägt vor, dass schon kein Datenschutzverstoß vorgelegen habe. Insbesondere seien nicht mangelhafte Sicherungsmaßnahmen der Beklagten ursächlich für den Datenzugriff durch einen unberechtigten Dritten. Ihr früherer externer Dienstleister ... sei verpflichtet gewesen, die nicht mehr benötigten Zugangsinformationen vollständig und dauerhaft zu löschen. Die Beklagte sei davon ausgegangen, dass der Dienstleister diese Verpflichtung erfüllt habe. Es fehle aber jedenfalls an einem ersatzfähigen Schaden des Klägers. Der Umstand, dass Daten des Klägers von einem unberechtigten Dritten erlangt worden seien, reiche für die Annahme eines Schadens nicht aus. Ein erhöhtes Aufkommen an Spam-E-Mails oder unerwünschten Anrufen sei nicht auf den Datensicherheitsvorfall bei der Beklagten zurückzuführen. Die zuständigen Datenschutzaufsichtsbehörden seien rechtzeitig, vollumfänglich und umgehend über den Datensicherheitsvorfall informiert worden. Mit dem Anwaltsschreiben vom 05.01.2023 (Anlage K 2) sei die Beklagte dem Auskunftsverlangen des Klägers vollumfänglich nachgekommen.

17

Die Beklagte meint, die Klage sei hinsichtlich der Klageanträge zu Ziffer 1., 2. Abs. 1 und 2. Abs. 2 bereits unzulässig. Im übrigen sei die Klage aber auch vollumfänglich unbegründet, denn es liege weder ein Verstoß gegen die DSGVO noch ein Verschulden der Beklagten vor. Jedenfalls habe der Kläger keinen kausalen Schaden erlitten, denn Art. 82 DSGVO verfolge lediglich den Zweck, tatsächlich entstandene Schäden zu kompensieren. Dieser Schaden müsse zudem hinreichend konkret sein. Der Kläger trage lediglich vor, Sorgen vor einem möglichen Missbrauch seiner Daten zu haben, ohne dass jedoch ein solcher Missbrauch eingetreten sei oder der Kläger Missbrauchsversuche substantiiert vorgetragen habe. Ein ersatzfähiger immaterieller Schaden könne nicht in jeder Befürchtung zu sehen sein, da prinzipiell jeder Verstoß gegen eine DSGVO-Norm zu solchen negativen Reaktionen wie Unmutsgefühlen führe, sodass ein derartiges Verständnis letztlich dem Verzicht auf die Voraussetzung eines Schadens gleichkommen würde. Unabhängig vom streitgegenständlichen Datenvorfall sei es immer sinnvoll, die eigenen Kontobewegungen stets gut im Auge zu behalten. Der Kläger habe schon gar nicht dargelegt, dass es ein echtes Angebot im Darknet gegeben habe, welches die im Zuge des Datenvorfalls abgegriffenen Kundendaten, insbesondere des Klägers, tatsächlich enthalten habe und dass die Daten tatsächlich veräußert wurden. Auch sei nicht hinreichend substantiiert, dass die Daten des Klägers für die behaupteten Missbrauchsversuche bei dem Telekommunikationsanbieter ... tatsächlich genutzt worden seien, jedenfalls aber, dass dies infolge des Datenvorfalls erfolgt sei. Jedenfalls wäre dieses aber auch nicht als Schaden zu qualifizieren. Nach Erwägungsgrund 146 S. 3 DSGVO sei der Begriff des Schadens unionsrechtlich auszulegen und umfasse Diskriminierungen, Identitätsdiebstahl oder -betrug, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, unbefugte Aufhebung der Pseudonymisierung oder andere gesellschaftliche Nachteile. Ein erhöhtes Spam-Aufkommen und Vorkommen von Onlinebzw. Telekommunikations-Betrugsversuchen sei nicht notwendigerweise dem streitgegenständlichen Datenvorfall zuzuordnen. Der Kläger sei somit jedenfalls hinsichtlich der Kausalität beweisfällig geblieben.

18
Ein Unterlassungsanspruch wegen eines vermeintlichen DSGVO-Verstoßes bestehe schon mangels Anspruchsgrundlage nicht. Er scheide hier aber auch deshalb aus, weil sich dieser nur auf beabsichtigte Offenlegungen von Information seitens der Beklagten an einen Dritten erstrecke und daher über die hier in Rede stehende Offenlegung im Zuge des Datenlecks hinausgehe und die Beklagte allgemein zu gesetzeskonformem Verhalten verpflichten wolle.

