LG Augsburg, Endurteil v. 04.02.2025 – 125 O 1155/24

Titel:

Beweislastverteilung bei datenschutzrechtlichem Schadensersatz

Normenketten:

DSGVO Art. 5 Abs. 2, Art. 82 Art. 1

ZPO § 253 Abs. 2 Nr. 2

Leitsätze:

1. Für einen Anspruch auf immateriellen Schadensersatz gem. Art. 82 I, II DSGVO aufgrund einer Cyberattacke bei der Beklagten trägt der Kläger die Beweislast für den bei ihm entstandenen Kontrollverlust über personenbezogene Daten. Dazu ist zu beweisen, dass ein Kontrollverlust nicht eingetreten wäre, wenn der Verantwortliche für die Verarbeitung personenbezogener Daten die erforderlichen technischen und organisatorischen Maßnahmen ergriffen hätte.

2. Der übereinstimmende Zeitraum von Spamnachrichten und einem Sicherheitsvorfall bei der Beklagten genügt nicht zur Annahme einer Kausalität.

3. Streitgegenständlich sind lediglich personenbezogene Daten, die klägerseits auch tatsächlich dargelegt wurden.

Schlagworte:

Immaterieller Schadensersatz, Datenschutzverletzung, Kausalität, Feststellungsinteresse, Auskunftserteilung, Unterlassungsanspruch, Beweislast

Fundstelle:

GRUR-RS 2025, 5920

Tenor

1. Die Klage wird abgewiesen.

2. Der Kläger hat die Kosten des Rechtsstreits zu tragen

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

Beschluss

Der Streitwert wird auf 6.000,00 € festgesetzt.

Tatbestand

1

Die Parteien streiten über Schadensersatzansprüche, Auskunftsansprüche, Feststellungsansprüche und Unterlassungsansprüche nach DSGVO.

2

Die Beklagte ist eine portugiesische Fluggesellschaft mit Sitz in Lissabon. Sie bietet ein Vielfliegerprogramm Namens …. Die Teilnahme an diesem Programm ist freiwillig und keine Voraussetzung für die Buchung von Flügen bei der Beklagten. Der Kläger registrierte sich am 13. Januar 2019 als Mitglied bei …. Für die Registrierung gab er persönliche Daten ein, insbesondere:

Anrede,

Vor- und Nachname,

Geburtsdatum,

Mobiltelefonnummer,

E-Mail-Adresse

Land,

Stadt,

Sprache.

3
Die Eingabe der persönlichen Daten war zwingend erforderlich um den Anmeldevorgang bei dem …-Programm abschließen zu können. Mit Abschluss des Registriervorgangs hat die Beklagte noch folgende Daten des Klägers gespeichert:

Datum der Kundenregistrierung,

Vielfliegernummer,

gesprochene Sprachen.

4
Am 25. August 2022 kam es bei der Beklagten zu einem Datenleck. Die Beklagte wurde von einer sogenannten „Ransomware“ angegriffen. Ransomware sind Schadprogramme, die den Computer sperren oder darauf befindliche Daten verschlüsseln. Die Täter versuchen dann die Opfer zu erpressen, indem sie deutliche machen, dass sie die Computer oder Daten erst wieder freigeben, nachdem die Opfer ein Lösegeld gezahlt haben. Den Angreifern gelang der Zugang zu den personenbezogenen Daten, durch den Zugriff auf eine Schnittstelle während der Übertragung der personenbezogenen Daten von dem …-System zu einem anderen Kundeninformationssystem. Der Eintritt in das System der Beklagten erfolgte durch den Diebstahl von Zugangsdaten zu dem Druckersystem eines Providers (Klageerwiderung S. 3).

5
Von dem Sicherheitsvorfall waren folgende personenbezogene Daten des Klägers betroffen:

Anrede,

Vor- und Nachname,

Geschlecht,

Geburtsdatum,

Wohnort,

E-Mail-Adresse,

Handynummer,

Datum der Kundenregistrierung

Vielfliegernummer.

6
Die Daten wurden anschließend auch im Dark Web veröffentlicht, wo sie einer unbestimmbaren Vielzahl Unbefugter zum Missbrauch zur Verfügung stehen (Klage S. 9).

