LG Traunstein, Endurteil v. 17.07.2026 – 9 O 1560/24

Titel:

Anforderungen an den Nachweis datenschutzrechtlicher Haftung

Normenketten:

DSGVO Art. 5 Abs. 1, Art. 24, Art. 25, Art. 32, Art. 82

ZPO § 253 Abs. 2 Nr. 2

Leitsätze:

1. Ein Unterlassungsantrag genügt den Anforderungen des § 253 Abs. 2 Nr. 2 ZPO nicht, wenn er den Verantwortlichen lediglich verpflichtet, personenbezogene Daten nicht ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen zugänglich zu machen. Eine derart offene Bezugnahme verlagert die Entscheidung darüber, welche konkreten technischen oder organisatorischen Maßnahmen geschuldet sind, unzulässig in das Vollstreckungsverfahren und macht den Antrag unbestimmt. (Rn. 34) (redaktioneller Leitsatz)

2. Ein Anspruch auf Schadensersatz nach Art. 82 DSGVO setzt eine datenschutzwidrige Verarbeitung personenbezogener Daten voraus. Verstöße gegen bloße Informations-, Transparenz- oder Organisationspflichten der DSGVO begründen für sich genommen keinen Schadensersatzanspruch, solange sie nicht in einer rechtswidrigen Verarbeitung wurzeln oder zu einer solchen führen. (Rn. 38 – 41 und 58) (redaktioneller Leitsatz)

3. Ein Verstoß gegen Art. 32 DSGVO kann nicht bereits aus dem Eintritt eines Datenlecks oder einem erfolgreichen Hackerangriff hergeleitet werden. Maßgeblich ist vielmehr, ob die vom Verantwortlichen ex ante getroffenen technischen und organisatorischen Maßnahmen unter Berücksichtigung des konkreten Risikos, des Stands der Technik und der Art der verarbeiteten Daten als geeignet anzusehen waren. Die betroffene Person muss konkrete Tatsachen vortragen, aus denen sich die Ungeeignetheit dieser Maßnahmen ergibt. Der bloße Hinweis auf den eingetretenen Sicherheitsvorfall genügt hierfür nicht. (Rn. 46 – 48 und 59 – 64) (redaktioneller Leitsatz)

4. Die betroffene Person trägt die Darlegungs- und Beweislast dafür, dass ihre personenbezogenen Daten von dem konkreten Datenschutzvorfall erfasst wurden, ihr hierdurch ein immaterieller Schaden entstanden ist und dieser kausal auf den geltend gemachten DSGVO-Verstoß beruht. Der Nachweis kann weder allein durch einen Eintrag auf Internetplattformen zum Auffinden früherer Datenlecks noch durch pauschale Behauptungen eines Kontrollverlusts oder allgemeine Befürchtungen eines Identitätsmissbrauchs geführt werden. (Rn. 73 – 90) (redaktioneller Leitsatz)

Schlagworte:

Stand der Technik, Darlegungslast, immaterieller Schaden, Kontrollverlust, Kausalität, Bestimmtheit des Klageantrags, unzureichende Sicherheitsvorkehrungen, unangemessenes Schutzniveau

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 8.000,00 € festgesetzt.

Tatbestand

1

Die Parteien streiten über Ansprüche aus der DSGVO aufgrund eines behaupteten Datenlecks bei der Beklagten.

2
Die Beklagte betreibt die Internetpräsenz ... . Bei den Angeboten der Beklagten handelt es sich im Wesentlichen um ... -Software, die sowohl kostenlose (Test-)Versionen als auch ein kostenpflichtiges Angebot beinhaltet. Mit der Software kann man im Wesentlichen … .

3
Der Kläger ist Nutzer des Angebots der Beklagten und hat dort zumindest seine E-Mail-Adresse angegeben.

4
Im Jahr 2020 wurde die Beklagte Opfer eines kriminellen Cyberangriffs bislang unbekannter Dritter, agierend unter dem Namen ... .

5
Diese Dritten waren keine Bediensteten der Beklagten und wurden auch nicht von dieser kontrolliert. Die Angreifer verschafften sich Zugriff auf einen Teilbestand der bei der Beklagten gespeicherten Kunden- bzw. Nutzerdaten und veröffentlichten diese anschließend im Darknet.

6
Diese Daten wurden laut Medienberichten zunächst in einem Hackerforum zu einem Startgebot von ... US-Dollar, später dann für ... US-Dollar und letztendlich kostenlos angeboten. Daraufhin wurden sie am ... 2021 auf der Rechercheplattform „HaveIbeenPwned.com“ hochgeladen, auf der Verwender überprüfen können, ob ihre Daten von vergangenen Datenlecks betroffen sind.

7
Der Kläger trägt vor, er habe sich auf der Internetpräsenz registriert und dort persönliche Daten eingegeben. Bereits zum Start der kostenlosen Testversion sei es notwendig gewesen, persönliche Daten im Rahmen einer Registrierung anzugeben.

8
Die Klagepartei behauptet weiter, dass die Datenschutzerklärung der Beklagte nicht DSGVO-konform sei. Durch den Verstoß gegen diese Vorschriften sei es der Klagepartei bereits deutlich erschwert gewesen, im Sinne der DSGVO Kontakt zu jemandem aufzunehmen, der für das behauptete Datenleck verantwortlich ist und entsprechende Informationen darüber erteilen könnte.

