Landgericht Braunschweig

Im Namen des Volkes

Urteil

7 O 47/24

in dem Rechtsstreit

[redacted]

- Klägerin -

Prozessbevollmächtigter:
[redacted]

gegen

[redacted]

- Beklagte -

Prozessbevollmächtigte:
[redacted]

hat das Landgericht Braunschweig – 7. Zivilkammer – durch [redacted] am Landgericht [redacted] als [redacted] auf die mündliche Verhandlung vom 17.01.2025 für Recht erkannt:

1. Die Beklagte wird verurteilt, an die Klägerin 22.600 Euro nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 01.05.2024 zu zahlen.

2. Die Beklagte wird verurteilt, an die Klägerin vorgerichtliche Rechtsanwaltskosten von 1.375,88 Euro zu zahlen.

3. Die Kosten des Rechtsstreits trägt die Beklagte.

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

Tatbestand:

Die Klägerin begehrt von der Beklagten die Rückzahlung des Kaufpreises für ein Fahrzeug infolge mangelnder Sicherheitsvorkehrungen beim elektronischen Rechnungsversand.

Die Beklagte, die ein Autohaus betreibt, schaltete im Dezember 2023 eine Verkaufsanzeige für einen Golf VII GTD auf der Webseite www.mobile.de. Die Klägerin wurde darauf aufmerksam und entsandte ihren Bruder, der in KfZ-Belangen versiert ist, zur Besichtigung. Seitens der Beklagten wurde die Besichtigung vom Zeugen [redacted] durchgeführt. Die Klägerin entschloss sich, das Fahrzeug zu kaufen. Dafür übersandte sie auf Anforderung der Beklagten eine Kopie ihres Personalausweises per E-Mail an den Zeugen[redacted] unter der Adresse [redacted] Den seitens der Beklagten unterzeichneten Kaufvertrag, in welchen ihre Personendaten eingepflegt worden waren, erhielt die Klägerin als PDF-Anhang zur E-Mail des Zeugen [redacted] vom 12.12.2023 15:28 Uhr. In diesem Vertragsdokument (Anlage Vergleich Verträge, Schriftsatz vom 06.08.2024, linke Seite, Bl. 106 d.A.) war die Bankverbindung der Beklagten bei der [redacted] (IBAN: [redacted]) ausgewiesen.

Am 12.12.2023 15:36 Uhr erhielt die Klägerin von der E-Mail Adresse des [redacted] eine weitere E-Mail mit der Aufforderung, „den Anhang der ersten E-Mail“ zu ignorieren und stattdessen den „richtigen Anhang“ dieser E-Mail zu beachten. Diese E-Mail wurde durch unbekannte Dritte versandt. Im Anhang der E-Mail befand sich ein weiteres Kaufvertragsdokument im PDF-Format, welches als Bankverbindung der Beklagten ein von dieser nicht geführtes Konto bei der [redacted] Bank auswies (IBAN: [redacted]). Um eine Verwechslung auszuschließen, löschte die Klägerin die erste E-Mail vom 12.12.2023 15:28 Uhr und das angehängte Vertragsdokument. Die Klägerin signierte den gefälschten Vertrag und schickte ihn an die E-Mail Adresse des Zeugen [redacted] zurück.

Im E-Mail-Postfach [redacted] hingegen ging ein Vertragsdokument ein, welches die korrekte Bankverbindung der Beklagten bei der [redacted] auswies (Anlage Vergleich Verträge, Schriftsatz vom 06.08.2024, rechte Seite, Bl. 106 d.A.). Auch dies wurde durch unbekannte Dritte manipuliert.