7
Personenbezogene Daten des Klägers wie die E-Mail-Adresse, die Telefonnummer, das Geburtsdatum, seine geografische Position und sogar Passwörter, die Wohnanschrift sowie die IP-Adresse des Klägers waren bereits im Jahr 2012, 2019, 2022 und 2023 Gegenstand weiterer Cyberattacken auf den Musikstreamingdienst Deezer, auf die Cloud Dropbox, die Hotelkette MGM Resorts sowie Bestandteil zweier Funde von Datensammlungen in Hackerforen (s. Anlage B 7 bzw. B6 Auszug aus der Website „Have I Been Pwned“ mit dem Suchbegriff …).

8
Der Kläger war und ist darüber hinaus im Internet aktiv. Er verfügt über ein Profil auf LinkedIn und Facebook. Zudem stellt der Kläger sich auf mindestens drei Internetseiten dar, zu denen ein Blog mit persönlichen Angaben sowie zwei Vorstellungen zu seiner Person im beruflichen Umfeld und seinem Lebenslauf gehört (Anlage B 6 bzw. laut Duplik B7, Auszug aus der Webpräsenz des Klägers).

9
Die Beklagte benachrichtigte einige Kunden zunächst mittels individueller E-Mails über den Vorfall. Nachdem sich jedoch zeigte, dass eine große Anzahl von Kunden von dem Vorfall betroffen war, waren weitere Ermittlungen erforderlich, um die betroffenen Kunden zweifelsfrei zu identifizieren. Aus diesen ergab sich sodann, dass individuelle Benachrichtigungen nicht mehr in allen Fällen hinreichend zeitig würden erfolgen können. Die Beklagte entschied sich daher für die öffentliche Meldung auf ihrer Website, die am 21. September 2022 erfolgte (Anlage B3) und gab Pressemitteilungen heraus (Anlage B2) (vgl. Klageerwiderung S. 6).

10
Nachdem der Kläger über seine Prozessbevollmächtigten von dem Datenschutzvorfall Kenntnis erlangt hatte, kontaktierten die Prozessbevollmächtigten des Klägers die Beklagte im Namen des Klägers (Anlage DB 2), um unter anderem Informationen zu den betroffenen persönlichen Daten zu erhalten und eine Erklärung der grundsätzlichen Regulierungsbereitschaft zu erlangen, auf die die Beklagte mit Schreiben vom 16.02.2024 (Anlage DB 3 = Anlage B4) reagierte, indem sie Auskunft erteilte und Ansprüche abwies.

11
Der Kläger erhob am 27.03.2024 Klage, die der Beklagten am 02.05.2024 zugestellt wurde.

12
Die Klagepartei behauptet:

13
Die Beklagte habe unzureichende Maßnahmen zum Schutz seiner personenbezogenen Daten ergriffen. Voraussetzung für eine erfolgreiche Cyberattacke seien unzureichende technische und organisatorische Maßnahmen zur Sicherung der Verarbeitung personenbezogener Daten. Das Auftreten eines Datenlecks indiziere, dass in technischer Hinsicht nicht ausreichender Schutz gewährleistet worden sei. Der Kläger meint, dass die Beklagte aufgrund offensichtlich unzureichender Sicherheitsmaßnahmen im Bereich des Datenschutzes für das Datenleck und das Abhandenkommen der Daten des Klägers verantwortlich sei.

14
Der Kläger meint ferner, die Beklagte habe die ihr anvertrauten personenbezogenen Daten nicht entsprechend der Anforderungen, die die DSGVO aufgibt, geschützt. Er behauptet, dass äußerst sensible Daten von dem Datenleck betroffen seien. Darunter unter anderem die Ausweisnummer.

15
Der Kläger behauptet weiter, dass die Beklagte, nach dem Auftreten des Datenlecks viel dafür getan habe, den Datenklau zu leugnen und so den Schaden intensiviert habe. Sie habe den Kläger nicht unverzüglich nach dem Auftreten über das Datenleck informiert. Der Kläger habe unbekannte Kontaktversuche per SMS sowie Anrufe und E-Mails erhalten.

16
Seit der Kenntnis des Datenlecks sei der Kläger in einem Zustand von großem Unwohlsein und Sorge über einen möglichen Missbrauch seiner Daten verblieben. Er habe ein verstärktes Misstrauen gegenüber E-Mails und Anrufen verspürt. Er habe seine Handynummer geändert, was zu erheblichem Mehraufwand geführt habe.