19
Der Auskunftsanspruch sei ordnungsgemäß erfüllt worden. Die Beklagte habe die Auskunft erteilt, wie sie vom Kläger verlangt worden sei. Das vom Kläger zitierte Urteil des EuGH vom 12. Januar 2023 statutiere nur eine Befugnis der betroffenen Person, Auskunft über die Identität der konkreten Empfänger der sie betreffenden Daten zu verlangen. Eine solche Auskunft habe der Kläger aber zunächst gar nicht verlangt. Vielmehr habe er verlangt „den Empfänger oder Kategorien von Empfängern“ mitzuteilen, denen die personenbezogenen Daten des Klägers offengelegt wurden. Der Kläger habe somit eine Beauskunftung bloßer „Kategorien von Empfängern“ (nach Wahl der Beklagten) ausreichen lassen. Dennoch habe die Beklagte im Schreiben vom 03.01.2023 (Anlage B 13) sowie im Anwaltsschreiben vom 05.01.2023 (Anlage K 2) unter Nennung der konkreten Empfänger informiert. Jedenfalls fehle dem Kläger für eine weitergehende Auskunft über seine Daten gem. Art. 15 DSGVO das Rechtsschutzbedürfnis, da er nach der umfassenden Beantwortung seiner Fragen mit dem Anwaltsschreiben vom 05.01.2023 (Anlage K 2) keine weitere Auskunft nach Art. 15 DSGVO von der Beklagten verlangt habe. Einem solchen weiteren Verlangen wäre die Beklagte ohne weiteres nachgekommen. Die gerichtliche Durchsetzung sei insoweit gänzlich unnötig.

20
Der Kläger habe auch keinen Schadensersatzanspruch wegen Nichterteilung von Auskunft, da die mit dem Anwaltsschreiben vom 05.01.2023 (Anlage K 2) erteilte Auskunft hinreichend und umfassend gewesen sei, insbesondere die Information über Kategorien von Empfängern dem Antrag des Klägers entsprochen habe, der gerade nicht die Mitteilung der Identität einzelner Empfänger verlangt habe. Zudem erfasse Art. 82 Abs. 1 DSGVO nur Schäden, die durch eine nicht der DSGVO entsprechende Verarbeitung entstünden. Dies folge aus Erwägungsgrund 146, der von Schäden spreche, die „auf Grund einer Verarbeitung“ einträten. Selbst eine verspätete oder unvollständige Auskunft stelle keine solche Verarbeitung der personenbezogener Daten dar, so dass bereits mangels Anspruchsgrundlage kein Schadensersatz wegen

Nichterteilung von Auskunft denkbar sei. Zudem fehle auch hier die Darlegung, worin der immaterielle Schaden bestehen solle.

21
Das Gericht hat in der mündlichen Verhandlung vom 15.03.2024 den Kläger informatorisch angehört.

22
Zur Ergänzung des Sachverhalts wird auf die gewechselten Schriftsätze der Parteien nebst Anlagen, das Protokoll der mündlichen Verhandlung vom 15.03.2024 sowie den übrigen Akteninhalt Bezug genommen.

Entscheidungsgründe

A.

23
Die Klage ist nur teilweise zulässig. Soweit sie zulässig ist, erweist sie sich als unbegründet.

I. Zulässigkeit

24
Bezüglich der Anträge Ziffer 1., 4. und 5. ist die Klage zulässig. Die Klageanträge zu 2. Abs. 1, 2. Abs. 2 und 3 sind unzulässig.

1. Klageantrag zu 1. (immaterieller Schadensersatz für Datenschutzverstoß)

25
Der Klageantrag zu 1. (immaterieller Schadensersatz für Datenschutzverstoß) ist hinreichend bestimmt, da sich der Umstand, für welche konkreten Datenschutzverstöße der Schadensersatz in welcher Höhe als Ausgleich dienen soll, nicht aus dem Antrag bzw. der Klage selbst ergeben muss. Vielmehr kann auch für die Bestimmung des Umfangs der Begründungsanteile des beantragten Schadensersatzes auf das Ermessen des Gerichts verwiesen werden, wie hier erfolgt.

