

Gericht:	Schleswig-Holsteinisches Oberlandesgericht 12. Zivilsenat
Entscheidungsdatum:	18.12.2024
Aktenzeichen:	12 U 9/24
ECLI:	ECLI:DE:OLGSH:2024:1218.12U9.24.00
Dokumenttyp:	Urteil
Quelle:	
Normen:	§ 242 BGB, § 254 BGB, § 280 Abs 1 BGB, § 362 Abs 2 BGB, § 631 BGB ... mehr

Sicherheitsvorkehrungen beim Versand von Emails mit angehängten Rechnungen im Geschäftsverkehr; Schadensersatzanspruch nach der Datenschutzgrundverordnung

Leitsatz

1. Die Zahlung eines Schlussrechnungsbetrags aus einer Werklohnrechnung durch einen privaten Kunden nicht auf das Konto des Werkunternehmers, sondern auf das Konto eines unbekannten Dritten, nachdem die vom Werkunternehmer per Email versandte Rechnung unbefugt verändert worden ist, führt nicht zur Erfüllung der Zahlungsverpflichtung im Sinne von § 362 Abs. 2 BGB.(Rn.52) (Rn.53)
2. Dem Kunden kann allerdings ein Schadensersatzanspruch in Höhe der auf das Drittkonto getätigten Überweisung zustehen, den er der Klagforderung des Werkunternehmers unter dem Gesichtspunkt der dolo-agit-Einwendung gemäß § 242 BGB entgegenhalten kann.(Rn.55)
3. Ein solcher Schadensersatzanspruch kann aus Art. 82 DSGVO resultieren.(Rn.56)
4. Art. 82 Abs. 2 DSGVO - der die in Art. 82 Abs. 1 DSGVO grundsätzlich normierte Haftungsregelung präzisiert - hat drei Voraussetzungen für die Entstehung eines Schadensersatzanspruchs, nämlich(Rn.64)
 - erstens eine Verarbeitung personenbezogener Daten im Sinne der Art. 5 Abs. 1 lit. a Var. 1, Art. 6 Abs. 1 UnterAbs. 1 lit. a, Art. 7 in Verbindung mit Art. 4 Nr. 1 und 2 DSGVO unter schuldhaftem Verstoß gegen die Bestimmungen der DSGVO,(Rn.65)
 - zweitens einen der betroffenen Person entstandenen Schaden und(Rn.66)
 - drittens einen Kausalzusammenhang zwischen der rechtswidrigen Verarbeitung und diesem Schaden (vgl. EuGH, Urteil vom 25. Januar 2024 - C-687/21, juris Rn. 58; EuGH, Urteil vom 04. Mai 2023 - C-300/21, juris Rn. 36).(Rn.67)
5. Ein Verstoß gegen die Vorschriften der Datenschutzgrundverordnung durch den Verantwortlichen kann in diesem Zusammenhang nicht schon allein deswegen angenommen werden, weil ein unbefugter Zugriff auf personenbezogene Daten durch Dritte im Sinne von Art. 4 Nr. 10 DSGVO stattgefunden hat (vgl. EuGH, Urteil vom 25. Januar 2024 - C-687/21, juris Rn. 45; EuGH, Urteil vom 14. Dezember 2023 - C-340/21, juris Rn. 22ff., 31-39).(Rn.70)
6. Umgekehrt ist nach der Rechtsprechung des Europäischen Gerichtshofs der Verantwortliche aber auch nicht gem. Art. 82 Abs. 3 DSGVO von seiner nach Art. 82 Abs. 1 und 2 DSGVO

bestehenden Pflicht zum Ersatz des einer Person entstandenen Schadens allein deswegen befreit, weil dieser Schaden die Folge eines unbefugten Zugangs zu personenbezogenen Daten durch einen Dritten ist (vgl. EuGH, Urteil vom 14. Dezember 2023 - C-340/21, juris Rn. 65ff., 74).(Rn.71)

7. Vielmehr hat der Verantwortliche 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 Datenschutzgrundverordnung verlangten Sicherheitsniveau vor dem Zugriff Unbefugter zu schützen (vgl. EuGH, Urteil vom 25. Januar 2024 - C-687/21, juris Rn. 40ff; ebenso EuGH, Urteil vom 14. Dezember 2023 - C-340/21, juris Rn. 48ff., 57).(Rn.72)

8. Der Europäische Gerichtshof hat die Anforderungen des Art. 32 DSGVO dahingehend ausgelegt, dass die Geeignetheit der vom Verantwortlichen nach diesem Artikel getroffenen technischen und organisatorischen Maßnahmen vor den nationalen Gerichten konkret zu beurteilen ist, wobei die mit der betreffenden Verarbeitung verbunden Risiken zu berücksichtigen sind und zu beurteilen ist, ob Art, Inhalt und Umsetzung dieser Maßnahmen diesen Risiken angemessen sind (vgl. EuGH, Urteil vom 14. Dezember 2023 - C-340/21, juris Rn. 40ff., 47).(Rn.77)

9. Nach Ansicht des Senats ist danach eine reine Transportverschlüsselung beim Versand von geschäftlichen Emails mit personenbezogenen Daten zwischen Unternehmer und Kunden jedenfalls bei dem hier bestehenden hohen finanziellen Risiko durch Verfälschung der angehängten Rechnung der Klägerin für den Kunden nicht ausreichend und kann keinen „geeigneten“ Schutz im Sinne der DSGVO darstellen. Vielmehr ist die End-to-End-Verschlüsselung zurzeit das Mittel der Wahl.(Rn.90)

10. Gemäß Art. 82 Abs. 3 DSGVO wird der Verantwortliche von der Haftung befreit, wenn er in keinerlei Hinsicht für den schadensverursachenden Umstand verantwortlich ist. Verantwortung ist dabei das Verschulden im Sinne der deutschen Rechtsterminologie und nicht die datenschutzrechtliche Verantwortung (LG Mainz, Urteil vom 12. November 2021 - 3 O 12/20, juris Rn. 73; Quaas, in: Wolff/Brink, BeckOK Datenschutzrecht, 50. Edition, Stand 01.08.2024, Art. 82 DSGVO Rn. 17 und 17.2; Geissler/Ströbel, in: NJW 2019, 3414 (3415)). Das Verschulden wird nach dem Wortlaut der Norm grundsätzlich vermutet.(Rn.96)

11. Ist bei dem Versand von geschäftlichen Emails kein ausreichendes Schutzniveau zur Sicherung der personenbezogenen Daten des Kunden eingehalten, obliegt dem Verantwortlichen der Beweis dafür, dass der dem Kunden entstandene Schaden nicht durch sein Fehlverhalten entstanden ist (EuGH, Urteil vom 14. Dezember 2023 - C-340/21, juris Rn. 72).(Rn.100)

12. Ein Mitverschulden des Kunden iSv § 254 BGB kann aus Abweichungen der Email - hier einer angehängten Rechnung - von früheren Rechnungen resultieren und obliegt einer Prüfung im Einzelfall.(Rn.104)

Verfahrensgang

vorgehend LG Kiel 9. Zivilkammer, 29. Dezember 2023, 9 O 110/23

Tenor

Auf die Berufung der Beklagten wird das Urteil des Landgerichts Kiel vom 29.12.2023, Az. 9 O 110/23, abgeändert. Die Klage wird abgewiesen.

Die Klägerin hat die Kosten des Rechtsstreits einschließlich der Kosten des Streithelfers zu tragen.