17
Der Kläger behauptet, dass die Beklagte mit ihrem Schreiben vom 16.02.2024 nicht adäquat auf die Anfrage des Klägervertreters reagiert haben. Er meint, dass die Beklagte den Auskunftsanspruch des Klägers nicht hinreichend bedient habe, indem die Auskunftserteilung keinerlei konkrete Aussagen enthielt.

18
Schließlich behauptet der Kläger, die Beklagte habe die bestehenden Sicherheitslücken nicht geschlossen. Sie habe es unterlassen, Schutzmaßnahmen gegen den Datenklau anzubringen. Es sei aktuell nicht prüffähig, ob die Beklagte, die ihr zumutbaren Maßnahmen ergriffen habe, um ein neuerliches Abgreifen zu verhindern.

19
Die Klagepartei beantragt zuletzt:

1. Die Beklagte wird verurteilt, an den Kläger als Ausgleich für Datenschutzverstöße und die Ermöglichung der unbefugten Erlangung persönlicher Daten einen immateriellen Schadensersatz, dessen Hohe in das Ermessen des Gerichts gestellt wird, den Betrag von 1.000 EUR aber nicht unterschreiten sollte, nebst Zinsen in Hohe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz der EZB seit Rechtshängigkeit zu zahlen.

2. Die Beklagte wird verurteilt, an den Kläger für die Nichterteilung einer den gesetzlichen Anforderungen entsprechenden außergerichtlichen Datenauskunft i.S.d. Art. 15 DSGVO einen weiteren immateriellen Schadensersatz, dessen Hohe in das Ermessen des Gerichts gestellt wird, den Betrag von 2.000 EUR aber nicht unterschreiten sollte, nebst Zinsen in Hohe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz der EZB seit Rechtshängigkeit zu zahlen.

3. 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 entstanden sind und/oder noch entstehen werden.

4. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall, der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000 EUR, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft, oder einer an ihrem Vertreter zu vollstreckender Ordnungshaft bis zu 6 Monaten, im Wiederholungsfall bis zu 2 Jahren, zu unterlassen, personenbezogene Daten des Klägers Dritten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzunehmen.

5. Die Beklagte wird verurteilt, dem Kläger Auskunft über personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, insbesondere welche Daten durch welche Empfänger zu welchem Zeitpunkt auf welche Art und Weise und aufgrund welcher Sicherheitslücke, soweit vorhanden, bei der Beklagten oder Partnerunternehmen, an die die Beklagte die Daten weitergeleitet hat, unbefugt erlangt werden konnten.

6. Die Beklagte wird verurteilt, den Kläger von außergerichtlich entstandenen Kosten für die anwaltliche Rechtsverfolgung in Höhe von 1.054 EUR freizustellen.

20
Die beklagte Partei beantragt,

die Klage abzuweisen.

21
Die Beklagte bringt im Wesentlichen vor:

22
Die Beklagte behauptet, der Umstand, dass sie Opfer eines kriminellen Angriffs geworden sei, nicht beweise, dass es auf ihrer Seite zu Versäumnissen kam. Vielmehr habe sie angemessene technische und organisatorische Maßnahmen ergriffen. Den Angreifern sei der Zugriff auf die … Datenbank selbst nicht gelungen. Sie hätten die personenbezogenen Daten während einer Übermittlung von dem … System zu einem anderen Kundeninformationssystem erlangt. Bei diesen Daten handle es sich im Übrigen nicht um äußerst sensible Daten, sondern um solche die heutzutage regelmäßig freiwillig im Internet preisgegen werden. Die Angreifer hätten entgegen der Behauptung des Klägers nicht die Ausweisnummer erlangt.

23
Die Beklagte behauptet weiter, dass sie den Sicherheitsvorfall keineswegs geleugnet habe. Sie habe ihre Meldepflicht gegenüber den zuständigen Behörden erfüllt. Darüber hinaus habe sie die Betroffenen in Kenntnis gesetzt.

24
Die Beklagte meint, dass sie dem Auskunftsbegehren des Klägers bereits vor Klageerhebung erfüllt habe.

25

Es seien unverzüglich die Notfallpläne der Beklagten in Gang gesetzt worden. Einige Stunden nach Entdeckung des Vorfalls, sei der Angriff gestoppt worden. Eindämmungs- sowie Reinigungs- und Löschungsmaßnahmen seien ebenfalls unverzüglich gestartet worden. Die Eintrittsstelle, durch die der Diebstahl gelang, sei geschlossen worden.