2. Klageantrag zu 2. Abs. 1 (Feststellung materieller Schadensersatz für die Zukunft)

26
Der Klageantrag zu 2. Abs. 1 (Feststellung materieller Schadensersatz für die Zukunft) ist auch in der Form, wie in der mündlichen Verhandlung vom 15.03.2024 gestellt, bereits unzulässig, da es am notwendigen Feststellungsinteresse des Klägers nach § 256 Abs. 1 ZPO fehlt. Die Möglichkeit eines Schadenseintritts (vgl. BGH, Urteil vom 29.06.2021 – ZR 52/18) materieller oder immaterieller Art ist durch den Kläger weder hinreichend dargelegt noch ersichtlich. Gerade im Hinblick auf die vergangene Zeit ist auch nicht damit zu rechnen, dass zukünftige Schäden noch eintreten werden.“

27
Nachrichten mit betrügerischen Absichten oder belästigender Wirkung sind gerichtsbekanntermaßen, wie auch zum Gegenstand der mündlichen Verhandlung vom 15.03.2024 gemacht (Protokoll S. 3,5), jedermann/jederfrau ausgesetzt, auch Personen, die von dem streitgegenständlichen Datenvorfall in keiner Weise betroffen sind. Die berechtigten Sorgen des Klägers vor Phishing-Nachrichten und sein verstärktes Misstrauen gegenüber E-Mails und Anrufen von Unbekannten mit unterdrückter Rufnummer wirken dieser Gefahr zudem vielmehr entgegen.

3. Klageantrag zu 2. Abs. 2 (Unterlassung)

28
Der Klageantrag zu 2. Abs. 2 (Unterlassung) ist zu unbestimmt i.S.v. § 253 Abs. 2 Nr. 2 ZPO, da er nicht deutlich macht, welche Fälle des „Dritten zugänglich (…) machens“ er erfassen soll, welche „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ die Beklagte bei jeglicher Zugänglichmachung vornehmen müsste und/oder welche „Rechtfertigungsgründe nach der DSGVO“ das Unterlassungsgebot nicht eingreifen lassen sollen. Die Klärung all dieser Fragen darf nicht vom Erkenntnisverfahren ins Vollstreckungsverfahren (Bestrafungsverfahren) verlagert werden (BGH NJW 2000, 2195). Eine diese Mängel beseitigende Klarstellung des Antrags ist trotz Hinweises in der Sitzung nicht erfolgt.

29

Unterlassungsanträge müssen über den Wortlaut einer etwaigen Verbotsnorm hinaus an die konkrete Verletzungsform angepasst sein, um inhaltlich nicht über den materiell-rechtlichen Anspruch hinauszugehen (BGH, Urt. v. 29.06.1995, Az. ZR 137/93 – juris; BGH, Beschluss vom 10.04.2018, Az. ZR 247/17, – juris). Der Streitgegenstand muss so klar gefasst sein, dass sich die Beklagte im Erkenntnisverfahren erschöpfend verteidigen kann (st. Rspr. BGH, zB Urt. v. 17.07.2003, Az. ZR 259/00, Rn. 41, juris). Unterlassungsanträge, die sich auf die Umschreibung gesetzlicher Verbote beschränken, sind grundsätzlich zu unbestimmt und damit unzulässig (BGH, Urt. v. 24.11.1999, Az. ZR 189/97, – juris). Derartige Anträge sind nur dann ausreichend bestimmt, wenn der im Antrag wiedergegebene Verbotstatbestand konkret und eindeutig ist oder sich aus dem klägerischen Sachvortrag ergibt, auf welche konkrete Verhaltensweise sich der Unterlassungsanspruch beschränkt. Zudem muss der Sachverhalt im Wesentlichen unstreitig sein, die Unstimmigkeiten der Parteien dürfen sich nur auf die rechtliche Qualifizierung einer an sich unstreitigen Verhaltensweise beziehen (BGH, Urt. v. 30.04.2015, Az. ZR 196/13, GRUR 2015, 1235). Diesen Erfordernissen entspricht der Unterlassungsantrag nicht. Es ist anhand des Antrags nicht erkennbar, welches eigene Handeln genau der Beklagten abverlangt werden soll.

30
Hierbei ist bereits fraglich, ob die verwendete Formulierung „die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ hinreichend bestimmt ist. Der verwendete Begriff „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ ist auslegungsbedürftig, da die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen einem ständigen Wandel unterliegen. Zur Gewährleistung effektiven Rechtsschutzes kann zwar eine gewisse Auslegungsbedürftigkeit hinzunehmen sein. Dies ist allerdings nur dann der Fall, wenn über den Sinngehalt der verwendeten Begriffe keine Zweifel bestehen. Dies gilt aber nicht, wenn zwischen den Parteien Streit darüber besteht, ob das konkret beanstandete Verhalten darunter fällt, weil sonst der im Erkenntnisverfahren beizulegende Streit ins Vollstreckungsverfahren verlagert würde (s. BGH NJW 2000, 2195). So liegt der Fall hier, da zwischen den Parteien Streit darüber besteht, ob die von der Beklagten ergriffenen Maßnahmen die nach „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ darstellten.