Das Urteil ist vorläufig vollstreckbar.

Die Revision gegen dieses Urteil wird zugelassen.

Gründe

I.

- 1 Die Parteien streiten darüber, ob die Klägerin (erneut) die Zahlung ihrer Werklohnforderung durch die Beklagte verlangen kann, nachdem der Überweisungsbetrag nach Manipulation der Rechnung durch kriminell handelnde Dritte dem Konto eines Unbekannten gutgeschrieben wurde.
- 2 Hinsichtlich des weiteren Sachverhalts wird Bezug genommen auf den Tatbestand des landgerichtlichen Urteils.
- 3 Das Landgericht hat der Klage stattgegeben.
- 4 Der Klägerin stehe gegen die Beklagte ein Anspruch auf Zahlung der ausstehenden Vergütung in Höhe von 15.385,78 € zu.
- 5 Zwischen den Parteien sei unstreitig, dass sie einen Werkvertrag i.S.d. § 631 BGB in Form eines Bauvertrags abgeschlossen hätten, die Klägerin ihre vertraglich geschuldeten Werkleistungen erbracht habe und infolge getätigter Abschlagszahlungen gem. § 641 Abs.1 S.1 BGB noch eine von der Beklagten geschuldete Vergütung in Höhe von 15.385,78 € nach Stellung einer Schlussrechnung am 26.09.2022 sowie durch Abnahme des Werkes am 12.01.2023 fällig gewesen sei.
- 6 Unstreitig sei ebenso, dass seitens der Beklagten in Bezug auf jene Schlussrechnung eine skontogeminderte Zahlung in Höhe von 14.924,20 € auf das Konto eines Dritten erfolgt sei. Allerdings sei durch diese Zahlung der Anspruch der Klägerin auf verbleibende Vergütung ihrer Leistung nicht gem. § 362 BGB erloschen.
- 7 Der zur Erfüllung erforderliche Leistungserfolg sei bei einer Überweisung erzielt, wenn der Gläubiger – vorliegend also die Klägerin – den geschuldeten Betrag endgültig zur freien Verfügung erhalte, mithin bei einer Gutschrift auf dem Konto des Gläubigers (vgl. BGH, Urteil vom 28.10.1998, VIII ZR 157/97 = NJW 1999, 210 f.). Da es sich bei dem Konto, auf das die Beklagte die Leistungsvergütung überwiesen habe, um das Konto eines Dritten und nicht der Klägerin gehandelt habe, sei der geschuldete Leistungserfolg nicht eingetreten. Eine Erfüllung durch Leistung an einen Dritten gem. § 362 Abs. 2 BGB sei durch die Zahlung der Beklagten auf das Konto aus der manipulierten Abrechnung gleichermaßen nicht gegeben. Die Leistung an einen Dritten habe nur dann erfüllende Wirkung, wenn dieser vom Gläubiger rechtsgeschäftlich ermächtigt sei, die Leistung im eigenen Namen in Empfang zu nehmen oder der Gläubiger dem Schuldner nach §§ 362 Abs. 2, 185 BGB die Ermächtigung erteile, die Leistung an einen bzw. jenen Dritten zu erbringen. Allein dass der Schuldner den Nichtberechtigten gutgläubig für empfangsbe-

rechtigt halte, bewirke – sofern keine gesetzlichen Sonderregelungen bestünden – kein Freiwerden des Schuldners. Vielmehr trete Erfüllungswirkung in einem solchen Fall erst dann ein, wenn der nicht empfangsbefugte Dritte die Leistung entsprechend den Weisungen des Schuldners an den Gläubiger weiterleite oder der Gläubiger die Leistungserbringung an den Dritten ausdrücklich oder schlüssig genehmige.

- 8 Vorliegend seien entsprechende Voraussetzungen nicht gegeben, da zwischen den Parteien unstreitig sei, dass die Manipulation der in Frage stehenden Abrechnung die Handlung eines deliktisch vorgehenden Dritten darstelle. Die in der manipulierten Rechnung enthaltene Angabe über das X-Bankkonto stelle keine Ermächtigung der Klägerin dar. Eine nachträgliche Genehmigung durch die Klägerin oder eine Weiterleitung der 14.924,20 € durch den Dritten seien nicht erfolgt und ein gesetzlich geregelter Sonderfall sei ebenfalls nicht ersichtlich.
- 9 Die Beklagte habe gegen die Klägerin auch keinen Schadensersatzanspruch wegen Verletzung einer Nebenpflicht gem. §§ 280 Abs. 1, 241 Abs. 2 BGB in der auf das Drittkonto getätigten Überweisungshöhe von 14.924,20 €, den sie der Klageforderung als dolo-agit-Einwendung gem. § 242 BGB entgegenhalten könnte.
- 10 Der Umstand, dass eine Manipulation der in Frage stehenden Rechnung durch einen Dritten vorgenommen worden sei, begründe keine Nebenpflichtverletzung der Klägerin aus ihrem Werkvertrag mit der Beklagten.
- 11 Konkrete gesetzliche Vorgaben für Sicherheitsvorkehrungen beim Versand von E-Mails im geschäftlichen Verkehr gebe es bisher nicht. Eine Konkretisierung könne jedoch anhand der Art. 5 Abs. 1 lit. f, 25 und 32 Abs. 1 DSGVO unternommen werden.
- 12 Auch wenn die Darlegungs- und Beweislast für das Vorliegen einer Pflichtverletzung sowie ihrer Kausalität für den eingetretenen Schaden nach § 280 Abs. 1 BGB grundsätzlich bei der Beklagten liege, habe die Klägerin vorliegend substantiiert vorgetragen, ausreichende Mindestschutzmaßnahmen in Form von SMTP (Simple Mail Transfer Protocol) über TLS (Transport Layer Security) beim E-Mail-Verkehr mit Vertragspartnern vorgenommen zu haben. Da es sich nach Vortrag der Parteien um die erste Rechnungsmanipulation im Rahmen der unternehmerischen Tätigkeit der Klägerin oder auf Seiten der Beklagten handele, sei ein erhöhtes Risiko, welches die Klägerin zu besonderen Schutzmaßnahmen verpflichten würde, mit Blick auf den Einzelfall nicht ersichtlich.
- 13 Selbst wenn man dem entgegen eine Nebenpflichtverletzung der Klägerin annehmen würde, fehle es weiterhin am Nachweis der Kausalität dieser Pflichtverletzung für den eingetretenen Schaden der Beklagten. Nach dem übereinstimmenden Vortrag der Parteien habe bisher nicht abschließend geklärt werden können, wie es tatsächlich dazu gekommen sei, dass die manipulierte Rechnung die Beklagte erreicht habe. Für eine kausale Pflichtverletzung der Klägerin sei entsprechend auch kein Beweis des ersten Anscheins gegeben.
- 14 Zudem wäre ein unterstellter Schadensersatzanspruch der Beklagten nach § 254 BGB erheblich zu kürzen, weil ein Mitverschulden zu berücksichtigen wäre.
- 15 Die Klägerin habe gem. §§ 280 Abs. 2, 286 Abs. 3 BGB vorgerichtliche Anwaltskosten für das Mahnschreiben vom 15.02.2023 in Höhe von 953,40 € geltend machen können.

Der von der Klägerin geltend gemachte Zinsanspruch ergebe sich aus §§ 286 Abs. 1, 288 Abs. 1 BGB.