9
Bei dem Datenleck sei ein rund .. GB großer Datensatz mit ... Aufzeichnungen abhandengekommen, die vor allem E-Mail-Adressen, Benutzernamen, Vorsowie Nachnamen, Titel, IP-Adressen, Account-IDs, Namen von Unternehmen, Adressen und Telefonnummern beinhaltet hätten.

10
Die Beklagte habe durch ihr erstes offizielles Statement vorgetäuscht, dass es habe sich nur um einen geringfügigen Vorfall („low impact security incident“) gehandelt habe.

11
Das Auftreten eines Datenlecks, bei dem unbefugte Dritte die Daten des Klägers erlangen konnten indiziere, dass in technischer Hinsicht nicht ausreichender Schutz der Daten gewährleistet worden ist.

12
Die Verknüpfung und nachgelagerte Veröffentlichung von personenbezogenen Daten öffnen dem Missbrauch Tür und Tor. Der Kläger habe einen Kontrollverlust über seine Daten erlitten. Er sei nach Bekanntwerden dieses Datenlecks in einem Zustand von Unwohlsein und Sorge über möglichen Missbrauch seiner Daten verblieben, insbesondere unter Berücksichtigung der vielfältigen Missbrauchsmöglichkeiten. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen gegenüber E-Mails und Anrufen.

13
Der Kläger meint, dass der Anspruch aus Art, 82 DSGVO keiner Erheblichkeitsschwelle unterläge.

14

Die mit dem Verlust der Datenkontrolle einhergehende seelisch belastende Ungewissheit über das Schicksal der personenbezogenen Daten stelle einen immateriellen Schaden im Sinne der DSGVO dar.

15
Der Verantwortliche müsse nachweisen, dass er in keinerlei Hinsicht für den Umstand, durch den der betreffende Schaden eingetreten ist, verantwortlich sei.

16
Der Kläger beantragt,

1. Die Beklagte wird verurteilt, an den Kläger als Ausgleich für Datenschutzverstöße und die Ermöglichung der unbefugten Erlangung persönlicher Daten einen immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 3.000,00 EUR aber nicht unterschreiten sollte, nebst Zinsen in Höhe 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 Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 2.000,00 EUR aber nicht unterschreiten sollte, nebst Zinsen in Höhe 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 250.000,00 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 den außergerichtlich entstandenen Kosten für die anwaltliche Rechtsverfolgung in Höhe von 1.054,10 EUR freizustellen.

17
Die Beklagte beantragt Klageabweisung.

18
Die beklagte Partei trägt vor, geeignete und risikoangemessene technische und organisatorische Sicherheitsstandards implementiert und aufrechterhalten habe. Obwohl sich die Ursache des Angriffs nicht abschließend aufklären ließ, sei der wahrscheinlichste Grund, dass der Angriff ermöglicht wurde, indem sich die Angreifer eigenmächtig und ohne Wissen und Zutun der Beklagten die Zugangsdaten zu einem Benutzerkonto einer/eines Beschäftigten der Beklagten verschafft hätten. Damit beruhe der Angriff alleine auf individuellem menschlichen Versagen.

19
Hinsichtlich des Klägers sei allein dessen E-Mail-Adresse von dem Vorfall betroffen gewesen. Andere personenbezogene Daten des Klägers seien bei der Beklagten, zum Zeitpunkt des Vorfalls, nicht vorhanden gewesen.

20

Der Kläger habe infolge des Vorfalls keine materiellen und immateriellen Nachteile erlitten.

21
Das Gericht hat am 26.06.2026 mündlich verhandelt und den Kläger informatorisch angehört. Auf das Sitzungsprotokoll vom 26.06.2026 wird Bezug genommen. Wegen des ergänzenden Sachvortrags wird auf die gewechselten Schriftsätze nebst Anlagen vollinhaltlich Bezug genommen.

Entscheidungsgründe

22
Die Klage ist teilweise unzulässig und im Übrigen unbegründet.

23
Die Klage ist teilweise zulässig.

24
1. Insbesondere ist das Landgericht Traunstein sachlich und örtlich zuständig.

25
a) Die deutsche Gerichtsbarkeit folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 2. Alt Eu-GVVO. Gemäß Art. 18 Abs. 1 2. Alt EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat. Die Klagepartei ist unzweifelhaft Verbraucher iSd Art. 17 Abs. 1 EuGVVO und hat ihren Wohnort im Bezirk des Landgerichts Kempten.

26
b) Die örtliche Zuständigkeit folgt aus Art. 18 Abs. 1 2. Alt. EuGVVO und Art. 79 Abs. 2 S. 2 DSGVO, § 44 Abs. 1 S. 2 BDSG.

27
c) Die sachliche Zuständigkeit ergibt sich aus §§ 23, 71 GVG.

28
2. Die Klageanträge sind nur teilweise hinreichend bestimmt gemäß § 253 Abs. 2 Nr. 2 ZPO.

29
a) Die Klageanträge 1 und 2 sind zulässig.