26
An der mündlichen Verhandlung am 28.11.2024 haben die Prozessbevollmächtigten und der Kläger gem. § 128 a ZPO mit Gestattung des Gerichts (vgl. Beschluss vom 14.10.2024, Bl. 87 f. d.A.) im Wege der Bild- und Tonübertragung vom jeweiligen Kanzleisitz und Wohnort aus teilgenommen.

27
Hinsichtlich der weiteren Einzelheiten des Sach- und Streitstandes wird auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen sowie auf die Sitzungsniederschrift vom 28.11.2024 (Bl. 109/112 d.A.), Bezug genommen.

Entscheidungsgründe

28
Die teilweise zulässige Klage ist unbegründet.

A. Zulässigkeit

29
Die Klageanträge sind teilweise zulässig.

I.

30
Das Landgericht Augsburg ist sachlich gem. §§ 71 I, 23 Nr. 1 GVG zuständig. Die internationale örtliche Zuständigkeit des Amtsgerichts Augsburg ergibt sich aus Art. 18 I Alt. 2 EuGVVO. Demnach können Klagen eines Verbrauchers vor dem Gericht erhoben werden, an dem der Verbraucher seinen Wohnsitz hat. Der Kläger ist Verbraucher und hat seinen Wohnsitz in …, mithin im Landgerichtsbezirk Augsburg.

II. Bestimmtheitsgrundsatz

31
1) Der Klageantrag zu 1 ist trotz fehlender Präzisierung in persönlicher, zeitlicher und sachlicher Hinsicht aufgrund der weiten Auslegung gerade noch bestimmt genug i.S.v. § 253 II Nr. 2 ZPO.

32
Zwar muss die Klageschrift gem. § 253 II Nr. 2 ZPO grundsätzlich neben dem Antrag auch die bestimmte Angabe des Gegenstandes und des Grundes des erhobenen Anspruchs enthalten. Zur Erfüllung dieser gesetzlichen Vorgaben kommt es aber nach der gefestigten Rechtsprechung des BGHs nicht darauf an, ob der maßgebende Lebenssachverhalt bereits in der Klageschrift vollständig beschrieben oder ob der Klageanspruch schlüssig und substanziiert dargelegt worden ist. Vielmehr ist es im Allgemeinen ausreichend, wenn der Anspruch als solcher identifizierbar ist, indem er durch seine Kennzeichnung von anderen Ansprüchen so unterschieden und abgegrenzt wird, dass er Grundlage eines der materiellen Rechtskraft fähigen Vollstreckungstitels sein kann. Es ist eindeutig, dass der Kläger immateriellen Schadensersatz begehrt. Dieser Anspruch ist auch klar von den anderen Ansprüchen abgegrenzt. Zwar wird im Antrag selbst nicht auf einen konkreten Sachverhalt eingegangen, der Kläger macht jedoch deutlich, woraus er seine begehrte Rechtsfolge ableitet, mithin als Ausgleich für Datenschutzverstöße.

33
2) Auch der Klageantrag zu 2 ist trotz seiner weiten Formulierung ebenfalls bestimmt genug i.S.d. § 253 II Nr. 2 ZPO. Er lässt sich unter Heranziehung des Klagevorbringens dahingehend auslegen, dass der Kläger immateriellen Schadensersatz von mindestens 2.000 EUR begehrt, für eine den in Art. 15 DSGVO gesetzlich vorgesehenen Anforderungen nicht entsprechende Datenauskunft. Auch wird unter Heranziehung des gesamten Klagevorbringens klar, dass der Kläger mit „weiterem“ immateriellen Schadensersatz, den aus dem Klageantrag zu 1 geforderten meint.

34

Allerdings können die immateriellen Schäden aufgrund desselben Vorfalls nicht in mehrere Ansprüche aufgespalten werden. Die Geltendmachung eines Schadenersatzbetrags in Hinblick auf den Scraping Vorfall und einen weiteren Betrag in Hinblick auf eine unzureichende Auskunft stellt eine Aufspaltung eines einheitlichen Anspruches, der sich auf mehrere Datenschutzverstöße bezieht, dar. (BGH, Urteil vom 18.11.2024, VI ZR 10/24, Rn. 16). Die Ziffern 1 und 2 der klägerischen Anträge sind daher als einheitlichen Antrag zu behandeln.