Die Klägerin veranlasste wenige Stunden nach Übersendung des von ihr unterzeichneten Vertragsdokuments die Zahlung des Kaufpreises über 22.600 Euro in drei Raten (2 x 10.000 Euro, 1 x 2.600 Euro) auf das Konto der [redacted] Bank mit o.g. Kontonummer. Zum Nachweis ihrer Zahlung schickte die Klägerin an die E-Mail Adresse des Zeugen [redacted] drei Buchungsbelege. Bei Absendung durch die Klägerin wiesen diese die Bankverbindung bei der [redacted] Bank aus (Anlagen K2 bis K4 Bl. 21-23 d.A.), wohingegen sie bei der Beklagten eingehend die richtige Bankverbindung bei der [redacted] auswiesen (Anlage K8, Bl. 27-29 d.A.).

Die PDF-Anhänge der E-Mails wurden unverschlüsselt versandt. Seitens der Beklagten gibt es mit Ausnahme einer 2-Faktor-Identifizierung beim Einloggen in Outlook keine Verschlüsselungs-Mechanismen beim Versand von E-Mails.

Die Falschüberweisung der Klägerin blieb zunächst unbemerkt und fiel erst Wochen später auf. Ein Überweisungsrückruf der Klägerin scheiterte.

Die Klägerin behauptet, dass es zu einer Kompromittierung des E-Mail Servers der Beklagten gekommen sei und beruft sich auf ein Privat-Gutachten der [redacted] (Anlage K14, Bl. 70 d.A.). Diese Kompromittierung sei möglich gewesen, weil die Beklagte keine hinreichenden Sicherheitsstandards beim Versand der E-Mails installiert habe.

Die Klägerin beantragt:

1. Die Beklagte zu verurteilen, an die Klägerin 22.600 Euro nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit Klageerhebung zu zahlen.

2. Die Beklagte zu verurteilen, vorgerichtliche Kosten in Höhe von 1.375.88 zu erstatten.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte bestreitet, dass ihr E-Mail-Server gehackt worden sei. Sie habe die Kundendaten durch eine Anti-Virus Software, eine Firewall und einen Passwortschutz hinreichend vor dem Zugriff unbefugter geschützt. Überdies sei eine Kompromittierung des E-Mail-Postfachs der Klägerin ebenso wahrscheinlich. Zudem habe die Klägerin selbst ihr obliegende Prüfpflichten verletzt. Die Fälschung des Vertragsdokuments hätte ihr bei Anwendung der gehörigen Sorgfalt auffallen müssen.

Wegen der weiteren Einzelheiten des Sach- und Streitstands wird auf die gewechselten Schriftsätze nebst Anlagen Bezug genommen.

Die Klage wurde den Beklagtenvertretern gegen Empfangsbekenntnis vom 30.04.2024 (Bl. 52 f. d.A.) zugestellt.

Entscheidungsgründe:

A.

Die Klägerin hat einen Anspruch gegen die Beklagte auf Zahlung von 22.600 Euro aus Art. 82 Abs. 1 DSGVO.

Dass sich die Klägerin nicht ausdrücklich auf Art. 82 Abs. 1 DSGVO berufen hat, hindert das Gericht nicht an dessen Anwendung. Die Klägerin hat alle erforderlichen Voraussetzungen für diesen Schadensersatzanspruch vorgetragen. Die Subsumption dieses Sachverhalts unter das Gesetz obliegt allein dem Gericht.

I.

Der Anwendungsbereich der DSGVO ist vorliegend eröffnet.