30
Zwar verlangt die Klägerseite immateriellen Schadensersatz aus Art. 82 DS-GVO ohne abschließende Bezifferung. Bei Ansprüchen auf eine billige Entschädigung in Geld ist ein unbezifferter Leistungsantrag jedoch ausnahmsweise mit § 253 Abs. 2 Nr. 2 ZPO vereinbar, sofern der zugrunde liegende Lebenssachverhalt und die Bemessungskriterien hinreichend dargelegt werden und zumindest die ungefähre Größenordnung des Anspruchs erkennbar ist. Die Klägerseite hat den einheitlichen Lebenssachverhalt – den streitgegenständlichen Datenschutzverstoß – sowie die daraus abgeleiteten Beeinträchtigungen substantiiert geschildert und im Antrag jeweils einen Mindestbetrag angegeben. Damit ist die Bestimmtheit des Klagebegehrens gewahrt; der Mindestbetrag bildet zugleich den Ausgangspunkt für die Streitwertbemessung und die Beschwer, ohne das Gericht bei der Bemessung der nach billigem Ermessen festzusetzenden Entschädigung rechtlich zu begrenzen.

31
b) Der Klageantrag 3 ist zulässig.

32
Der Kläger begehrt die Feststellung, dass die Beklagte verpflichtet ist, ihm sämtliche materiellen Schäden zu ersetzen, die ihm aus dem unbefugten Zugriff Dritter auf das von der Beklagten gehaltene Datenarchiv bereits entstanden sind oder künftig noch entstehen werden. Ein solcher Feststellungsantrag genügt § 256 Abs. 1 ZPO, weil der zugrunde liegende einheitliche Lebenssachverhalt – der streitgegenständliche Datenschutzvorfall – konkret beschrieben ist und aus Sicht des Klägers die Möglichkeit weiterer Vermögensschäden (etwa infolge Identitätsmissbrauchs, betrugsbedingter Verfügungen oder erforderlicher Abwehr- und Sicherungsmaßnahmen) besteht. Die Gefahr künftiger Schadensentstehung ist damit nicht nur

theoretischer Natur, sondern beruht auf der bereits eingetretenen Datenoffenlegung; hierdurch wird das nach § 256 ZPO erforderliche Feststellungsinteresse begründet. Der Antrag ist ausreichend bestimmt, weil er die haftungsbegründenden Umstände und die Art der geltend gemachten Schäden durch die Bezugnahme auf alle aus dem Zugriff resultierenden materiellen Schäden eingrenzt und die Feststellungspflicht der Beklagten auf diesen Lebenssachverhalt beschränkt.

33
c) Der Klageantrag 4 ist unzulässig.

34
Der Klageantrag ist bereits unzulässig, da er nicht den gesetzlichen Bestimmtheitsanforderungen des § 253 Abs. 2 Nr. 2 ZPO entspricht. Nach ständiger Rechtsprechung des Bundesgerichtshofs muss ein Unterlassungsantrag so konkret gefasst sein, dass der Streitgegenstand klar umrissen ist, der Beklagte sein Verhalten darauf einstellen kann und die Entscheidung darüber, was verboten ist, nicht unzulässig aus dem Erkenntnisverfahren in das Vollstreckungsverfahren nach § 890 ZPO verlagert wird (vgl. BGH, Urteil vom 26.01.2017 – ZR 207/14, Rn. 17; BGH, Urteil vom 11.02.2021 – ZR 132/19, Rn. 26). Diesen Anforderungen wird der klägerische Antrag nicht gerecht, da die Formulierung, Daten nicht ohne „die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ zugänglich zu machen, gänzlich unbestimmt ist. Sie lässt völlig offen, welche konkreten technischen oder organisatorischen Vorkehrungen die Beklagte ergreifen muss. Da der „Stand der Technik“ zudem ein hochgradig dynamischer Begriff ist, müsste die komplexe Frage, welche konkreten Sicherheitsvorkehrungen im Zeitpunkt einer potenziellen Zuwiderhandlung tatsächlich möglich und geboten waren, erst im Vollstreckungsverfahren – gegebenenfalls mithilfe von IT-Sachverständigen – geklärt werden. Eine solche Verlagerung des materiellrechtlichen Streits ist jedoch unzulässig und führt zur Abweisung des Antrags (vgl. auch BGH, Urteil vom 16.05.2013 – ZR 216/11, Rn. 9; BGH, Urteil vom 02.06.2022 – ZR 140/21, Rn. 20).

35
Die Klage ist im Übrigen unbegründet.

36
1. Die Klagepartei hat gegen die Beklagte keinen Anspruch auf Ersatz immaterieller Schäden aus Art. 82 Abs. 1 DSGVO.

37
a) Bereits der Anwendungsbereich des Art. 82 DSGVO ist nicht eröffnet.

38
Nach Art. 82 Abs. 1 DSGVO setzt ein Anspruch auf Schadensersatz voraus, dass einer Person wegen eines Verstoßes gegen die Verordnung ein materieller oder immaterieller Schaden entstanden ist. Da der sachliche Anwendungsbereich der DSGVO gemäß Art. 2 Abs. 1 DSGVO die ganz oder teilweise automatisierte bzw. strukturierte nichtautomatisierte Verarbeitung personenbezogener Daten umfasst, ist Anknüpfungspunkt der Haftung stets eine datenschutzwidrige Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO. Dies bestätigt auch Erwägungsgrund 146 S. 1, wonach der Schadensersatz Schäden auffangen soll, die einer Person „aufgrund einer Verarbeitung“ entstehen, die mit der DSGVO nicht im Einklang steht.