- 16 Gegen dieses Urteil hat die Beklagte Berufung eingelegt.
- 17 Das angefochtene Urteil sei rechtsfehlerhaft. Die Klägerin habe gegen die Beklagte keinen Anspruch auf Zahlung eines Betrages in Höhe von brutto 15.385,78 €.
- 18 Die Angabe einer neuen Bankverbindung in der Rechnung vom 26.09.2022 sei bei verständiger Würdigung aus Sicht des Erklärungsempfängers als konkludent erklärter Widerruf der Einverständniserklärung hinsichtlich des zuvor angegebenen Kontos auszulegen (§§ 133, 157 BGB). Die Mitteilung einer Bankverbindung in einer Rechnung lasse mangels anderer Anhaltspunkte keinen anderen Schluss zu, als dass das Einverständnis des Gläubigers mit einer Überweisung des Rechnungsbetrags sich auf die nunmehr angegebene Bankverbindung beschränke.
- 19 In Anbetracht der vorgenannten Rechtsprechung des BGH verkenne das Landgericht, dass die Beklagte auf Grund der Kontodaten aus der 3. Abschlagsrechnung nur auf das von der Klägerin angegebene Konto hätte zahlen können. Zum Zeitpunkt der Überweisung sei der Beklagten nicht bekannt gewesen, dass die Rechnung im Machtbereich der Klägerin manipuliert worden sei. Eine gesonderte Überprüfung der Bankverbindungsdaten habe weder der Beklagten noch dem streitverkündeten Zeugen A. obliegen.
- 20 Selbst wenn man zu dem Ergebnis komme, dass der Klägerin ein Anspruch auf Werklohn zustehe, habe die Beklagte gegen sie einen Schadensersatzanspruch gemäß §§ 280 Abs. 1, 241 Abs. 2 BGB in Höhe der auf das Drittkonto getätigten Überweisung des streitgegenständlichen Betrags, den die Beklagte der Klagforderung unter dem Gesichtspunkt der dolo-agit-Einwendung gemäß § 242 BGB entgegenhalten könne.
- 21 Die Klägerin habe vorliegend substantiiert vorgetragen, ausreichende Mindestschutzmaßnahmen in Form von SMTP über TLS beim E-Mail-Verkehr mit Vertragspartnern vorgenommen zu haben. Dieser Vortrag sei ausdrücklich im Termin zur mündlichen Verhandlung vom 29.11.2023 bestritten worden. Die seitens der Klägerin angebotenen Zeugen seien hierzu schlicht nicht angehört worden.
- 22 Weiter führe das Landgericht aus, dass es an einem Nachweis der Kausalität dieser Pflichtverletzung für den eingetretenen Schaden der Beklagten fehle. Auch dies sei unzutreffend. Das strafrechtliche Verfahren gegen Herrn B. wegen Abfangens von Daten, Betrug und Geldwäsche beim Amtsgericht Y. zum dortigen Az. xxx sei noch nicht abgeschlossen. Das Gericht führe aus, dass es naheliegen würde, dass die Manipulation in der Sphäre des Zeugen A. stattgefunden habe, welcher der Beklagten die Rechnung habe zukommen lassen und sein E-Mail-Konto nach der streitgegenständlichen Manipulation von xxx zu yyy gewechselt haben solle. Auch dieser Vortrag sei streitig.
- 23 Das Landgericht nehme diese Behauptung zum Anlass, eine Nebenpflichtverletzung der Klägerin zu verneinen. Dies sei rechtsfehlerhaft. Mit Schriftsatz vom 19.12.2023 sei vorgetragen worden, dass nach der Orientierungshilfe der DSK eine Transportverschlüsselung beim E-Mail-Versand von personenbezogenen Daten vorgesehen sei, wenn der Bruch der Vertraulichkeit ein Risiko für natürliche Personen darstellen könne. Gerade aufgrund der fehlenden Transportverschlüsselung habe in der Sphäre der Klägerin die

E-Mail manipuliert werden können. Dies sei unter Sachverständigenbeweis gestellt worden.

- 24 Schließlich führe das Landgericht aus, dass ein unterstellter Schadensersatzanspruch der Beklagten nach § 254 BGB erheblich zu kürzen wäre, da ein Mitverschulden zu berücksichtigen wäre. Das Gericht stelle darauf ab, dass optische Unterschiede und zahlreiche fehlende Elemente der manipulierten Rechnung von den zuvor erhaltenen Abschlagsrechnungen abwichen. Auch dies sei rechtsfehlerhaft.
- 25 Der auf Seiten der Beklagten beigetretene Streitverkündete A. wendet sich ebenfalls gegen das landgerichtliche Urteil.
- 26 Es sei festzustellen, dass die Vorinstanz in den Entscheidungsgründen teilweise schlicht unrichtige Tatsachen zugrunde gelegt habe und teilweise auch streitigen Sachvortrag als vermeintlich unstreitig eingeordnet und der dortigen Entscheidungsfindung zugrunde gelegt habe.
- 27 Entgegen der rechtlichen Bewertung und Würdigung der Vorinstanz stehe der Beklagten sehr wohl jedenfalls ein Schadensersatzanspruch wegen Verletzung einer Nebenpflicht gemäß §§ 280 Abs. 1, 241 Abs. 2 BGB zu. Dabei seien folgende Kriterien und Umstände zu berücksichtigen:
- 28 Mit dem beigefügten Schreiben per E-Mail vom 04.06.2024 habe der Streithelfer seinem Prozessbevollmächtigten mitgeteilt, dass er die Original-pdf der streitgegenständlichen Rechnung ausgelesen habe. Dabei habe der Streithelfer festgestellt, dass die pdf ohne jedwede Schutzfunktionen verschickt worden sei (Beweis: Zeugnis des Streithelfers; Sachverständigengutachten).
- 29 Die Klägerin sei es gewesen, die die Übertragungsmethode für die Versendung der Rechnung per E-Mail als pdf-Datei gewählt habe. Die hiermit verbundenen Risiken gingen dann allerdings vollständig zu ihren Lasten. Letzteres sei insbesondere dann der Fall, wenn die Klägerin selbst keinerlei Schutzvorkehrungen gegen nachträgliche Veränderungen, Manipulationen etc. an pdf-Dateien und von dem Account der Klägerin versandten E-Mails treffe.
- 30 Dabei spiele es auch keine Rolle, ob es sich vermeintlich um eine erste Manipulation von Schriftverkehr per E-Mail auf Seiten der Klägerin gehandelt habe oder nicht. Ohnehin werde eine derartige Behauptung der Klägerin mit Nichtwissen bestritten.
- 31 Entgegen den landgerichtlichen Ausführungen sei die dortige reine Mutmaßung, es liege nahe, dass die Manipulation in der Sphäre des Streithelfers stattgefunden habe, schlicht unrichtig. Es treffe nicht zu, dass der Streithelfer im Anschluss an den hier streitgegenständlichen Schadenfall seinen E-Mail-Account geändert habe (Beweis: Zeugnis des Streithelfers, Zeugnis des Rechtsanwalts Dr. Z.).
- 32 Entgegen den Ausführungen im angefochtenen Urteil sei vielmehr davon auszugehen, dass der streitgegenständliche Rechnungsversand per E-Mail bereits bei der Klägerin gehackt worden sei. Die E-Mail der Klägerin vom 27.09.2022 gemäß Anlage K 5 weise ausdrücklich den E-Mail-Account auf: xxx.
- 33 Soweit die Vorinstanz darauf abstelle, dass das Bestreiten der Beklagten mit Nichtwissen im Zusammenhang mit dem E-Mail-Account des Streithelfers unzulässig sei, sei auch die-

se rechtliche Bewertung nicht zutreffend. Das Vertragsverhältnis zwischen der Beklagten und dem Streithelfer sei zum Zeitpunkt des in der Vorinstanz anhängigen Rechtsstreits bereits beendet gewesen. Der Beklagten habe überhaupt kein Recht und keine Befugnis zugestanden, den Streithelfer nach irgendwelchen dortigen internen Sicherheitsvorkehrungen etc. zu befragen bzw. von dort aus entsprechende Auskünfte einzuholen.