35
3) Der Feststellungsantrag in Ziffer 3 ist zulässig, das erforderliche Feststellungsinteresse gem. § 256 Abs. 1 ZPO liegt vor. Vorliegend ist, da der Kläger die Verletzung seines Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG, mithin seines allgemeinen Persönlichkeitsrechts als einem sonstigen absolut geschützten Rechtsgut im Sinne von § 823 Abs. 1 BGB behauptet, die bloße Möglichkeit künftiger Schäden ausreichend (BGH, Urteil vom 18.11.2024, VI ZR 10/24, Rn. 46 ff).

36
4) Der Klageantrag zu 4 hingegen ist nicht hinreichend bestimmt.

37
Der Kläger begehrt, dass die Beklagte es unterlasse, personenbezogene Daten der Klägerseite Dritten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzunehmen. Dieser Unterlassungsantrag ist an den Anforderungen von § 253 II Nr. 2 ZPO gemessen, nicht hinreichend bestimmt.

38
Ein Unterlassungsanspruch ist idR bestimmt genug, wenn auf die konkrete Verletzungshandlung Bezug genommen wird oder wenn der Klageantrag zumindest unter Heranziehung des Klagevortrags unzweideutig erkennen lässt, worin das Unterlassungsgebot liegen soll, also welches Verhalten Seitens des Beklagten Anknüpfungspunkt für die Annahme eines Rechtsverstoßes sein soll. Der Beklagten und dem Vollstreckungsgericht muss klar sein, was genau dem Beklagten verboten ist.

39
Die Formulierung im Unterlassungsantrag „die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzunehmen“ ist zum einen stark an den Gesetzeswortlaut des Art. 32 I DS-GVO angelehnt, der von „unter Berücksichtigung des Stand der Technik (…) geeigneten technischen und organisatorischen Maßnahmen“ spricht. Unterlassungsanträge, die lediglich den Wortlaut eines Gesetzes wiederholen, sind grundsätzlich als zu unbestimmt und damit als unzulässig anzusehen (vgl. BGH GRUR 2024, 1910 Rn. 54, beck-online). Zum anderen sind Formulierungen wie „Dritte“ oder „nach den Stand der Technik mögliche Sicherheitsmaßnahmen“ auch auslegungsbedurftig und damit unzulässig. Dem Kläger wäre es durchaus zumutbar gewesen, zu konkretisieren wen er unter „Dritte“ versteht, indem er die konkrete Verletzungshandlung näher definiert.

III.

40
Der Klageantrag zu 4 enthält zudem ein unzulässiges Antragsbegehren. Vorliegend begehrt der Kläger kein Unterlassen, sondern ein aktives Tun.

41
Unterlassen i.S.d. § 890 I ZPO ist ein untätiges Verhalten, das einen bestimmten Kausalverlauf nicht mitbestimmend beeinflusst. Hier verlangt der Kläger aber, dass die Beklagte die personenbezogenen Daten Dritten nur zugänglich macht, nachdem sie die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vornimmt. Der Kläger fordert also im Schwerpunkt ein aktives Tun, das einen Kausalverlauf in Gang setzt und nicht ein untätiges Verhalten.

B. Begründetheit

42
Die Klage ist aber, soweit sie zulässig ist, unbegründet. Denn einen relevanten Kontrollverlust kausal durch den streitgegenständlichen Vorfall konnte der Kläger nicht zur Überzeugung des Gerichts nachweisen.

I. Kein Anspruch auf Zahlung von Schadensersatz für immateriellen Schaden (Anträge 1 und 2)

43
Der Anspruch auf immateriellen Schadensersatz gem. Art. 82 I, II DSGVO ist unbegründet, denn es liegt kein kausaler Schaden, auch kein durch den Vorfall kausal verursachter Kontrollverlust, vor.

44
Ein Anspruch aus Art. 82 I, II DSGVO setzt voraus, dass personenbezogener Daten unter Verstoß gegen die Bestimmungen der DSGVO von dem Verantwortlichen verarbeitet wurden, der betroffenen Person ein Schaden entstanden ist und zwischen dem Verstoß und dem Schaden ein Kausalzusammenhang besteht.

45
1) Die hier in Rede stehenden Daten (Anrede, Vor- und Nachname, Geschlecht, Geburtsdatum, Wohnort, E-Mail-Adresse, Handynummer, Datum der Kundenregistrierung und Vielfliegernummer) sind unzweifelhaft personenbezogene Daten i.S.v. Art. 4 Nr. 1 DSGVO.