39
Gemäß Art. 4 Nr. 2 DSGVO ist eine „Verarbeitung“ jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang (oder jede solche Vorgangsreihe) im Zusammenhang mit personenbezogenen Daten, wie etwa das Erheben, Erfassen, Speichern, Auslesen oder Offenlegen.

40
Die behauptete Verletzung bloßer Benachrichtigungs- oder Informationspflichten wird von diesem Begriff hingegen nicht erfasst (vgl. LG Essen, Urteil vom 10.11.2022, Az. 6 O 111/22; AG Strausberg, Urteil vom 13.10.2022, Az. 24 C 54/22, BeckRS 2022, 27811; LG Heilbronn, Urteil vom 13.01.2023, Az.

41
Bu 8 O 131/22). Eventuelle Verstöße gegen die Artt. 13, 14, 15, 24, 25 und 34 DSGVO, die lediglich Informations-, Transparenz- oder Organisationspflichten begründen, scheiden als haftungsbegründende Tatbestände im Rahmen des Art. 82 DSGVO somit aus.

42

b) Jedenfalls liegen keine anspruchsbegründenden Pflichtverstöße der Beklagten gegen die Bestimmungen der Datenschutz-Grundverordnung (DSGVO) vor.

43
aa) Kein Verstoß gegen Art. 5 Abs. 1 DSGVO

44
Ein Verstoß der Beklagten gegen die in Art. 5 Abs. 1 DSGVO normierten Grundsätze der Datenverarbeitung ist nicht festzustellen.

45
Nach diesen Grundsätzen müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“). Diese allgemeinen Prinzipien werden durch die Informations- und Aufklärungspflichten der Art. 12, 13 und 14 DSGVO konkretisiert.

46
Diesem Maßstab ist die Beklagte gerecht geworden. Sie hat substantiiert dargelegt, dass sie angemessene technische und organisatorische Vorkehrungen gegen den unbefugten Abfluss von Daten getroffen hatte und das schädigende Ereignis auf individuellem, ex ante nicht vermeidbarem menschlichen Versagen beruhte.

47
Demgegenüber erweist sich das Vorbringen des Klägers, das bloße Auftreten eines Datenlecks indiziere bereits unzureichende Sicherheitsvorkehrungen und ein unangemessenes Schutzniveau, als unsubstantiiert und damit prozessual unbeachtlich. Nach ständiger höchstrichterlicher Rechtsprechung ist der Vortrag einer Partei nur dann hinreichend substantiiert, wenn sie Tatsachen anführt, die in Verbindung mit einem Rechtssatz geeignet sind, das geltend gemachte Recht als in ihrer Person entstanden erscheinen zu lassen; pauschale Behauptungen ohne greifbare Anhaltspunkte genügen dem nicht (vgl. BGH, Beschluss vom 9. Februar 2009 – II ZR 77/08, WM 2009, 1154 Rn. 4; BGH, Beschluss vom 21. Mai 2007 – II ZR 266/04, ZIP 2007, 1524 Rn. 8; BGH, Urteil vom 25. Juli 2005 – VIII ZR 199/03, WM 2005, 1847, 1848 m.w.N.).

48
Soweit die Klägerseite meint, aus dem Vorfall selbst auf einen Verstoß schließen zu können, verkennt sie die Verteilung der Darlegungslast. Nach der Rechtsprechung des Gerichtshofs der Europäischen Union begründet eine Verletzung des Schutzes personenbezogener Daten als solche nicht bereits die Annahme, dass die von dem Verantwortlichen getroffenen Sicherheitsmaßnahmen nicht „geeignet“ im Sinne der Art. 24, 32 DSGVO waren (vgl. EuGH, Urteil vom 14. Dezember 2023 – C-340/21 [Natsionalnaagentsia za prihodite], NJW 2024, 515 Rn. 30 ff.). Ein „Verschulden auf erster Stufe“ allein durch das Gelingen eines Hackerangriffs scheidet aus.

49
bb) Kein Verstoß gegen Art. 6 Abs. 1, Art. 13 Abs. 1 DSGVO Ein Verstoß gegen Art. 6 Abs. 1 und Art. 13 Abs. 1 DSGVO liegt nicht vor. Der unbefugte Abzug der Daten durch kriminelle Dritte („Datenleck“) stellt keine der Beklagten zuzurechnende Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar, die einer gesetzlichen Erlaubnis nach Art. 6 Abs. 1 DSGVO bedurft hätte. Da die Beklagte den unbefugten Zugriff nicht veranlasst oder gesteuert hat, war sie insoweit auch nicht zu einer vorherigen Information des Klägers nach den Maßgaben der Art. 13 oder Art. 14 DSGVO verpflichtet.