- 34 Was den QR-Code angehe, sei dieser in der streitgegenständlichen Rechnung vom 26.09.2022 gemäß Anlage K 4 unten in der Mitte aufgeführt. Es treffe aber nicht zu, dass die Klägerin von diesem Zeitpunkt an durchgehend einen QR-Code in den Rechnungen verwendet habe. Außerdem unterstelle die Vorinstanz relativ schlank (aber fehlerhaft), dass die Beklagte bei der Eingabe der neuen Bankverbindung der manipulierten Rechnung den Kontowechsel hätte feststellen und hierauf aktiv reflektieren müssen. Bereits in erster Instanz hätten die Prozessbevollmächtigten der Beklagten den durch diese handschriftlich ausgefüllten Überweisungsbeleg vorgelegt. Insofern sei unstreitig, dass ein entsprechender und sicherlich üblicher Vorschlag für eine Kontoverbindung im Rahmen von Online-Überweisungen überhaupt nicht relevant sei. Und schließlich sei zu verweisen auf den Sachvortrag der Beklagten, wonach das Wasserzeichen auf der Kopie der Rechnung nicht erkennbar gewesen sei. Auch insoweit habe die Vorinstanz dieses Kriterium nicht ohne weitergehende Aufklärung zulasten der Beklagten bewerten dürfen.
- 35 Bislang sei offensichtlich noch nicht behandelt bzw. hinterfragt worden, mit welchem Begleitschreiben per E-Mail die Klägerin die „korrekte“ Rechnung gemäß Anlage K 4 per Email versandt habe. Es werde beantragt, der Klägerin aufzugeben, das Begleitschreiben per E-Mail vorzulegen, den Zeitpunkt der Versendung per E-Mail mitzuteilen und diejenige Person zu benennen, welche die E-Mail verfasst und den Versand der E-Mail veranlasst habe. Es werde davon ausgegangen, dass spätestens diese Daten und Informationen belegten, dass die Manipulation im Zusammenhang mit der Versendung der Rechnung gemäß Anlage K 4 einzig und allein in der Sphäre der Klägerin begründet sei.
- 36 Die Beklagte beantragt,
- 37 das Urteil des Landgerichts Hamburg vom 29.12.2023, Az. 9 O 110/23 abzuändern und die Klage abzuweisen.
- 38 Hilfsweise beantragt sie,
- 39 das Urteil aufzuheben und die Sache zur erneuten Verhandlung und Entscheidung an das Landgericht Kiel zurückzuverweisen.
- 40 Der Vertreter des beigetretenen Streitverkündeten A. stellt keinen Antrag.
- 41 Die Klägerin beantragt,
- 42 die Berufung zurückzuweisen.
- 43 Die Klägerin verteidigt das landgerichtliche Urteil.
- 44 Die Berufung der Beklagten sei unbegründet.
- 45 Der Anspruch der Klägerin sei nicht untergegangen. Die von der Beklagten getätigte Zahlung habe keine Erfüllungswirkung nach § 362 Abs. 1 BGB. Zwar könne eine Banküberweisung der Erfüllung dienen, dem Bankkonto der Klägerin sei jedoch kein dem Vergütungsanspruch entsprechender Betrag gutgeschrieben worden. Eine Erfüllung sei auch

nicht dadurch eingetreten, dass die Beklagte auf ein Bankkonto eines Dritten gezahlt habe. Die Klägerin habe weder einen Dritten dazu ermächtigt, die Geldzahlung im eigenen Namen in Empfang zu nehmen, noch die Beklagte ermächtigt, an einen Dritten zu zahlen.

- 46 Der Anspruch der Klägerin sei auch durchsetzbar. Die Beklagte könne der Klägerin einen Schadensersatzanspruch nicht entgegenhalten, der sich aufgrund der Grundsätze von Treu und Glauben auf den Vergütungsanspruch der Klägerin auswirken würde. Zum einen liege eine Pflichtverletzung der Klägerin nicht vor. Zum anderen treffe die Klägerin kein Verschulden. Die Beklagte sei für das Vorliegen der anspruchsbegründenden Voraussetzungen darlegungs- und beweisbelastet. Ein solcher Beweis sei ihr nicht gelungen.
- 47 Die Klägerin habe hinreichende Sicherheitsvorkehrungen für den Versand von E-Mails getroffen. Sie habe unmittelbar nach Kenntnis von dem Manipulationsvorwurf einen Fachmann, den Zeugen C., eingeschaltet, um das Computersystem der Firma zu überprüfen (Beweis: Zeugnis C.). Auch beim Provider D. hätten keine Probleme vorgelegen (Beweis: Sachverständigengutachten).
- 48 Auffällig sei hingegen, dass der Architekt der Beklagten, der Streitverkündete, unmittelbar nach Entdecken des Vorfalls seine ursprüngliche E-Mail-Adresse xxx in yyy geändert habe, womit auch ein Wechsel des Providers verbunden gewesen sei (Beweis: Zeugnis A.).
- 49 Im Übrigen sei das Landgericht nicht gehalten gewesen, den von der Beklagten angebotenen Sachverständigenbeweis über eine angeblich fehlende Transportverschlüsselung der E-Mail der Klägerin einzuholen. Die unterlassene Beweisaufnahme stelle keinen Verfahrensfehler dar. Die Behauptung der Beklagten sei ohne nähere Anhaltspunkte ins Blaue hinein erfolgt. Es liege mithin ein reiner Ausforschungsbeweis vor.

II.

- 50 Die zulässige Berufung ist begründet. Die Klägerin hat keinen Anspruch auf (erneute) Zahlung des vereinbarten Werklohns durch die Beklagte, ebenso wenig auf Zahlung außergerichtlicher Rechtsanwaltsgebühren.
- 51 1. Zwischen den Parteien ist unstreitig ein Werkvertrag i.S.d. § 631 BGB in Form eines Bauvertrages zustande gekommen. Die Klägerin hat ihre vertraglich geschuldeten Werkleistungen erbracht und infolge getätigter Abschlagszahlungen war gem. § 641 Abs.1 S.1 BGB noch eine Vergütung in Höhe von 15.385,78 € nach Stellung einer Schlussrechnung am 26.09.2022 von der Beklagten geschuldet, sowie nach Abnahme des Werkes am 12.01.2023 fällig.
- 52 Unstreitig ist ebenso, dass seitens der Beklagten in Bezug auf jene Schlussrechnung eine skonto-geminderte Zahlung in Höhe von 14.924,20 € auf das Konto eines Dritten erfolgt ist. Allerdings ist die Forderung der Klägerin dadurch nicht erfüllt im Sinne von § 362 Abs. 2 BGB. Insoweit folgt der Senat dem Landgericht.
- 53 Für die Erfüllungswirkung bei Zahlung an einen Dritten genügt es gerade nicht, dass der Schuldner nur gutgläubig meint, auf ein Konto des Gläubigers zu zahlen. Dies hat das Landgericht zu Recht betont. Die Leistung an einen Dritten hat vielmehr nur dann erfüllende Wirkung, wenn dieser tatsächlich vom Gläubiger rechtsgeschäftlich ermächtigt ist, die Leistung im eigenen Namen in Empfang zu nehmen oder der Gläubiger dem Schuld-