46
2) Diese personenbezogenen Daten hat die Beklagte auch unzweifelhaft automatisiert verarbeitet i.S.v. Art. 4 Nr. 7 DSGVO. Durch die Erstellung eines Accounts wurden die Daten des Klägers automatisch erhoben, erfass und gespeichert, mithin verarbeitet.

47
3) Die Beklagte ist Verantwortliche i.S.v. Art. 4 Nr. 7 DSGVO. Sie wird in der Datenschutzrichtlinie, die auf der Internetseite einsehbar ist, als Verantwortliche genannt.

48
4) Ob die Beklagte gegen die Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 I, Art. 32 I DSGVO und damit gegen Bestimmungen der DSGVO gem. Art. 82 DSGVO verstoßen hat, kann offen bleiben.

49
Obwohl es sich bei dem für die Haftung nach Art. 82 I, II DSGVO erforderlichen Verstoß gegen die Grundsätze für die Verarbeitung personenbezogener Daten um eine anspruchsbegründende Voraussetzung des Art. 82 I DSGVO handelt, ist nicht der Kläger, sondern die Beklagte darlegungs- und beweisbelastet. Diese Beweislastumkehr folgt aus der in Art. 5 II DSGVO enthaltenen spezifischen Beweislastregelung. Art. 5 II DSGVO stellt klar, dass die Beweislast für die Rechtmäßigkeit der Datenverarbeitung beim Verantwortlichen liegt. Dies gilt nicht nur gegenüber Behörden. Auch im Zivilprozess muss die Verantwortliche den Nachweis erbringen (Ehmann/Selmayr/Heberlein, 3. Aufl. 2024, DS-GVO Art. 5 Rn. 43, beck-online). Hierfür muss konkret vorgetragen werden. Ob dies der Fall war und ob der angebotene Sachverständigenbeweis den Nachweis für ausreichende Sicherung gebracht hätte, war nicht entscheidungsrelevant, da kein kausaler Schaden nachgewiesen werden konnte.

50
5) Denn es steht zwar durchaus zur Überzeugung des Gerichts fest, dass der Kläger einen Kontrollverlust über seine persönlichen Daten erlitten hat, sogar echte Einschränkungen in seinem Alltag in Kauf nehmen musste. Letztere ergeben sich auch aus seiner persönlichen Anhörung am 28.11.2024.

51
6) Doch der Kläger hat die erforderliche Kausalität zwischen dem (hierfür unterstellten) Verarbeitungsverstoß seitens der Beklagten und dem ihm entstandenen Kontrollverlust nicht bewiesen. Das Risiko der Nichtbeweisbarkeit verbleibt beim Anspruchsteller (BGH GRUR 2024, 1910 Rn. 37, beck-online).

52
Der Kläger konnte nicht beweisen, dass das bei der Beklagten eingetretene Datenleck vom 25. August 2022, ursächlich dafür war, dass er die Kontrolle über seine personenbezogenen Daten verloren hat.

53
Das Datenleck bei der Beklagten steht fest. Ebenfalls steht fest, dass die Anrede, der Vor- und Nachname, das Geschlecht, das Geburtsdatum, der Wohnort, die E-Mail-Adresse, die Handynummer, das Datum der Kundenregistrierung und die Vielfliegernummer des Klägers von dem Sicherheitsvorfall betroffen waren.

54
Zu dem Kontrollverlust hat der Kläger angeben, dass die Kontaktaufnahmen erstmals oder gehäuft vor zwei Jahren begonnen haben. Dieser Zeitraum würde mit dem des Datenlecks der Beklagten übereinstimmen. Der Kläger hat auch vorgetragen, dass er die betroffene E-Mail-Adresse nur vertrauenswürdigen Adressaten preisgibt, mithin nicht wähl- und grundlos der Öffentlichkeit zugänglich mache. Jedoch verfügt der Kläger über verschiedene persönliche Profile auf mehreren Internetplattformen wie LinkedIn, Facebook und einem persönlichen Blog (Anlage B6 bzw. B7). Die vom Datenleck betroffenen Daten sind zwar auf den Plattformen LinkedIn und Facebook für die Allgemeinheit wiederzufinden, jedoch musste der Kläger diese – jedenfalls zu großen Teilen – für seine Registrierungen bei den jeweiligen Anbietern angeben. Mithin hat der Kläger die vom Datenleck betroffenen personenbezogenen Daten nicht nur der Beklagten preisgegeben, sondern diese auch anderen Anbietern mitgeteilt. Personenbezogene Daten des Klägers, bereits im Jahr 2012, 2019, 2022 und 2023 Gegenstand weiterer Cyberattacken waren. Dies ergibt sich aus der von der Beklagten vorgelegten Suche bei der – von der Klageseite für glaubwürdig befundenen – Webseite https://haveibeenpwned.com (Anlage B7, bzw. B6). Die Anlage B7 bzw. B6 wurde mit der Duplik vom 27.11.2024 zwar zu spät vorgelegt. Der Kläger bestritt ihre Richtigkeit jedoch weder in der mündlichen Verhandlung, noch im nachgelassenen Schriftsatz vom 13.01.2025, sodass keine Beweisaufnahme notwendig wird und damit keine Verzögerung vorliegt.