50
cc) Kein Verstoß gegen Art. 15 DSGVO

51
Die Beklagte hat ihre Pflichten aus Art. 15 Abs. 1 DSGVO nicht verletzt.

52
Der Auskunftsanspruch des Klägers ist durch das außergerichtliche Auskunftsschreiben der Beklagten (Anlage DB 3) gemäß § 362 Abs. 1 BGB durch Erfüllung erloschen. Dieses Schreiben enthält erschöpfende Angaben über die konkret verarbeiteten personenbezogenen Daten, deren Verwendungszweck, Herkunft,

Speicherdauer, das Nichtvorliegen eines Profilings sowie über potenzielle Empfänger im Sinne des Art. 15 Abs. 1 lit. c DSGVO.

53
Soweit die Beklagte im Rahmen dieses Schreibens keine Angaben dazu gemacht hat, an welche konkreten unbefugten Dritten die Daten im Zuge des Hackerangriffs abgeflossen sind, führt dies nicht zu einer Unvollständigkeit der Auskunft. Der Anspruch aus Art. 15 Abs. 1 DS-GVO ist insoweit wegen Unmöglichkeit nach § 275 Abs. 1 BGB ausgeschlossen. Der unbefugte Zugriff erfolgte unstreitig von außen durch unbekannte Akteure. Da die Identität der Angreifer für die Beklagte nicht ermittelbar ist, ist ihr die Erteilung dieser Auskunft im Rechtssinne unmöglich.

54
Gleiches gilt für die exakte zeitliche Eingrenzung des Datenabflusses bezüglich der konkreten Daten des Klägers. Die Beklagte hat im Rahmen des ihr Möglichen über den bekannten Gesamtzeitraum des Vorfalls informiert. Weitergehende Auskunftspflichten treffen den Verantwortlichen nach Art. 15 DSGVO nicht, wenn die Informationen außerhalb seines Kenntnis- und Ermittlungsbereichs liegen (vgl. zur Begrenzung des Auskunftsanspruchs auf das tatsächlich Ermittelbare: BGH, Urteil vom 5. März 2024 – VI ZR 330/21, NJW 2024, 1805 Rn. 18 ff.).

55
dd) Kein Verstoß gegen die Art. 24, 25 Abs. 2 DSGVO Ein Verstoß gegen die Pflicht zur Gewährleistung datenschutzfreundlicher Voreinstellungen gemäß Art. 25 Abs. 2 DSGVO (sog. „privacy by default“) liegt nicht vor.

56
Die Vorschrift des Art. 25 Abs. 2 DSGVO verpflichtet den Verantwortlichen, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Dies soll insbesondere verhindern, dass Daten ohne Zutun der betroffenen Person einer unbestimmten Zahl von Personen zugänglich gemacht werden.

57
Diesen Vorgaben hat die Beklagte entsprochen. Für die Registrierung auf der Plattform der Beklagten war unstreitig lediglich die Angabe einer E-Mail-Adresse erforderlich. Diese Adresse war für andere Nutzer oder die Öffentlichkeit von vornherein nicht einsehbar, sondern wurde ausschließlich intern verwendet. Eine restriktivere, datenschutzfreundlichere Voreinstellung war mithin technisch und konzeptionell nicht möglich.

58
Zudem scheidet ein Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO wegen eines etwaigen Verstoßes gegen Art. 25 DSGVO bereits aus Rechtsgründen aus. Bei den Vorgaben aus Art. 25 DSGVO handelt es sich um rein organisatorische und der eigentlichen Datenverarbeitung vorgelagerte Pflichten (Vollzugspflichten im Rahmen der Systemgestaltung). Ein bloßer Verstoß gegen diese strukturellen Pflichten zur Systemeinrichtung vermag für sich genommen – ohne eine daran anknüpfende, konkrete rechtswidrige Verarbeitungstätigkeit – keinen Schadensersatzanspruch der betroffenen Person auszulösen (vgl. BGH, Urteil vom 9. Juli 2024 – VI ZR 34/23, NJW 2024, 2741 Rn. 22 ff.; siehe auch Gola/Heckmann/Nolte/Werkmeister, DSGVO, 3. Aufl. 2022, Art. 25 Rn. 3, 34).

59
ee) Kein Verstoß gegen Art. 32 DSGVO

60
Die Beklagte hat auch nicht gegen ihre Pflicht zur Gewährleistung der Sicherheit der Verarbeitung aus Art. 32 DSGVO verstoßen.

61
Nach Art. 32 Abs. 1 DSGVO haben der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Norm verlangt jedoch keinen absoluten, unüberwindbaren Schutz gegen jedwede kriminelle Angriffe ex post. Maßgeblich ist vielmehr eine exante-Betrachtung im Wege einer risikobasierten Prognoseentscheidung unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie

der Eintrittswahrscheinlichkeit und der Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen (vgl. EuGH, Urteil vom 14. Dezember 2023 – C-340/21, NJW 2024, 515 Rn. 35).

62
Dass die von der Beklagten ergriffenen Sicherheitsvorkehrungen diesen Anforderungen ex ante nicht genügten, hat der Kläger nicht hinreichend substantiiert dargelegt. Die Beklagte hat demgegenüber detailliert und klägerseits unbestritten vorgetragen, welche konkreten Sicherheitsbarrieren und Schutzmechanismen zum Zeitpunkt des Vorfalls implementiert waren, um die verarbeiteten E-Mail-Adressen vor unbefugten externen Zugriffen zu schützen.