ner nach §§ 362 Abs. 2, 185 BGB die Ermächtigung erteilt, die Leistung an einen Dritten zu erbringen. Die Leistung an einen nichtberechtigten Dritten - wie hier wegen der Manipulation der Kontodaten - erlangt hingegen grundsätzlich erst dann erfüllende Wirkung, wenn der nicht empfangsbefugte Dritte die Leistung entsprechend den Weisungen des Schuldners an den Gläubiger weiterleitet oder der Gläubiger die Leistungserbringung an den Dritten ausdrücklich oder schlüssig genehmigt (vgl. OLG Karlsruhe, Urteil v. 27.07.2023 - 19 U 83/22, juris; auch BGH NJW 2023, 1287, 1288f. Rn. 29; Grüneberg/Grüneberg, BGB, 83. Aufl., § 362 Rn. 6). Diese Voraussetzungen sind vorliegend unstreitig nicht gegeben.

- 54 Auch in der von der Berufung zitierten Entscheidung des Bundesgerichtshofs (BGH, Urteil v. 17.03.2004 - VIII ZR 161/03, juris Rn 17) hat dieser keine Erfüllung angenommen. Er hat es lediglich als rechtsmissbräuchlich angesehen, dass die dortige Beklagte sich auf die fehlende Erfüllung beruft. Die dortige Klägerin musste sich insofern widersprüchliches Verhalten der dortigen Zedentin nach Treu und Glauben (§ 242 BGB) entgegenhalten lassen mit der Folge, dass sie sich so behandeln lassen musste, als habe sie die Verbuchung und Verrechnung des überwiesenen Betrags seitens der Streithelferin genehmigt (a.a.O. Rn. 19). Ein solcher Fall liegt hier nicht vor.
- 55 2. Anders als das Landgericht meint, steht der Beklagten allerdings ein Schadensersatzanspruch in Höhe der auf das Drittkonto getätigten Überweisung des streitgegenständlichen Betrags zu, den die Beklagte der Klagforderung unter dem Gesichtspunkt der dolo-agit-Einwendung gemäß § 242 BGB entgegenhalten kann.
- 56 a) Ein solcher Anspruch resultiert vorliegend jedenfalls aus Art. 82 DSGVO.
- 57 Die DSGVO verlangt von Unternehmen, sensible Daten gegen Datenschutzverletzungen zu sichern. Sensible Daten sind z.B. personenbezogene Daten, die übertragen, gespeichert oder anderweitig verarbeitet werden. Als Datenschutzverletzungen werden versehentliche oder unrechtmäßige Zerstörung, Verlust, Veränderung, unbefugte Offenlegung oder Zugriff auf personenbezogene Daten definiert. Um solche Sicherheitsvorfälle zu vermeiden, werden Unternehmen dazu angehalten, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die sichere Verarbeitung personenbezogener Daten zu gewährleisten. 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 Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter“. Art. 82 Abs. 1 DSGVO eröffnet einen direkten eigenen deliktischen Schadensersatzanspruch mit Verschuldensvermutung, wobei der Verantwortliche nach Abs. 3 den Entlastungsbeweis führen kann.
- 58 Dass die Beklagte sich nicht ausdrücklich auf Art. 82 Abs. 1 DSGVO berufen hat, hindert eine Anwendbarkeit nicht, denn die Subsumtion des unterbreiteten Sachverhalts obliegt allein dem Gericht. Insoweit hat die Beklagte alle erforderlichen Voraussetzungen für einen solchen Schadensersatzanspruch vorgetragen.
- 59 aa) Der Anwendungsbereich der DSGVO ist in zeitlicher, sachlicher und räumlicher Hinsicht eröffnet.
- 60 Gemäß Art. 2 Abs. 1 DSGVO gilt diese für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung perso-

nenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

- 61 Personenbezogene Daten sind Daten, über die sich ein konkreter Personenbezug herstellen lässt. Demnach geht es um Daten, die konkreten Personen zuzuordnen sind. Die in der streitgegenständlichen Email als Anhang enthaltenen Angaben zur Beklagten (Name, Anschrift, Kunde der Klägerin, offene Rechnung über eine Werkleistung) sind personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO. Die Versendung der Rechnung mit den enthaltenen Daten per E-Mail an die Beklagte über den streitverkündeten Zeugen A. stellt eine Verarbeitung im Sinne von Art. 4 Nr. 2 DSGVO dar ("Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung"). Daran ändert sich auch nichts dadurch, dass nicht die personenbezogenen Daten der Beklagten, sondern die Kontoverbindung der Klägerin durch einen Dritten unbefugt manipuliert wurde, denn ohne den gleichzeitigen unbefugten Zugriff auf die Daten der Beklagten wäre diese durch die abgewandelte, an die Email angehängte Rechnung nicht dazu veranlasst worden, auf ein falsches Bankkonto zu zahlen.
- 62 Das sog. Haushaltsprivileg des Art. 2 Abs. 2 lit. c DSGVO, wonach die DSGVO keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten findet, greift nicht, da die Verarbeitung vorliegend durch ein Unternehmen im Rahmen des geschäftlichen Betriebs stattgefunden hat.
- 63 Die Beklagte ist für den geltend gemachten Anspruch aktivlegitimiert. Denn anspruchsberechtigt ist nach Art. 82 Abs. 1 DSGVO jede Person, der wegen eines Verstoßes gegen die DSGVO ein Schaden entstanden ist. Die Klägerin ist als Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO passivlegitimiert im Sinne von Art. 82 Abs. 1 DSGVO.
- 64 bb) Im Übrigen hat Art. 82 Abs. 2 DSGVO - der die in Art. 82 Abs. 1 DSGVO grundsätzlich normierte Haftungsregelung präzisiert - drei Voraussetzungen für die Entstehung eines Schadensersatzanspruchs, nämlich
- 65 - erstens eine Verarbeitung personenbezogener Daten im Sinne der Art. 5 Abs. 1 lit. a Var. 1, Art. 6 Abs. 1 UnterAbs. 1 lit. a, Art. 7 in Verbindung mit Art. 4 Nr. 1 und 2 DSGVO unter schuldhaftem Verstoß gegen die Bestimmungen der DSGVO,
- 66 - zweitens einen der betroffenen Person entstandenen Schaden und
- 67 - drittens einen Kausalzusammenhang zwischen der rechtswidrigen Verarbeitung und diesem Schaden
- 68 (vgl. EuGH, Urteil v. 25.01.2024 - C-687/21, juris Rn. 58; EuGH, Urteil v. 04.05.2023 - C-300/21 -, juris Rn. 36).
- 69 (1) Vorliegend hat nach Ansicht des Senats die Klägerin - anders als das Landgericht meint - im Zuge der Verarbeitung der personenbezogenen Daten der Beklagten bei Versand der streitgegenständlichen Email mit Anhang gegen die Grundsätze der Art. 5, 24 und 32 DSGVO verstoßen.
- 70 (aa) Ein Verstoß gegen die Vorschriften der Datenschutzgrundverordnung kann in diesem Zusammenhang nicht schon allein deswegen angenommen werden, weil - was unstrittig ist - ein unbefugter Zugriff auf personenbezogene Daten durch Dritte im Sinne

von Art. 4 Nr. 10 DSGVO stattgefunden hat. Denn dies allein reicht nach der Rechtsprechung des Europäischen Gerichtshofs nicht aus, um gleichzeitig davon auszugehen, dass die technischen und organisatorischen Maßnahmen des für die Verarbeitung Verantwortlichen nicht "geeignet" im Sinne von Art. 24 und 32 DSGVO waren, vgl. EuGH, Urteil v. 25.01.2024 - C-687/21 -, juris Rn. 45; EuGH, Urteil v. 14.12.2023 - C-340/21, juris Rn. 22ff., 31-39).