Vom sachlichen Anwendungsbereich der DSGVO ist gem. Art. 2 Abs. 1 DSGVO die Verarbeitung personenbezogener Daten erfasst, wobei diese Begriffe in Art. 4 Nr. 1, Nr. 2 DSGVO legaldefiniert werden. Die in dem der E-Mail vom 12.12.2023 15:28 Uhr angehängten Vertragsdokument enthaltenen Angaben der Klägerin (Name, Anschrift, Kaufinteressentin) sind personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO. Diese beziehen sich auf eine natürliche Person, nämlich die Klägerin (anders in OLG Karlsruhe, Urteil vom 27.7.2023 – 19 U 83/22 –, MMR 2023, 761, wo ein B2B-Geschäft vorlag). Die Versendung der Rechnung mit den enthaltenen Daten per E-Mail an die Klägerin stellt eine Verarbeitung im Sine von Art. 4 Nr. 2 DSGVO in Form der Offenlegung durch Übermittlung, Verbreitung oder andere Form der Bereitstellung dar. Unerheblich ist hierbei, dass nicht die personenbezogenen Daten der Klägerin, sondern die Kontoverbindung der Beklagten durch einen unbekannten Dritten manipuliert wurde (OLG Schleswig, Urt. v. 18.12.2024 – 12 U 9/24 –, BeckRS 2024, 39951, Rn. 58). Ohne den gleichzeitigen unbefugten Zugriff auf die Daten der Klägerin wäre diese durch die abgewandelte, an die E-Mail vom 12.12.2023 15:36 Uhr angehängte Rechnung nicht dazu veranlasst worden, den Kaufpreis von 22.600 Euro auf ein falsches Bankkonto zu überweisen.

Zudem ist die Klägerin als natürliche Person, der wegen eines Verstoßes gegen die DSGVO ein Schaden entstanden ist, aktivlegitimiert. Die Beklagte ist als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO passivlegitimiert.

II.

Der Klägerin steht ein Schadensersatzanspruch aus Art. 82 Abs. 1 DSGVO gegen die Beklagte zu, da die Beklagte personenbezogene Daten der Klägerin unter schuldhaftem Verstoß gegen die Bestimmungen der DSGVO verarbeitet hat (1.), der Klägerin hierdurch ein Schaden entstanden ist (2.) und ein Kausalzusammenhang zwischen der rechtswidrigen Verarbeitung und diesem Schaden besteht (3.).

1.

Die Beklagte hat bei der Verarbeitung der personenbezogenen Daten der Klägerin schuldhaft gegen Bestimmungen der DSGVO verstoßen.

a.

Vorliegend liegt ein Verstoß der Beklagten gegen die Grundsätze der Art. 5, 24 und 32 DSGVO vor. Nach diesen Normen trifft den Verantwortlichen die Pflicht, geeignete technische und organisatorische Maßnahmen zu schaffen, um für die verarbeiteten personenbezogenen Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Verantwortliche hat die Möglichkeit, aber auch die Verpflichtung, nach dem in Art. 5 Abs. 2 DSGVO formulierten und in Art. 24 DSGVO konkretisierten Grundsatz seiner Rechenschaftspflicht darzulegen und zu beweisen, dass die von ihm getroffenen Sicherheitsmaßnahmen geeignet waren, um die personenbezogenen Daten entsprechend dem von der DSGVO verlangten Sicherheitsniveau vor dem Zugriff Unbefugter zu schützen (vgl. EuGH, Urt. v. 25.01.2024 – C-687/21, NZA 2024, 320, Rn. 40 ff; ebenso EuGH, Urt. v. 14.12.2023 – C-340/21 –, NJW 2024, 1091, Rn. 48 ff., 57).

Dies ist der Beklagten vorliegend nicht gelungen. Die Beklagte hat vorgetragen, dass sie über ein Antivirus Programm, eine Firewall sowie eine Passwortsicherung und 2-Faktor-Identifizierung ihres Outlook-Accounts verfügt. Eine irgendwie geartete Verschlüsselung ihrer E-Mails (Transport- oder End-to-End-Verschlüsselung) wurde von der Beklagten nicht

behauptet. Auch der Zeuge [redacted], der vom Geschäftsführer der Beklagten als deren IT-Fachmann ausgewiesen wurde, bestätigte, dass es seinen Kenntnissen zufolge keine Verschlüsselung beim Versand der geschäftlichen E-Mails der Beklagten gäbe.

Die Sicherheitsvorkehrungen der Beklagten sind nicht ausreichend und mithin nicht „geeignet" im Sinne der Art. 24, 32 DSGVO, um die personenbezogenen Daten von Kunden vor dem unbefugten Zugriff Dritter zu schützen.