55
Auf der genannten Webseite wird unter anderem angegeben, im Juli 2019 sei bei MGM Resorts ein Datenleck im Cloud Service entstanden, wodurch 2020 142 Millionen Datensätze im Darknet zum Verkauf angeboten worden seien. Die betroffenen Daten seien Geburtsdaten, E-Mail-Adressen, Namen, Telefonnummern und physische Adressen.

56
Allein hierdurch hatte der Kläger bereits 2019/2020 die Kontrolle über die oben genannten Daten, insbesondere E-Mail-Adresse und Handynummer verloren.

57
Der Kläger konnte auch nicht mit hinreichender Sicherheit sagen, ob die Anrufe oder E-Mails einen konkreten Bezug zu der Beklagten hatten. Dies wäre beispielsweise dann der Fall, wenn sich die Absender oder Anrufer als die Beklagte ausgegeben hätten.

58
Der Kläger konnte nicht ausreichend beweisen, dass der Kontrollverlust, sowie der Erhalt der Anrufe und Spam-Nachrichten auf den Sicherheitsvorfall der Beklagten zurückzuführen sind. Allein der übereinstimmende Zeitraum zwischen dem Sicherheitsvorfall bei der Beklagten und dem vom Kläger angegebenen Zeitraum für den Beginn der Spam-Anrufe und E-Mails genügen dem Gericht nicht, um überzeugt zu sein, dass der Kontrollverlust – selbst wenn dieser nicht mit Sicherheit nachgewiesen sein muss (vgl. BGH GRUR 2024, 1910 Rn. 32, beck-online) – aufgrund des Datenlecks entstanden ist. Mithin wurde nicht hinreichend dargelegt, dass der Kontrollverlust nicht eingetreten wäre, wenn die Beklagte die erforderlichen technischen und organisatorischen Maßnahmen ergriffen hätte.

59
Die nicht in den früheren Kontrollverlusten angegebenen Daten, nämlich Anrede, Vielfliegernummer und Datum der Registrierung, wurden in den klägerischen Schriftsätzen nicht problematisiert. Angesichts der Tatsache, dass der Kläger seinen Account bei der Beklagten zwar nicht aufgelöst hat, deren E-Mails für ihn aber „nicht relevant“ sind und er deren App nicht nutzt und mit der Beklagten auch nicht mehr fliegt (s. Protokoll S. 4), ist hierdurch keine Schadensvertiefung zu erkennen.

60
Das gleiche gilt zu einem – unterstellten – Verstoß gegen eine Benachrichtigungspflicht. Auch hier ist kein zusätzlicher Schaden des Klägers festzustellen.

II. Kein Anspruch auf Feststellung (Antrag 3)

61
Auch der Feststellungsantrag unbegründet, da dem Kläger der Nachweis, dass die vom Vorfall betroffenen, personenbezogenen Daten nicht bereits zuvor zugänglich waren, nicht gelang. Hinsichtlich der nicht vorher bereits bekannten Daten nämlich Anrede, Datum der Kundenregistrierung und Vielfliegernummer ist wie

erörtert keine Gefahr eines Missbrauchs ersichtlich und besteht allenfalls eine theoretische Möglichkeit eines Schadens hierdurch. Diese aber ist für ein Feststellungsinteresse nicht ausreichend.

III. Kein Anspruch auf Auskunftserteilung (Antrag 5)

62
1) Dem Kläger stand ein Anspruch auf Auskunftserteilung gem. Art. 15 DSGVO zu.

63
2) Dieser Anspruch ist jedoch spätestens mit Schreiben vom 17. Juni 2024 durch Erfüllung erloschen, denn das Auskunftsbegehren hat die Beklagte entgegen der Auffassung des Klägers spätestens mit Schreiben vom 17. Juni 2024 erfüllt i.S.v. § 362 I BGB.