63
Bei der Bemessung des Schutzniveaus war insbesondere zu berücksichtigen, dass die Beklagte von der Klagepartei lediglich die E-Mail-Adresse ohne ein dazugehöriges Passwort verarbeitete. Die Verarbeitung einer isolierten E-Mail-Adresse weist eine verhältnismäßig geringe Schadensgeneigtheit auf, weshalb an die Sicherheitsmaßnahmen keine überspannten Anforderungen zu stellen waren.

64
Das Gericht konnte sich insoweit auch nach informatorischer Anhörung des Klägers nicht davon überzeugen, dass dieser über seine E-Mail-Adresse hinausgehende weitere personenbezogene Daten bei der Beklagten angegeben hatte. Dies wurde von der Beklagten substantiiert bestritten, welche mitteilte, dass eine Negativauskunft ergeben habe, dass der Beklagte allenfalls den ... dienst der Beklagten genutzt haben könne, weil keine Daten über ihn vorlägen. Der Kläger konnte darauf keine weiteren sein Vorbringen stützende Nachweise vorlegen, etwa Bestätigungs-E-Mails oder Screenshots.

65
ff) Kein Verstoß gegen Art. 33 DSGVO

66
Schließlich hat die Beklagte nicht gegen ihre Meldepflicht gegenüber der Aufsichtsbehörde aus Art. 33 Abs. 1 DSGVO verstoßen.

67
Nach dieser Vorschrift hat der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten unverzüglich – und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde – der zuständigen Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die persönliche Rechtssphäre führt.

68
Die Beklagte hat diese Frist gewahrt. Ihr wurde der Vorfall unstreitig am ... 2020 durch ihren Dienstleister ... bekannt. Die Meldung an die nach Art. 55, 56 DSGVO im Wege des „One-Stop-Shop-Verfahrens“ international zuständige irische Datenschutzbehörde (Irish Data Protection Commission – IDPC) erfolgte am ... 2020 (Anlage B 34).

69
Eine frühere Meldung war der Beklagten nicht zumutbar, da zu diesem Zeitpunkt das tatsächliche Ausmaß und das Vorliegen eines konkreten Risikos für die Betroffenen noch verifiziert werden mussten. Eine Pflichtverletzung scheidet zudem aus, weil die Meldepflicht nach Art. 33 Abs. 1 DSGVO voraussetzt, dass dem Verantwortlichen ein systemischer oder kausaler Datenschutzverstoß anzulasten ist, was vorliegend – wie dargetan – gerade nicht der Fall ist.

70
c) Jedenfalls fehlt es aber an einem ersatzfähigen Schaden der Klagepartei im Sinne des Art. 82 DSGVO

71
aa) Nach dem Ergebnis der persönlichen Anhörung des Klägers konnte sich das Gericht nicht mit der für nötigen Sicherheit davon überzeugen, dass der Kläger über seine E-Mail-Adresse hinaus weitere personenbezogene Daten bei der Beklagten angegeben hat. Der Kläger hat zwar behauptet, seine vollständigen Personalien, also Name, Adresse und Telefonnummer bei der Beklagten angegeben zu haben. Diese von der Beklagten bestrittene Behauptung konnte aber durch nichts verifiziert werden. Insbesondere ergab eine Abfrage der Telefonnummer des Klägers ... auf der Rechercheplattform databreach.com, dass diese von keinerlei Datenleaks betroffen war.

72
Ob die isolierte E-Mail-Adresse des Klägers ohne Verknüpfung mit weiteren Identifikationsmerkmalen überhaupt eine Information über eine identifizierbare natürliche Person im Sinne des Art. 4 Nr. 1 DSGVO darstellt, kann jedoch letztlich dahinstehen, da die Klage bereits aus anderen Gründen unbegründet ist.

73
bb) Der Kläger hat nicht einmal schlüssig dargetan und bewiesen, dass seine E-Mail-Adresse tatsächlich von dem konkreten Datenvorfall bei der Beklagten betroffen war.

74
Als anspruchsbegründende Tatsache trägt die Klägerseite hierfür die volle Darlegungs- und Beweislast; eine Beweislastumkehr oder Beweiserleichterung zugunsten der betroffenen Person sieht die DSGVO insoweit nicht vor (vgl. BGH, Urteil vom 18. November 2024 – VI ZR 10/24, GRUR-RS 2024, 31967 Rn. 24).

75
Diesen Beweis hat der Kläger nicht erbracht:

76
Der Kläger legt diesbezüglich lediglich einen Auszug der Plattform haveibeenpwned.com vor. Ein Eintrag auf einer derartigen Plattform ist für sich genommen nicht geeignet, den Vollbeweis für die tatsächliche Betroffenheit von einem spezifischen Datenleck zu erbringen (vgl. OLG Dresden, Hinweisbeschluss vom 18. Juni 2024 – 4 U 156/24, GRUR-RS 2024, 19396; LG Freiburg, Urteil vom 24. Mai 2024 – 8 O 304/23, ZD 2024, 534; LG Lübeck, Urteil vom 16. Februar 2024 – 15 O 214/23, GRUR-RS 2024, 13166 Rn. 49). Die Funktionsweise und die Datengrundlage dieser Plattform entziehen sich einer verlässlichen gerichtlichen Überprüfung. Der Plattformbetreiber weist in seinen Nutzungsbedingungen selbst darauf hin, dass ein Treffer nicht zwingend eine tatsächliche Betroffenheit des Nutzers impliziert (vgl. von Wickede/Berchtold, ZD 2025, 258; Hillert, jurisPR-ITR 6/2024, Anm. 5).