- 71 (bb) Umgekehrt ist nach der Rechtsprechung des Europäischen Gerichtshofs der Verantwortliche aber auch nicht gem. Art. 82 Abs. 3 DSGVO von seiner nach Art. 82 Abs. 1 und 2 DSGVO bestehenden Pflicht zum Ersatz des einer Person entstandenen Schadens allein deswegen befreit, weil dieser Schaden die Folge eines unbefugten Zugangs zu personenbezogenen Daten durch einen Dritten ist (vgl. EuGH, Urteil v. 14.12.2023 - C-340/21, juris Rn. 65ff., 74).
- 72 (cc) Vielmehr hat der Verantwortliche 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 Datenschutzgrundverordnung verlangten Sicherheitsniveau vor dem Zugriff Unbefugter zu schützen (vgl. EuGH, Urteil v. 25.01.2024 - C-687/21, juris Rn. 40ff; ebenso EuGH, Urteil v. 14.12.2023 - C-340/21, juris Rn. 48ff., 57). Das ist der Klägerin vorliegend nicht gelungen, da der Senat die Transportverschlüsselung, die sie beim Versand der streitgegenständlichen Email – von der Beklagten bestritten – verwendet haben will (in Form von SMTP über TLS), nicht für ausreichend und damit auch nicht für „geeignet“ im Sinne der Datenschutzgrundverordnung hält. Es kann damit auch dahinstehen, ob eine solche Transportverschlüsselung tatsächlich erfolgt ist. Das von der Klägerin zum Beweis dafür und für die Frage, ob eine Transportverschlüsselung dem üblichen Sicherungsmaß entspricht oder sogar darüber hinausgeht, angebotene Sachverständigengutachten ist insoweit nicht einzuholen.
- 73 (aaa) Der Senat verkennt dabei nicht, dass es konkrete gesetzliche Anforderungen an eine Verschlüsselung von Emails nicht gibt.
- 74 Auch in der Datenschutzgrundverordnung ist eine Verschlüsselung nicht zwingend vorgeschrieben. Sie wird jedoch mehrfach im Text der Verordnung erwähnt, jedes Mal als Empfehlung. In Artikel 32 heißt es, dass unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie der Risiken und der Schwere der Folgen für die Rechte und Freiheiten natürlicher Personen der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen umsetzen müssen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, wozu unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten gehören. Da die DSGVO die Verschlüsselung jedoch nicht zwingend vorschreibt, bietet sie keine Klarheit darüber, wann die Verschlüsselung verwendet werden sollte und welche Standards dabei angewendet werden müssen.
- 75 Nach der „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, sind ausgehend vom Stand der Technik, den typischen Implementierungskosten und deren

Verhältnis zu den Risiken einer Übermittlung personenbezogener Daten per E-Mail Anforderungen an die Maßnahmen, die Verantwortliche und Auftragsverarbeiter zur ausreichenden Minderung der Risiken zu treffen haben, zu bestimmen. Die Verantwortlichen und Auftragsverarbeiter sind verpflichtet, die Besonderheiten ihrer Verarbeitungen, darunter insbesondere den Umfang, die Umstände und die Zwecke der vorgesehenen Übermittlungsvorgänge zu berücksichtigen, die ggf. in abweichenden Anforderungen resultieren können (vgl. https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschlueselung.pdf).

- 76 Danach muss es im Ausgangspunkt heute jedem Unternehmen, das Daten seiner privaten Kunden computertechnisch verarbeitet, bewusst sein, dass der Schutz dieser Daten hohe Priorität – auch beim Versenden von Emails – genießt. Es ist daher zur Überzeugung des Senats auch verpflichtet, diesen Schutz durch entsprechende Maßnahmen so weit wie möglich zu gewährleisten.
- 77 Der Europäische Gerichtshof hat die Anforderungen des Art. 32 DSGVO dahingehend ausgelegt, dass die Geeignetheit der vom Verantwortlichen nach diesem Artikel getroffenen technischen und organisatorischen Maßnahmen vor den nationalen Gerichten konkret zu beurteilen ist, wobei die mit der betreffenden Verarbeitung verbunden Risiken zu berücksichtigen sind und zu beurteilen ist, ob Art, Inhalt und Umsetzung dieser Maßnahmen diesen Risiken angemessen sind (vgl. EuGH, Urteil v. 14.12.2023 – C-340/21, juris Rn. 40ff., 47).
- 78 (bbb) Tastet man sich an die Frage einer „geeigneten“ Verschlüsselung „von unten“ heran, ist es nach Ansicht des Senats für einen Geschäftsbetrieb wie den der Klägerin ausgeschlossen, geschäftliche Emails mit personenbezogenen Daten völlig ohne jede Verschlüsselung zu versenden.
- 79 Nach einer Information des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu aktuell möglichen und gebräuchlichen Verschlüsselungsmethoden kommen für den Email-Versand die folgenden Verfahren in Betracht:
- 80 „Bei E-Mail-Verschlüsselung gibt es grundsätzlich zwei verschiedene Arten: die Punkt-zu-Punkt- beziehungsweise Transportverschlüsselung und die Ende-zu-Ende-Verschlüsselung.
- 81 Wo der entscheidende Unterschied liegt, wird im Folgenden erklärt:
- 82 Transportverschlüsselung
- 83 Bei der Transportverschlüsselung wird zwischen dem E-Mail-Programm (Client) und dem E-Mail-Server eine Verbindung aufgebaut und diese z.B. gemäß dem weit verbreiteten Protokoll "Transport Layer Security" (TLS) verschlüsselt. Dies wird inzwischen von den allermeisten E-Mail-Anbietern unterstützt. Alle Daten, die zwischen dem Client und dem E-Mail-Server ausgetauscht werden, sind damit während des Versands verschlüsselt. E-Mails werden beim Versand allerdings über unterschiedliche Knotenpunkte im Web zwischen den Servern der E-Mail-Anbieter zur Empfängerin oder dem Empfänger weitergeleitet und sind in diesen Punkten nicht verschlüsselt und dazwischen nicht immer. Sowohl beim E-Mail-Anbieter als auch an den Knotenpunkten des Versands liegt die E-Mail im Klartext vor.