In Art. 32 Abs. 1 lit. a) DSGVO wird als geeignete Maßnahme die Pseudonymisierung und Verschlüsselung personenbezogener Daten aufgezählt. Die Verschlüsselung wird in der DSGVO indes nicht zwingend vorgeschrieben, was das Gericht bei seiner Entscheidung nicht verkannt hat.

Der EuGH hat die Anforderungen des Art. 32 DSGVO dahingehend ausgelegt, dass die Geeignetheit der vom Verantwortlichen nach diesem Artikel getroffenen technischen und organisatorischen Maßnahmen von den nationalen Gerichten konkret zu beurteilen ist. Hierbei sind die mit der betreffenden Verarbeitung verbundenen Risiken zu berücksichtigen und es ist zu beurteilen, ob Art, Inhalt und Umsetzung dieser Maßnahmen diesen Risiken angemessen sind (EuGH, Urteil v. 14.12.2023 – C-340/21 –, NJW 2024, 1091 Rn. 40 ff., 47).

Zur Bestimmung der geeigneten Maßnahmen beim Versand von E-Mails im geschäftlichen Verkehr kann die „Orientierungshilfe des Arbeitskreises technische und organisatorische Datenschutzfragen vom 27.05.2021", die von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder entwickelt wurde und die Konkretisierung der Vorgaben des Art. 5 Abs. 1 lit. f), Art. 25 und Art. 32 Abs. 1 DSGVO zum Ziel hat, herangezogen werden. Nach dieser ist der Einsatz von Transportverschlüsselung beim Versand von E-Mails ein „Basis-Schutz" und stellt eine „Mindestmaßnahme" zur Erfüllung der gesetzlichen Anforderungen dar. Nach 4.2.1 der Orientierungshilfe soll eine Transportverschlüsselung beim Versand von E-Mail-Nachrichten dann ausreichen, wenn ein Bruch der Vertraulichkeit ein „normales" Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt. Bei einem hohen Risiko (welches vom OLG Schleswig, a.a.O. für den Versand einer Werklohnrechnung über ca. 15.000 Euro per E-Mail angenommen wurde) wird in 4.2.2 der Orientierungshilfe eine Ende-zu-Ende-Verschlüsselung sowie eine qualifizierte Transportverschlüsselung vorausgesetzt.

Die Frage, ob vorliegend ein normales oder ein hohes Risiko für die Rechte der Klägerin vorgelegen hat, kann vorliegend dahinstehen, da die Beklagte nicht einmal das geringere Schutzniveau der Transportverschlüsselung umgesetzt hat, sondern ihre E-Mail an die Klägerin ohne jegliche Verschlüsselung versandt hat. Für einen Geschäftsbetrieb wie den der Beklagten ist es absolut ungeeignet im Sinne der DSGVO, geschäftliche Daten völlig ohne jede Verschlüsselung zu versenden. Die Maßnahmen der Implementierung einer Firewall, eines Anti-Viren-Programms und der Passwortverschlüsselung des Outlook-Accounts entfalten keinerlei Schutzwirkungen gegenüber dem Versand geschäftlicher E-Mails und scheiden von vornherein als geeignete Maßnahmen zum Schutz personenbezogener Daten im E-Mail-Verkehr aus (vgl. OLG Schleswig, a.a.O. Rn. 71).

b.

Die Beklagte handelte auch schuldhaft.

Der Rechtsprechung des Europäischen Gerichtshofs folgend sieht Art. 82 DSGVO Artikel ein Haftungsregime für Verschulden vor, bei dem die Beweislast nicht beim Geschädigten liegt,

sondern beim Verantwortlichen (EuGH, Urt. v. 21.12.2023 – C-667/21, ZD 2024, 146 Rn. 92 ff.). Dies folgt aus Art. 83 Abs. 3 DSGVO, wonach der Verantwortliche von der Haftung nur dann befreit wird, wenn er in keinerlei Hinsicht für den schadensverursachenden Umstand verantwortlich ist. Das Verschulden wird nach dieser Norm grds. vermutet. Um die Feststellung treffen zu können, dass der Verantwortliche „in keinerlei Hinsicht“ verantwortlich sei, muss dieser nachweisen, dass er alle Sorgfaltspflichten erfüllt hat und ihm nicht die geringste Fahrlässigkeit vorgeworfen werden kann (OLG Schleswig, Urt. v. 18.12.2024 – 12 U 9/24 –, BeckRS 2024, 39951, Rn. 80; Quaas, in: Wolff/Brink, BeckOK Datenschutzrecht, 50. Ed, 01.08.2024, Art. 82 DSGVO Rn. 17).