77
Einer Einholung des beantragten Sachverständigengutachtens bedurfte es mangels greifbarer Anhaltspunkte und einer verlässlichen Datengrundlage nicht; die Beweiserhebung liefe auf einen unzulässigen Ausforschungsbeweis hinaus.

78
cc) Selbst bei Unterstellung einer DSGVO-Pflichtverletzung der Beklagten und einer Betroffenheit des Klägers ist dem Kläger kein durch den Verstoß kausal verursachter Schaden entstanden.

79
(1) Der Verantwortliche haftet nach Art. 82 Abs. 1 DSGVO nur für Schäden, die kausal durch die konkrete rechtswidrige Verarbeitung verursacht wurden (vgl. EuGH, Urteil vom 25. Januar 2024 – C-687/21 [MediaMarktSaturn], NZG 2024, 320 Rn. 58).

80
Die Klägerseite trägt für das Vorliegen des Schadens sowie für dessen Kausalität die volle Darlegungs- und Beweislast nach den allgemeinen zivilprozessualen Grundsätzen des § 286 ZPO. Erforderlich ist ein für das praktische Leben brauchbarer Grad an Gewissheit, der Zweifeln Schweigen gebietet, ohne sie völlig auszuschließen (vgl. BGH, Urteil vom 23. Juni 2020 – VI ZR 435/19, VersR 2021, 1497 Rn. 13).

81
Einen solchen Grad an Gewissheit vermochte das Gericht nicht zu gewinnen.

82
Ein immaterieller Schaden des Klägers ist nicht feststellbar.

83
Zwar kann nach der aktuellen höchstrichterlichen Rechtsprechung bereits der – auch bloß kurzzeitige – Verlust der Kontrolle über personenbezogene Daten einen ersatzfähigen immateriellen Schaden im Sinne des Art. 82 Abs. 1 DSGVO begründen, ohne dass der Nachweis weiterer spürbarer negativer Folgen oder das Erreichen einer Erheblichkeitsschwelle erforderlich ist (vgl. BGH, Urteil vom 18. November 2024 – VI

ZR 10/24, GRUR-RS 2024, 31967 Rn. 30; EuGH, Urteil vom 4. Oktober 2024 – C-200/23, juris Rn. 145 f. – Agentsia po vpisvaniyata; EuGH, Urteil vom 20. Juni 2024 – C-590/22, DB 2024, 1676 Rn. 33). Ein solcher Schaden setzt jedoch voraus, dass der betroffene Nutzer einen tatsächlichen, subjektiv empfundenen Kontrollverlust erlitten hat, der sich in einer konkreten persönlichen Beeinträchtigung (wie etwa Unwohlsein, Ängsten oder Sorgen) manifestiert. Die bloße Verletzung einer DSGVO-Norm als solche begründet noch keinen Schadensersatzanspruch (vgl. EuGH, Urteil vom 4. Mai 2023 – C-300/21 [Österreichische Post], NJW 2023, 1940 Rn. 42).

84
Eine solche subjektive Beeinträchtigung des Klägers vermochte das Gericht nach dem Ergebnis der persönlichen Anhörung des Klägers gemäß § 141 ZPO nicht festzustellen:

85
Die Schilderungen des Klägers in der mündlichen Verhandlung waren unkonkret und ließen die erforderliche persönliche Betroffenheit vermissen. Der pauschale Vortrag in der Klageschrift zu „großer Sorge vor Identitätsmissbrauch“ erschöpft sich in standardisierten Textbausteinen, die von den Prozessbevollmächtigten des Klägers in einer Vielzahl gleichgelagerter Verfahren wortgleich verwendet werden.

86
Eine objektive Nachvollziehbarkeit von Ängsten scheidet zudem im Hinblick darauf aus, dass ausschließlich die E-Mail-Adresse des Klägers betroffen war.

87
(2) Soweit der Kläger den vermehrten Erhalt von Spam-E-Mails und unerwünschten Anrufen als Schaden rügt, fehlt es an dem Nachweis der Kausalität zum streitgegenständlichen Datenvorfall.

88
Der Erhalt von Spam-E-Mails ist ein im Alltag allgegenwärtiges Phänomen, das zahlreiche Ursachen haben kann. Nach dem eigenen Vortrag des Klägers und der vorgelegten Anlage DB 1 war dessen E-Mail-Adresse bereits in der Vergangenheit von mindestens einem weiteren, zeitlich vorgelagerten Datenleak bei Drittanbietern betroffen.