- 84 Internetkriminelle könnten einen "Man-in-the-Middle-Angriff" durchführen, der auf diese Punkte ausgerichtet ist. Bei diesem Angriff platziert sich ein Angreifer "in der Mitte" der Kommunikation zwischen zwei Kommunikationspartnerinnen oder -partnern und kann ohne deren Wissen Daten (z.B. E-Mails) abfangen, kopieren oder verändern.
- 85 Ende-zu-Ende-Verschlüsselung
- 86 Im Unterschied zur Transportverschlüsselung werden bei der Ende-zu-Ende-Verschlüsselung nicht die einzelnen Abschnitte des Versandkanals verschlüsselt, sondern die E-Mails selbst. Nur Sender(in) und Empfänger(in) können die E-Mail im Klartext lesen, wenn sie über den notwendigen Schlüssel verfügen. Weder die beteiligten E-Mail-Anbieter können die E-Mail lesen, noch haben potentielle Angreifer die Möglichkeit, die E-Mails unterwegs zu lesen oder zu manipulieren. Damit erfüllt nur diese Technik die drei Ziele der Verschlüsselung im Internet: Vertraulichkeit, Authentizität, Integrität.
- 87 Zwar ist eine Transportverschlüsselung einer unverschlüsselten Kommunikation vorzuziehen, doch gerade bei sensiblen oder persönlichen Inhalten empfiehlt es sich, auf den Einsatz einer Ende-zu-Ende-Verschlüsselung Wert zu legen. Bisher gestaltete sich der Einsatz dieser Kryptografiertechnik noch als mühsam. Anwenderinnen und Anwender müssen bei der Ende-zu-Ende-Verschlüsselung oft selbst aktiv werden und zusätzliche Plugins in den meisten E-Mail-Clients aktivieren, um die Technologie nutzen zu können. Eine weitere Hürde ist der Austausch der öffentlichen Schlüssel. Allerdings ist dies unter anderem mit einem vom Bundesamt für Sicherheit in der Informationstechnik entwickelten Protokoll richtungsweisend vereinfacht und so Anwenderinnen und Anwendern zugänglicher gemacht worden.“
- 88 (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesst-kommunizieren/E-Mail-Verschlueselung/e-mail-verschlueselung_node.html)
- 89 In der bereits zitierten Orientierungshilfe der Datenschutzkonferenz (vgl. https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschlueselung.pdf) heißt es weiter zu dem von einem Verarbeiter danach zu verlangenden Schutzniveau, dass sowohl End-to-End-Verschlüsselung als auch Transportverschlüsselung für ihren jeweiligen Anwendungszweck Risiken für die Vertraulichkeit der übertragenen Nachrichten mindern. Daher müssten Verantwortliche beide Verfahren in der Abwägung der notwendigen Maßnahmen berücksichtigen. Der durchgreifendste Schutz der Vertraulichkeit der Inhaltsdaten werde durch End-to-End-Verschlüsselung erreicht. End-to-End-Verschlüsselung schütze nicht nur den Transportweg, sondern auch ruhende Daten; der Einsatz von Transportverschlüsselung biete einen Basis-Schutz und stelle eine Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen dar. Die Verantwortlichen müssten die Risiken sorgfältig einschätzen, die mit dem Bruch der Vertraulichkeit und Integrität von E-Mail-Nachrichten verbunden seien, die sie versendeten oder gezielt empfangen.
- 90 (ccc) Nach Ansicht des Senats ist danach eine Transportverschlüsselung beim Versand von geschäftlichen Emails mit personenbezogenen Daten zwischen Unternehmer und Kunden jedenfalls bei dem hier bestehenden hohen finanziellen Risiko durch Verfä-

schung der angehängten Rechnung der Klägerin für den Kunden nicht ausreichend und kann keinen „geeigneten“ Schutz im Sinne der DSGVO darstellen. Vielmehr ist die End-to-End-Verschlüsselung zurzeit das Mittel der Wahl.

- 91 Soweit in der Orientierungshilfe der Datenschutzkonferenz zur Einzelfallentscheidung darauf abgestellt wird, dass in Verarbeitungssituationen mit normalen Risiken bereits durch die Transportverschlüsselung eine ausreichende Risikominderung erreicht wird, zeigt der zu entscheidende Fall nach Ansicht des Senats deutlich, dass hier keine „Verarbeitungssituation mit normalen Risiken“ vorliegt. Er ist zwar anders gelagert als die üblicherweise für die Annahme eines hohen Risikos herangezogenen Emails z.B. mit Arztbriefen oder Rechtsanwaltsschreiben im Anhang, die vor allem wegen des hohen Umfangs und der Intensität der persönlichen Daten besonders schutzwürdig sein sollen. Bei der hier streitgegenständlichen Email mit der Rechnung der Klägerin im Anhang sind die persönlichen Daten der Beklagten als Privatkundin wie Name und Adresse und die Tatsache, dass die Beklagte einen Werkvertrag abgeschlossen hat, nicht in dem Maße tiefgreifend persönlich. Der Zugriff durch einen unbefugten Dritten darauf führte aber im konkreten Fall in Verbindung mit der ebenfalls „gehackten“ und unberechtigt veränderten Kontoverbindung der Klägerin dazu, dass die Beklagte auf ein falsches Konto gezahlt hat und – wie die Ausführungen unter 1. zeigen – den Werklohn nunmehr erneut zahlen soll, so dass ihr ein massiver finanzieller Schaden von über 15.000,-- € entstanden ist. Dass Kunden von Unternehmen bei einem Datenhacking solche Vermögenseinbußen drohen, ist ein Risiko, das dem Versand von Rechnungen per Email immanent ist, von der Klägerin bei ihrer Planung zur Emailsicherheit erkannt werden musste und bei ihren Überlegungen zu Schutzmaßnahmen beim Versand von Rechnungen per Email mit einzubeziehen war. Anders, als das Landgericht meint, kommt es darauf, dass bei der Klägerin bislang ein Hackerangriff noch nicht vorgekommen war, nicht an. Die stetig wachsende Gefahr von Hackerangriffen auf Unternehmen ist allgemein bekannt und die hohe Schadensträchtigkeit des Versands von Rechnungen per Email verlangt von einem Unternehmen wie der Klägerin eine entsprechende Voraussicht und ein entsprechendes proaktives Handeln.
- 92 Der Senat verkennt dabei nicht, dass die hier für einen Email-Versand mit angehängter Rechnung verlangte End-to-End-Verschlüsselung für ein Unternehmen wie die Klägerin einen gewissen technischen Aufwand erfordert, der sich möglicherweise nicht darauf beschränkt, in dem benutzten Standard-Email-Programm lediglich eine Aktivierung vorzunehmen. Vielmehr dürfte hier vielfach eine technische Beratung und der Einsatz von gesonderten Programmen erforderlich sein. Dies ändert aber nach Ansicht des Senats die an die Verschlüsselung von geschäftlichen Emails mit angehängten Rechnungen zu stellenden Anforderungen nicht. Angesichts der allgemein bekannten und vielfältig veröffentlichten Hackermöglichkeiten, des gerichtsbekannt rasanten Anstiegs von Hackerangriffen und den im Einzelfall weitreichenden finanziellen Folgen für den einzelnen Kunden, dessen Rechnung verfälscht wird und der selbst keinen Einfluss auf die Verarbeitung seiner Daten hat, ist daher auch von einem kleineren Unternehmen – wie der Klägerin als mittelständischem Handwerksbetrieb – zu erwarten, dass es sich zum Schutz der Daten seiner Kunden zu computertechnischen Sicherheitsanforderungen informiert und sich diesbezüglich beraten, fortbilden und mit der notwendigen Software ausstatten lässt. Die Klägerin kann sich nicht darauf berufen, dass es sich bei der End-to-End-Verschlüsselung im Geschäftsleben um eine unübliche Verschlüsselung handeln würde, die von ihr nicht verlangt werden könne. Vielmehr beschäftigen sich vielfache, allgemein zugängliche Empfehlungen und Informationen aktuell mit den entsprechenden

Möglichkeiten, so auch die Information des BSI zur Praxis der Emailverschlüsselung unter Nennung verschiedener Email-Tools, die eine solche Verschlüsselung ermöglichen (s. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesst-kommunizieren/E-Mail-Verschluesseleung/E-Mail-Verschluesseleung-in-der-Praxis/e-mail-verschluesseleung-in-der-praxis_node.html). Dass einer End-to-End-Verschlüsselung im konkreten Fall technische, organisatorische und/oder finanzielle Hindernisse im Weg gestanden hätten, hat die Klägerin nach entsprechendem Hinweis des Senats in der mündlichen Verhandlung, welche Schutzmaßnahmen er erwarte, nicht vorgetragen.