Diesen Nachweis hat die Beklagte nicht geführt. Ihr ist der Vorwurf eines unzureichenden Schutzniveaus für den Versand von PDF-Dokumenten per E-Mail mit personenbezogenen Daten zu machen. Insoweit kann auf die obige Darstellung vollumfänglich verwiesen werden.

2.

Der Klägerin ist ein Schaden über 22.600 Euro entstanden.

Durch diese Zahlung auf das Konto eines unbekannten Dritten trat keine Erfüllungswirkung gem. § 362 Abs. 2 BGB gegenüber der Beklagten ein (OLG Schleswig, a.a.O., Rn. 50; OLG Karlsruhe, Urt. v. 27.07.2023 – 19 U 83/22 – MMR 2023, 761). Der Rückforderungsanspruch der Klägerin gegen den Empfänger Ihrer Zahlung ist nicht realisierbar, da der Anspruchsgegner nicht ermittelbar ist. Nach allgemeiner Lebenserfahrung wird das unberechtigt erlangte Geld von den Dritten zeitnah nach dessen Eingang auf ein anderes Konto im Ausland verschafft und dem Zugriff der deutschen Behörden entzogen bzw. dieser erschwert. Dies wird durch das bislang erfolglose Ermittlungsverfahren bestätigt, welches offensichtlich bislang nicht zur Ermittlung der Täter geführt hat.

3.

Dieser der Klägerin entstandene Schaden stellt auch eine kausale Folge des Verstoßes gegen die DSGVO dar.

Da nach den obigen Darlegungen die Beklagte bei Versand ihrer E-Mail mit dem angehängten Vertragsdokument kein ausreichendes Schutzniveau zur Sicherung der personenbezogenen Daten der Klägerin eingehalten hat, obliegt der Beklagten der Beweis dafür, dass der der Klägerin entstandene Schaden nicht durch ihr Fehlverhalten entstanden ist (EuGH, Urteil v. 14.12.2023 – C-340/21 –, NJW 2024, 1091 Rn. 72). Dies ist ihr vorliegend nicht gelungen.

Seitens der Beklagten wird keine Verschlüsselung der PDF-Dateien bzw. der E-Mail als solcher eingesetzt. Hierdurch besteht kein Schutz vor dem Zugriff Unbefugter auf das Computersystem der Beklagten oder deren Server. Ferner ist damit auch während des Transports der E-Mail vom Verantwortungsbereich der Beklagten hin zum Empfangsbereich der Klägerin ein Angriff durch Hacker möglich.

Einen Beweis dafür, dass der Zugriff im streitgegenständlichen Fall nicht im Bereich der Beklagten, sondern erst im Bereich der Klägerin erfolgt ist, hat die Beklagte nicht angeboten. Die Beklagte ist dem substantiierten und durch ein Privatgutachten untermauertem Vortrag der Klägerin, wonach die Kompromittierung im Machtbereich der Beklagten erfolgt sein muss, nicht einmal in erheblicher Weise entgegengetreten. Mit nachgelassenem Schriftsatz vom 20.01.2025 (Bl. 140 f. d.A.) hat die Beklagte lediglich vorgetragen, dass sie sich zu dem Gutachten nicht erklären könne und dies auch nicht müsse.