89
Es ist daher prozessual nicht auszuschließen, dass der Spam-E-Mail-Eingang auf diese anderweitigen Datenabflüsse zurückzuführen ist. Die zeitliche Nähe zum hiesigen Vorfall reicht für den Kausalitätsnachweis nach § 286 ZPO nicht aus. Soweit der Kläger zudem Spam-Anrufe auf seinem Mobiltelefon rügt, scheidet eine Kausalität von vornherein aus, da seine Mobilfunknummer im Rahmen des Registrierungsprozesses bei der Beklagten unstreitig überhaupt nicht erhoben oder verarbeitet wurde.

90
Darüber hinaus hat der Kläger eigenverantwortlich seinen vollen Namen, sein Geburtsjahr, seine E-Mail-Adresse und seine Telefonnummer zusammen mit einem Foto seiner Person in der im Internet frei verfügbaren Pressemappe der (Anlage B42) veröffentlicht.

91
Die Kontrolle über seine personenbezogenen Daten hat der Kläger damit lange vor dem streitgegenständlichen Vorfall selbst aufgegeben.

92
2. Klageantrag 2 ist unbegründet.

93
Verstöße gegen die Datenschutz-Grundverordnung können nicht isoliert beurteilt werden, da sie sämtlich in einem einheitlichen Geschehen wurzeln, das hinsichtlich der damit verbundenen Folgen nicht in einzelne Datenschutzverstöße aufgespalten werden kann. Der Schadensersatzanspruch der Klagepartei ist unter Ziffer 1 bereits abschließend beurteilt worden, wobei nur ergänzend anzuführen ist, dass es im Hinblick auf eine etwaige unterlassene / verspätete Meldung des Vorfalls gegenüber der Klagepartei und der irischen Datenschutzbehörde jedenfalls an der Kausalität des vorgetragenen Schadens fehlt. Der vorgetragene Kontrollverlust ist nicht auf die vorgenannten Verstöße zurückzuführen. Einen darüber hinausgehenden Schaden hat die Klagepartei nicht substantiiert dargelegt.

94
Ungeachtet dessen besteht wie oben dargelegt überhaupt kein Schaden und Schadensersatzanspruch.

95
3. Klageantrag 3 ist unbegründet.

96
Da demnach bereits dem Grunde nach kein Schadensersatzanspruch aus Art. 82 Abs. 1 DSGVO besteht, erweist sich auch der Feststellungsantrag bezüglich künftiger materieller Schäden als unbegründet.

97
4. Klageantrag 5 ist unbegründet.

98
Der Kläger hat gegen die Beklagte keinen Anspruch auf weitergehende Auskunft.

99
Soweit dem Kläger ein Anspruch auf Auskunft über die ihn betreffenden, von der Beklagten verarbeiteten Daten nach Art. 15 Abs. 1 DSGVO zustand, ist dieser Anspruch durch das detaillierte Auskunftsschreiben der Beklagten vom ... 2024 (Anlage DB 3) gemäß § 362 Abs. 1 BGB durch Erfüllung erloschen.

100
Soweit der Kläger darüber hinaus Auskunft über die genauen technischen Details der Sicherheitslücke, den exakten Zeitpunkt des Zugriffs der Angreifer sowie die konkreten Empfänger des Datenlecks begehrt, besteht ein solcher Anspruch nicht. Da der Kläger eine Betroffenheit seiner Daten bereits nicht nachzuweisen vermochte (siehe oben), ist die Beklagte ihm gegenüber nicht auskunftspflichtig.

101
Überdies ist die Beklagte im Rechtssinne nicht verpflichtet, die Identität der unbefugten Angreifer („Hackergruppierung“) offenzulegen. Zwar erstreckt sich das Auskunftsrecht aus Art. 15 Abs. 1 lit. c DSGVO grundsätzlich auch auf die konkreten Empfänger der Daten (vgl. EuGH, Urteil vom 12. Januar 2023 – C-154/21 [Österreichische Post], NJW 2023, 973 Rn. 37 ff.). Das Auskunftsrecht findet jedoch unter Berücksichtigung des Verhältnismäßigkeitsprinzips seine Grenze dort, wo dem Verantwortlichen die Ermittlung der konkreten Empfänger – wie bei kriminellen, anonym agierenden Hackern – unmöglich oder unzumutbar ist (vgl. EuGH, Urteil vom 12. Januar 2023 – C-154/21, NJW 2023, 973 Rn. 47 f.; BGH, Urteil vom 18. November 2024 – VI ZR 10/24, GRUR-RS 2024, 31967 Rn. 75-77).

102
5. Mangels Anspruch in der Hauptsache waren auch die Nebenansprüche abzuweisen.

III. Nebenentscheidungen

103
1. Die Kostenentscheidung ergibt sich aus § 91 Abs. 1 S. 1 ZPO.

104
2. Der Ausspruch zur vorläufigen Vollstreckbarkeit folgt aus §§ 708 Nr. 11, 711 ZPO.

105
3. Der Streitwert war entsprechend dem klägerischen Begehren festzusetzen, §§ 39 Abs. 1, 48 Abs. 1 GKG, §§ 1 ff ZPO. So ergibt sich der Streitwert für die Klageanträge 1 und 2 aus der Bezifferung und für die weiteren Klagenanträge hat das Gericht jeweils einen Wert von 1.000,00 € angesetzt.