64
Der Kläger begehrt Auskunft darüber, welche Daten durch welche Empfänger zu welchem Zeitpunkt auf welche Art und Weise und aufgrund welcher Sicherheitslücke, soweit vorhanden, bei der Beklagten oder Partnerunternehmen, an die die Beklagte die Daten weitergeleitet hat, unbefugt erlangt werden konnten. Dieses Auskunftsrecht steht dem Kläger gem. Art. 15 I lit c. DSGVO zu.

65
Der Auskunftsanspruch erlischt, wenn die geschuldete Leistung an den Gläubiger bewirkt wird. Bereits vor der Klageerhebung hat die Beklagte dem Kläger auf Nachfrage am 16. Februar 2024 mitgeteilt, welche personenbezogene Daten durch den Angriff am 25. August 2022 betroffen waren. Später hat die Beklagte im Rahmen der Klageerwiderung erneut alle betroffenen personenbezogenen Daten deutlich und verständlich aufgelistet (Anrede, Vor- und Nachname, Geschlecht, Geburtsdatum, Wohnort, E-Mail-Adresse, Handynummer, Datum der Kundenregistrierung und die Vielfliegernummer). Sie hat auch hervorgehoben welche Daten eben nicht betroffen waren (Ausweisnummer, Festnetznummer, vollständige Postanschrift, Staatsangehörigkeit, gesprochene Sprachen). In dem Schreiben gab die Beklagte ferner an, dass der Angriff von einer Gruppe von Personen, die sich „Ragnar Locker“ nennen stattfand und die dafür eine sog. Ransomware verwendet haben.

66
Sie gab auch an, aufgrund welcher Sicherheitslücke die Daten erlangt werden konnten, nämlich durch eine Schnittstelle zwischen der Übermittlung personenbezogener Daten von dem …-System zu einem anderen Kundeninformationssystem. Nähere Informationen wie die genaue Identität der Personen, die sich hinter dieser Gruppe verstecken, sind der Beklagten nicht bekannt. Es ist der Beklagten auch auf Grund der besonderen Umstände nicht möglich, Informationen über den konkreten Empfänger zu erhalten und dem Kläger mitzuteilen (s. auch BGH GRUR 2024, 1910 Rn. 76, beck-online). Damit hat die Beklagte ihre Auskunftspflicht hinreichend erfüllt.

IV. Keine Freistellung von Anwaltskosten (Antrag 6)

67
Der Kläger hat entsprechend auch keinen Anspruch auf Freistellung von angefallenen Anwaltskosten.

68
Hierfür hätte, jedenfalls im Zeitpunkt der Einschaltung des Anwalts, ein Schadensersatzanspruch des Klägers bestehen müssen oder die Beklagte hätte sich im Verzug befinden müssen. Selbst bei Unterstellung einer Pflichtverletzung der Beklagten hat nie ein Schadensersatzanspruch des Klägers bestanden, da die Kausalität zum Schaden des Klägers fehlte. Verzug hinsichtlich der Auskunftserteilung lag ebenfalls nicht vor, da der Kläger sich selbst nie an die Beklagte hinsichtlich einer Auskunft gewandt hatte.

C. Kostenentscheidung

69
Die Kostenentscheidung folgt § 91 ZPO.

D. Entscheidung zur vorläufigen Vollstreckbarkeit

70
Die Entscheidung über die vorläufige Vollstreckbarkeit ergibt sich aus 709 ZPO.

E. Streitwert

71
Die Streitwertfestsetzung basiert auf § 63 Abs. 2 S. 1 GKG. Maßgebend war zunächst gemäß § 48 Abs. 1 S. 1 GKG i.V.m. § 4 Abs. 1 Halbsatz 1 ZPO der geltend gemachte Hauptsachebetrag (1.000 + 2.000 € Mindestbetrag Schmerzensgeld). Den Wert des Feststellungsantrags in Ziffer 3 hat das Gericht gem. § 48 Abs. 1 GKG i.V.m. § 3 ZPO auf 1.000 € festgesetzt, den Wert des Unterlassungsantrags auf 1.500 €, des Auskunftsanspruchs auf 500 €. Insgesamt ergibt dies gem. § 48 Abs. 1 GKG i.V.m. § 5 ZPO einen Streitwert von bis zu 6.000 €.