31
Jedenfalls fehlt es aber auch an einer hinreichenden Bestimmtheit des Unterlassungsantrags, soweit der Kläger Unterlassung begehrt, seine Daten „Dritten zugänglich zu machen, … ohne, dass … ein Rechtfertigungsgrund nach der DSGVO [vorliegt]“. Denn dieser Antrag wäre im Falle des Zusprechens nicht vollstreckungsfähig. Der Antrag ist unter Berücksichtigung seiner Begründung und seines Ziels nach §§ 133, 157 BGB auszulegen (vgl. BGH, Beschl. V. 22.05.1995 – ZB 2/95, NJW-RR 1995, 1183). Offensichtlich wendet sich der Kläger gegen das von der Beklagten nicht beabsichtigte Abgreifen seiner Daten durch Dritte unter Umgehung der vorhandenen Sicherungsmaßnahmen der Beklagten, die als unzureichend kritisiert werden. Mit dieser Maßgabe ist aber weder klar und bestimmbar, wie das zu verbietende „zugänglich machen“ durch die Beklagte aussehen soll, noch welche Rechtfertigungsgründe ausgenommen sein sollen.

32
Im Falle eines von der Beklagten nicht beabsichtigten Abgreifens der klägerischen Daten durch Dritte liegt bereits keine Handlung der Beklagten vor. Vielmehr handelt es sich um eine Handlung des Dritten, über welche die Beklagte keine Kontrolle hat. Die Unterlassung eines solchen Dritthandelns, das außerhalb der Einflusssphäre der Beklagten liegt, kann der Beklagten nicht auferlegt werden, da ihr die Erfüllung unmöglich ist. Unterlassungsgebote können sich nur auf eigenes Handeln erstrecken, über welches der Unterlassungsschuldner die Kontrolle hat. Es verbleibt daher unklar, welches eigene Tun die Beklagte gem. dem Klageantrag zu 2. Abs. 2 genau unterlassen soll.

33
Mangels eindeutiger Bestimmung des zu unterlassenden Tuns der Beklagten bleibt folgerichtig ebenfalls unklar, welche Erlaubnistatbestände i.S.v. Art. 6 DSGVO für dieses Tun eingreifen könnten. Bei von der Beklagten nicht kontrollierbaren Handlungen Dritter handelt es sich nicht um Verarbeitungen, für die die Beklagte als Verantwortliche i.S.v. Art. 4 Nr. 7 DSGVO agieren könnte, so dass sie insoweit nicht für die Einhaltung der Erlaubnistatbestände nach der DSGVO sorgen kann.

34

Mit einem Unterlassungsantrag kann der Kläger die Beklagte auch nicht allgemein zu gesetzeskonformem Handeln oder zu einem positiven Tun, wie z.B. der Einführung der jeweils nach dem aktuellen „Stand der Technik möglichen Sicherheitsmaßnahmen“ verpflichten. Vielmehr sind etwaige künftige Verstöße der Beklagten gegen die DSGVO oder die nach dem jeweils aktuellen „Stand der Technik möglichen Sicherheitsmaßnahmen“ in einem neuen Erkenntnisverfahren zu klären.

35
Eine umfassende Sicherung seiner Daten vor einem künftigen erneuten Abgreifen durch Dritte bei der Beklagten kann der Kläger nur erreichen, indem er diese aus seinem Kundenkonto bei der Beklagten entfernt bzw. dieses vollständig löscht. Da dies ersichtlich jederzeit möglich ist, fehlt es insoweit auch an einem Rechtsschutzbedürfnis für eine Unterlassungsklage.

36
Da der Unterlassungsantrag bereits unzulässig ist, kommt es vorliegend auch nicht mehr darauf an, ob für diesen nach der DSGVO bzw. nach allgemeinem Zivilrecht überhaupt eine Anspruchsgrundlage gegeben ist.

4. Klageantrag zu 3. (Auskunft)

37
Der Klageantrag zu 3. (Auskunft) ist ebenfalls unzulässig, da es dem Kläger diesbezüglich an einem Rechtsschutzbedürfnis fehlt.