Im Übrigen ist der Beklagten – sollte der unbefugte Zugriff tatsächlich im Bereich der Klägerin und nicht schon im Bereich der Beklagten erfolgt sein – anzulasten, dass sie einen solchen Zugriff durch den von ihr gewählten Versand der Daten per E-Mail ohne jegliche Verschlüsselung erst ermöglicht hätte. Hätte die Beklagte sich der End-to-End-Verschlüsselung bedient wäre die E-Mail auch auf dem Server / Computer der Klägerin ganz wesentlich geschützt gewesen (OLG Schleswig, a.a.O., Rn. 86).

4.

Der Anspruch ist nicht infolge eines Mitverschuldens der Klägerin an der Schadensentstehung zu kürzen, § 254 BGB.

Der Klägerin oblag keine Überprüfung des ihr mit E-Mail vom 12.12.2023 15:36 Uhr übersandten Kaufvertrags auf dessen Richtigkeit. Zum einen hatte die Klägerin entsprechend der Aufforderung in dieser E-Mail die ihr zuvor von der Beklagten übersandte E-Mail gelöscht, weshalb ihr kein Vergleichsdokument vorlag. Zum anderen sind die Manipulationen im Vertragsdokument nicht in einer Art offensichtlich, die es als schuldhaft erscheinen ließen, diese nicht zu erkennen. Auch die Tatsache, dass es sich nicht um eine [redacted]Bankverbindung handelt, führt nicht zu einer Erkundigungsobliegenheit der Klägerin. Im Geschäftsverkehr ist es nicht unüblich, dass Unternehmen sich auch internationaler Banken bedienen, zumal es sich bei der[redacted] Bank um eine [redacted]Bank handelt.

B.

Gem. Art. 82 Abs. 1, Abs. 2 DSGVO steht der Klägerin gegen die Beklagte auch ein Schadensersatzanspruch auf Zahlung vorgerichtlicher Rechtsanwaltskosten über 1.375,88 Euro zu.

Der autonome Schadensbegriffs des Unionsrechts, der von den nationalen Gerichten zu beachten ist (BVerfG NJW 2001, 1267 (1268)), ist nach dem Erwägungsgrund 146 S. 3 weit auszulegen. Nach den Erwägungsgründen 75 und 85 sind finanzielle Verluste oder andere erhebliche wirtschaftliche Nachteile auszugleichen. (Quaas, in: BeckOK Datenschutzrecht, Art. 82 Rn. 23 ff.). Die vorgerichtlichen Rechtsanwaltskosten sind von diesem Schadensbegriff umfasst und sind durch die Beklagte gem. Art. 82 Abs. 1, Abs. 2 DSGVO zu erstatten.

C.

Der nicht nachgelassene Schriftsatz der Klägervertreter vom 24.01.2025 und 05.02.2025 geben keinen Anlass die mündliche Verhandlung gem. § 156 ZPO wiederzueröffnen.

Im Schriftsatz vom 24.01.2025 werden keine neuen Tatsachen mitgeteilt. Vielmehr erschöpft sich der Schriftsatz darin, die Bedeutung des Gutachtens, welches bereits Gegenstand der mündlichen Verhandlung geworden war und zu welchem die Beklagte rechtliches Gehör erhalten hat, hervorzuheben sowie die Rechtsauffassung der Klägerin, dass die IT-Systeme der Beklagten nicht hinreichend gegen Zugriffe Dritter geschützt seien, zu wiederholen.

Im Schriftsatz vom 05.02.2025 wurde lediglich eine bereits veröffentlichte Gerichtsentscheidung des OLG Schleswig und die Rechtsauffassung der Klägerin, dass diese zutreffend sei, mitgeteilt. Rechtsansichten können zu jedem Zeitpunkt des Verfahrens, auch nach Schluss der mündlichen Verhandlung vorgetragen werden. Dies gebietet aber keine Wiedereröffnung der mündlichen Verhandlung-

D.

Die Kostenentscheidung folgt aus § 91 Abs. 1 ZPO.

Die Entscheidung zur vorläufigen Vollstreckbarkeit beruht auf § 709 S. 1, S. 2 ZPO.

[redacted]
[redacted]am Landgericht