38
Es ist nicht ersichtlich, welche Auskunft der Kläger von der Beklagten nach dem Erhalt der Antworten mit dem Anwaltsschreiben vom 05.01.2023 (Anlage K 2) noch begehrt. Unstreitig hat er nach dem Erhalt dieser Antworten (Anlage K 2) keine weitere Auskunft nach Art. 15 DSGVO von der Beklagten mehr verlangt. Nach ihrem insoweit unwidersprochenen Vortrag wäre die Beklagte einem solchen weiteren Verlangen – z.B. nach den konkreten Empfängern (nicht nur „Kategorien von Empfängern“) der personenbezogenen Daten des Klägers – ohne weiteres nachgekommen. Für eine gerichtliche Durchsetzung einer Auskunft ohne vorherige außergerichtliche Anforderung der vermeintlich noch fehlenden Informationen fehlt dem Kläger ein Rechtsschutzbedürfnis.

39
Ohne dass es darauf noch ankäme, dürfte der Auskunftsanspruch im vorliegenden Fall aber auch bereits ordnungsgemäß erfüllt worden sein. Insbesondere wurde die Auskunft bereits mit Schreiben vom 05.01.2023 (Anlage K 2) so erteilt, wie sie vom Kläger bis dahin verlangt wurde. Mit Schreiben vom 21.12.2022 (Anlage K 1) verlangten die Klägervertreter von der Beklagten Auskunft über u.a. „4. … den Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten unsere Mandantschaft – befugt oder unbefugt – offengelegt worden sind“.

40
Soweit der Kläger hiermit die „Empfänger“ der Daten aus dem Datenvorfall zu erfassen meint, ist der Beklagten die Auskunfterteilung über die genauen „Empfänger“ unmöglich, da die entsprechenden Täter der Beklagten unstreitig unbekannt sind. Die Beklagte kann nur über solche Umstände Auskunft geben, bezüglich derer sie Informationen hat, also insbesondere ihr eigenes Verhalten in Form von willentlicher Verarbeitung oder Übermittlung von Daten. Dies entspricht dem allgemeinen Grundsatz „nemo ultra posse obligatur“, dass Unmögliches nicht verlangt werden kann (vgl. Gola/Heckmann/Franck, 3. Auflage 2022, DSGVO, Art. 15, Rn. 51ff.; Lembke, Der datenschutzrechtliche Auskunftsanspruch im Anstellungsverhältnis, NJW 2020,1841,1845). Als „Kategorien von Empfängern“ war eine Auskunft überflüssig, da dem Kläger bereits bekannt war, dass die Täter des entsprechenden Datenvorfalls seine Daten erhalten hatten.

41
Soweit sich die Anfrage auf „befugte Offenlegungen“ der klägerischen Daten beziehen soll, wurde diese Auskunft mit Schreiben vom 03.01.2023 (Anlage B13) bereits mit konkreten Empfängern erteilt und in dem Anwaltsschreiben vom 05.01.2023 (Anlage K 2) erneut hierauf verwiesen. Darüber hinaus hat die Beklagte dem Kläger nach Klagezustellung am 28.04.2023 erneut vorsorglich die konkreten Empfänger seiner Daten mitgeteilt. Der Kläger hat hierzu keine Erklärung mehr abgegeben, insbesondere den Rechtsstreit nicht insoweit für erledigt erklärt oder sonstwie erläutert, welche Auskünfte er konkret noch nicht erhalten haben will.

42
Vielmehr hat er lediglich pauschal und vage behauptet, sein Auskunftsanspruch sei „nicht, jedenfalls nicht hinreichend erfüllt“ worden. Soweit hierdurch die Vollständigkeit und Richtigkeit der gegebenen Auskunft angezweifelt werden sollte, ergibt sich hieraus kein Anspruch auf weitere Auskunft. Etwaige Anhaltspunkte für eine etwaige Unrichtigkeit oder Unvollständigkeit der Auskunft hat der Kläger im dafür vorgesehenen Verfahren (Antrag auf Abgabe einer eidesstattlichen Versicherung) anzubringen. Hieraus folgt kein – weitergehender – Auskunftsanspruch.

5. Klageanträge zu 4. (immaterieller Schadensersatz für Nichterteilung Datenauskunft) und 5.

(außergerichtliche Anwaltskosten)

43
Hinsichtlich der Klageanträge zu 4. und 5. bestehen keine Zweifel an der Zulässigkeit.

II. Begründetheit

44
Soweit die Klage zulässig ist, ist sie unbegründet.

1. Klageantrag zu 1. (immaterieller Schadensersatz für Datenschutzverstoß)

45
Der Kläger hat keinen Anspruch auf immateriellen Schadenersatz aus Art. 82 Abs. 1 DSGVO gem. dem Klageantrag Ziff. 1. Denn es fehlt jedenfalls am Eintritt eines immateriellen Schadens, der sich kausal auf den streitgegenständlichen Datenschutzvorfall zurückführen lässt.

46
a) Nach Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder den Auftragsverarbeiter.

47
Das Merkmal des immateriellen Schadens ist autonom auszulegen (Paal / Aliprandi NJW 2023, 1914 Rn. 5). Erwägungsgrund 146 S. 3 zur DSGVO bestimmt, dass der Begriff des Schadens im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden soll, die den Zielen dieser Verordnung in vollem Umfang entspricht. Erwägungsgrund 75 zur DSGVO nennt etwa Identitätsdiebstahl, finanzielle Verluste, Rufschädigung oder den Verlust der Kontrolle personenbezogener Daten. Ein deutsches Verständnis bzw. eine enge Auslegung des Schadensbegriffs ist mithin nicht angezeigt (vgl. dazu BVerfG, Beschluss vom 14.01.2021, 1 BvR 2853/19, NJW 2021, 1005, 1007). Eine Erheblichkeitsschwelle für das Vorliegen eines solchen Schadens ergibt sich aus der DSGVO nicht. Bagatellschäden sind daher nicht auszuschließen. Erforderlich ist aber jedenfalls, dass ein konkreter immaterieller Schaden auch tatsächlich eingetreten („entstanden“ bzw. „erlitten“, vgl. Erwägungsgrund 146 S. 6) ist. Ein bloßer Verstoß gegen die Bestimmungen der DSGVO reicht nicht aus, um einen Schadenersatzanspruch zu begründen (EuGH, Urteil vom 04.05.2023, Az. C-300/21, NZA 2023, 621 = NJW 2023, 1930, Rz. 34, 42). Denn ein Schadensersatzanspruch setzt das Vorliegen eines „Schadens“ ebenso wie das Vorliegen eines Verstoßes gegen die DSGVO und eines Kausalzusammenhangs zwischen Verstoß und Schaden voraus, „wobei diese drei Voraussetzungen kumulativ sind“ (vgl. EuGH a.a.O. Rn. 32).

48
Die Klagepartei ist für den konkreten Schaden darlegungs- und ggf. beweispflichtig (OLG Frankfurt a.M. 02.03.2022, 13 U 206/20, GRUR-RS 2022, 4491 Rn. 57, 65).

49
Unter Zugrundelegung dieses Maßstabs hat der Kläger nicht zur Überzeugung des Gerichts dargelegt, dass bei ihm aufgrund eines möglichen Datenschutzverstoßes der Beklagten tatsächlich ein immaterieller Schaden eingetreten ist. Die Ausführungen hierzu in der Klageschrift erschöpfen sich lediglich in allgemeinen formelhaften Wendungen, die mit identischem Inhalt in einer Vielzahl von Verfahren vorgebracht wurden und werden. Diesbezüglich wurde nur vorgetragen, der Kläger leide seither unter einem erhöhten Spamaufkommen, er lebe seither in Sorge vor einem Missbrauch seiner Daten und habe einen „anhaltenden Kontrollverlust über persönliche und sensible Daten“ erlitten.

50
Die informatorische Anhörung des Klägers hat ergeben, dass die vom Kläger zur Substantiierung seiner Missbrauchsbefürchtungen vorgetragenen „drei verdächtigen Anfragen bei ... erst vor ca. 1 Jahr auftraten, mithin nicht in engem zeitlichem Zusammenhang mit dem Datenvorfall. Von diesen verdächtigen Anfragen hat der Kläger erfahren, weil er das Angebot der Beklagten auf Nutzung der „MeineSchufa+“-Funktion auf ihre Kosten wahrgenommen hat. Nachdem er diese drei verdächtigen Anfragen bei ... der Schufa gemeldet hatte, hat der Kläger sich laut eigener Aussage nicht weiter darum gekümmert, zumal auch nichts weiter passierte, insbesondere keine finanziellen Nachteile feststellbar waren. Da der Kläger seine Bankkontotransaktionen genau beobachtet hatte und keine missbräuchlichen Vorgänge feststellen konnte, hielt er es auch nicht für nötig, sich direkt an ... zu wenden. Es kann daher nicht angenommen werden, dass diese „verdächtigen Anfragen“ den Kläger besonders „bekümmert“ oder emotional belastet haben. Der Kläger ist auch weiter Kunde bei der Beklagten, was sicherlich nicht der Fall wäre, wenn er aufgrund des früheren Verhaltens der Beklagten spürbar belastet wäre.

51
Allein der Umstand, dass der Kläger seit ca. 1 Jahr zunehmend betrügerische Kontaktversuche auf seiner bereits seit ca. 20 Jahren von ihm genutzten Handynummer erhält, ist kein Indiz für eine missbräuchliche Nutzung gerade der aus dem streitgegenständlichen Vorfall abgegriffenen Daten. Denn in diesem Zeitraum ist das Allgemeine Lebensrisiko für derartige Kontaktversuche enorm gestiegen und hatten entsprechende Absender aus der bereits ca. 20-jährigen Nutzungsdauer der Handynummer bereits genügend andere Möglichkeiten, um an diese zu gelangen.

52
Es wurde zum Gegenstand der mündlichen Verhandlung gemacht, dass sowohl der Beklagtenvertreter als auch die Einzelrichterin selbst, obwohl vom Datenvorfall bei der Beklagten nicht betroffen, ebenfalls vergleichbare Nachrichten erhalten.

53
Unerwünschte Kontaktaufnahmeversuche sind zwar durchaus lästig, aber im Hinblick auf die vermehrte Angabe von Kontaktdaten bei OnlineEinkäufen, Reservierungen etc. nicht zu vermeiden. Unerwünschte Kurznachrichten oder auch Anrufe mit betrügerischem Inhalt sind typische, mit der Nutzung digitaler Kommunikationsmittel verbundene Beeinträchtigungen und Risiken, die allgemein auftreten und auch Personen treffen, die nicht bei der Beklagten angemeldet oder von dem streitgegenständlichen Datenvorfall betroffen sind.

54
Anhaltspunkte für einen echten Kontrollverlust über Informationen, über die bisher Kontrolle bestanden hätte, oder für tatsächliche psychische Beeinträchtigungen, die auf den streitgegenständlichen Datenvorfall zurückzuführen sein könnten, wurden nicht vorgebracht. Insbesondere wurden keinerlei Anhaltspunkte dafür vorgebracht, dass die Ausweis- oder Kontodaten des Klägers tatsächlich bereits selbst in den Händen von Betrügern waren und von diesen genutzt wurden. Im Gegenteil dazu dienen die vom Kläger vorgetragenen Anrufe aus Afrika, SMSe und „verdächtigen Anfragen bei ... gerade erst der Erlangung solcher sensibler Daten.

55
Der Datenvorfall mag bei dem Kläger ein unangenehmes Gefühl hinsichtlich der eigenen Daten ausgelöst haben, bloße Unannehmlichkeiten begründen jedoch noch keine haftungsrelevante Beeinträchtigung.

56
Dass es in sonstiger Weise zu einem konkreten Missbrauch seiner Daten gekommen sei, hat der Kläger nicht behauptet.

57
Vor diesem Hintergrund kann es im vorliegenden Fall offenbleiben, ob der Beklagten tatsächlich ein Verstoß gegen die Bestimmungen der DSGVO zur Last fällt. Die Beklagte hat zwar die Zugangsdaten ihres früheren Dienstleisters nach Vertragsende nicht selbst aktiv gesperrt und hierdurch das Risiko für unauthorisierte Datenabgriffe unnötig erhöht (gelassen). Hieraus ist dem Kläger jedoch, wie ausgeführt, jedenfalls kein kausaler Schaden – materieller oder immaterieller Natur – entstanden oder wäre noch ernsthaft – kausal – zu befürchten.

58
b) Darüber hinaus fehlt es im vorliegenden Fall auch an der erforderlichen Kausalität zwischen dem streitgegenständlichen Datenvorfall und dem vom Kläger geschilderten „erhöhten Spamaufkommen“.

59
Die Kausalität zwischen Datenschutzverstoß und Schaden ist nach dem eindeutigen Wortlaut des Art. 82 Abs. 2 DSGVO erforderlich.

60
Grundsätzlich werden auch Personen, die kein Nutzerkonto bei der Beklagten haben und weder von dem streitgegenständlichen, noch von anderen gerichtsmassigen Datenvorfällen betroffen sind, regelmäßig Opfer von Spam-Anrufen, -SMS und -E-Mails, sowohl mit unerwünschter Werbung, als auch mit betrügerischen Absichten. Diese können nicht ohne weitere konkrete Anhaltspunkte mit dem hier streitgegenständlichen Datenvorfall in Verbindung gebracht werden. Insbesondere ist nicht ersichtlich, dass bei den Kontaktaufnahmeversuchen Informationen verwendet wurden, die der Anrufer oder Absender aus den Daten der Beklagten erlangt hat. Die Anrufe und Emails könnten somit vielmehr auch Ergebnis einer rein zufälligen Rufnummernanwahl und/oder Kontaktierung von im Internet leicht abgreifbaren Telefonnummern und E-Mail-Adressen gewesen sein.

61
Die geltend gemachten Rechtshängigkeitszinsen teilen als Nebenforderung das Schicksal der Hauptforderung und unterliegen insoweit ebenfalls der Klageabweisung.

2. Klageantrag zu 4. (immaterieller Schadensersatz für Nichterteilung Datenauskunft)

62
Aus den gleichen Erwägungen ist auch der Klageantrag zu 4. (immaterieller Schadensersatz für Nichterteilung Datenauskunft) offensichtlich unbegründet. Auch hier fehlt es jedenfalls am Eintritt eines – immateriellen – Schadens. Es ist nicht einmal ansatzweise vorgetragen, dass der Kläger aufgrund der behaupteten verspäteten Auskunft eine Beeinträchtigung in irgendeiner Form erfahren hat.

63
Der geltend gemachte Anspruch ist zudem auch noch aus weiteren Gründen abwegig:

64
Der Kläger wurde unstreitig im Oktober 2020 unmittelbar nach Kenntniserlangung durch die Beklagte von dem Datenvorfall unterrichtet. Hierauf hat er auch nicht etwa seinerseits unverzüglich Auskunft bei der Beklagten begehrt. Vielmehr erfolgte dies unstreitig erstmals mit anwaltlichem Schreiben vom 21.12.2022 (Anlage K 1). Für die begehrte Auskunft wurde eine Frist von einem Monat ab Zugang des Schreibens gesetzt. Mit Schreiben vom 03.01.2023 (Anlage B 13) und vom 05.01.2023 (Anlage K 2) erteilte die Beklagte sodann dem Kläger die begehrte Auskunft.

65
Unstreitig hat der Kläger nach dem Erhalt dieser Antworten keine weitere Auskunft nach Art. 15 DSGVO von der Beklagten mehr verlangt. Eine verspätete Auskunftserteilung lag daher nicht vor, selbst wenn man nach der erteilten Auskunft gem. Anlage K 2 noch weitere Auskunftsansprüche als bestehend ansehen würde.

66
Im hiesigen Verfahren hat der Kläger aber auch nicht einmal ansatzweise dargelegt, warum die erteilte Auskunft ungenügend gewesen sein sollte. Zu den klägerischen Spekulationen über eine mögliche Unvollständigkeit oder Unrichtigkeit ist auf die obigen Ausführungen zum hierfür statthaften Verfahren (auf Abgabe einer eidesstattlichen Versicherung) zu verweisen.

67
Außerdem ist der begehrte Schadensersatz von der Anspruchsgrundlage des Art. 82 Abs. 1 DSGVO für immateriellen Schadensersatz nicht gedeckt. Denn dieser erfasst nur Schäden, die durch eine nicht der DSGVO entsprechende Datenverarbeitung entstehen. Dies ergibt sich aus Erwägungsgrund 146, der von Schäden spricht, die „auf Grund einer Verarbeitung“ eintreten. Selbst eine verspätete oder unvollständige Auskunft stellt aber keine Verarbeitung von personenbezogenen Daten dar. Deshalb ist bereits mangels Anspruchsgrundlage kein immaterieller Schadensersatz wegen Nichterteilung von Auskunft denkbar.

68
Der geltend gemachte Zinsanspruch teilt als Nebenforderung das Schicksal der Hauptforderung und unterliegt deshalb ebenfalls der Klageabweisung.

3. Klageantrag zu 5. (außergerichtliche Anwaltskosten)

69
Da kein Anspruch in der Hauptsache besteht, hat der Kläger auch keinen Anspruch auf Ersatz vorgerichtlicher Rechtsanwaltskosten.

70
Die geltend gemachten Rechtshängigkeitszinsen teilen als Nebenforderung das Schicksal der Hauptforderung und unterliegen insoweit ebenfalls der Klageabweisung.

B.

71
Die Kostenentscheidung beruht auf § 91 ZPO.

72
Die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus § 709 S. 1, S. 2 ZPO. C.

73
Die Streitwertfestsetzung richtet sich nach §§ 63, 48, 39 GKG.

74
Die Wertangaben des Klägers in der Klageschrift zu den Anträgen auf Feststellung, Unterlassung und Auskunft wurden von der Beklagtenseite nicht in Frage gestellt.