- 93 Soweit dieser zu erwartende hohe Standard zum Schutz der personenbezogenen Daten beim Versand von Emails mit angehängten Rechnungen nicht sichergestellt werden kann, bleibt für ein Unternehmen – ohne dass hierfür größerer technischer und/oder finanzieller Aufwand betrieben werden müsste – wie eh und je der Versand von Rechnungen per Post das Mittel der Wahl.
- 94 (dd) Die Klägerin trifft auch ein Verschulden.
- 95 Nach der Rechtsprechung des Europäischen Gerichtshofs ist einer kombinierten Analyse der verschiedenen Bestimmungen von Art. 82 DSGVO zu entnehmen, dass dieser Artikel ein Haftungsregime für Verschulden vorsieht, bei dem die Beweislast nicht der Person obliegt, der ein Schaden entstanden ist, sondern dem Verantwortlichen (EuGH, Urteil v. 21.12.2023 - C-667/21, juris Rn. 92 ff.).
- 96 Gemäß Art. 82 Abs. 3 DSGVO wird der Anspruchsverpflichtete von der Haftung – hier für unzureichende Schutzmaßnahmen in Bezug auf die Versendung personenbezogener Daten – befreit, wenn er in keinerlei Hinsicht für den schadensverursachenden Umstand verantwortlich ist. Verantwortung ist dabei das Verschulden im Sinne der deutschen Rechtsterminologie und nicht die datenschutzrechtliche Verantwortung (LG Mainz, Urteil vom 12.11.2021 - 3 O 12/20, juris Rn. 73; Quaas, in: Wolff/Brink, BeckOK Datenschutzrecht, 50. Edition, Stand 01.08.2024, Art. 82 DSGVO Rn. 17 und 17.2; Geissler/Ströbel, in: NJW 2019, 3414 (3415)). Das Verschulden wird nach dem Wortlaut der Norm grundsätzlich vermutet. Um die Feststellung treffen zu können, der Verantwortliche sei "in keinerlei Hinsicht" verantwortlich, hat dieser nachzuweisen, dass er alle Sorgfaltspflichten erfüllt hat und ihm damit nicht die geringste Fahrlässigkeit vorgeworfen werden kann (Quaas, in: Wolff/Brink, BeckOK Datenschutzrecht, a.a.O., Art. 82 DSGVO Rn. 18). Diesen Nachweis hat die Klägerin nicht zu führen vermocht. Ihr ist insofern – wie oben dargestellt – der Vorwurf eines unzureichenden Schutzniveaus für den Versand von Emails mit personenbezogenen Daten – insbesondere mit der hier angehängten Rechnung – zu machen.
- 97 Die Klägerin kann sich auch nicht darauf berufen, dass sie sich ausreichend hätte beraten lassen und auch ihr IT-Berater, der Zeuge C., im Rahmen zu treffender Schutzmaßnahmen lediglich eine Transportverschlüsselung vorgeschlagen habe. Da es keine gesetzlich festgelegten Schutzmaßnahmen gibt, obliegt es letztlich allein der Klägerin zu entscheiden, wie sie ihren Email-Versand mit personenbezogenen Daten sichern will und muss. Ihr IT-Berater konnte insofern lediglich die Optionen nennen; die Entscheidung hatte sie zu treffen. Diesbezüglich hat sie zumindest fahrlässig nicht auf ein ausreichendes Schutzniveau geachtet.

- 98 (2) Der Beklagten ist unstreitig ein Schaden entstanden, der in dem – wie oben dargestellt – mangels Erfüllung erneut zu zahlenden Werklohn liegt.
- 99 (3) Dieser von der Beklagten geltend gemachte Schaden ist auch eine kausale Folge des Verstoßes gegen die Datenschutzgrundverordnung.
- 100 Da nach den obigen Darlegungen die Klägerin bei Versand ihrer Email mit der angehängten Rechnung kein ausreichendes Schutzniveau zur Sicherung der personenbezogenen Daten der Beklagten eingehalten hat, obliegt ihr der Beweis dafür, dass der der Beklagten entstandene Schaden nicht durch ihr Fehlverhalten entstanden ist (EuGH, Urteil v. 14.12.2023 – C-340/21, juris Rn. 72). Dies ist ihr vorliegend nicht gelungen.
- 101 Unstreitig ist bei der von der Klägerin (maximal) verwendeten Transportverschlüsselung ein Zugriff durch unbefugte Dritte auf ihrem Computer, ihrem Server oder auf weiteren Servern auf dem Weg zum streitverkündeten Zeugen A. ohne Weiteres möglich; die Email ist definitionsgemäß nur auf dem Transport verschlüsselt. Einen Beweis dafür, dass im konkreten Fall der Zugriff nicht im Bereich der Klägerin, sondern erst im Bereich der Beklagten bzw. des Zeugen A. erfolgt ist, hat die Klägerin, der – wie ausgeführt und auch in der mündlichen Verhandlung erörtert – die Darlegungs- und Beweislast dafür obliegt, nicht angeboten. Die Einholung eines Sachverständigengutachtens von Amts wegen scheidet aus, da es sich mangels Anknüpfungstatsachen um einen Ausforschungsbe-
weis handeln würde. Auch die bei dem Zeugen A. vorhandenen Schutzmaßnahmen sind aus diesem Grund nicht weiter aufzuklären.
- 102 Im Übrigen wäre der Klägerin – selbst wenn der unbefugte Zugriff im Bereich des Zeu-
gen A. und nicht schon im Bereich der Klägerin erfolgt sein sollte – weiterhin anzulasten, dass sie einen solchen Zugriff durch den von ihr gewählten Versand der Daten per Email lediglich mit Transportverschlüsselung und damit mit unzureichender Sicherung erst ermöglicht hätte, denn auch bei einem von der Klägerin angesprochenen Datenhacking im Bereich des Zeugen A. wäre die streitgegenständliche Email samt Anhang aufgrund der End-to-End-Verschlüsselung wegen des eigenen erforderlichen Schlüssels bei Einhaltung entsprechender Standards auch auf dem Server/Computer des Zeugen jedenfalls ganz weitgehend geschützt gewesen.
- 103 (4) Ein Mitverschulden an der Schadensentstehung gem. § 254 BGB trifft die Beklagte nicht.
- 104 Anders als das Landgericht meint, oblag der Beklagten bzw. dem Zeugen A., dessen Verschulden ihr möglicherweise gem. § 278 BGB zuzurechnen wäre, nach Ansicht des Senats keine genaue Überprüfung der letztlich auf dem Computer des Zeugen verfälscht, da hinsichtlich der Kontoverbindung manipuliert vorliegenden Rechnung. Die von der Klägerin aufgezeigten Unterschiede zu früheren (Abschlags-)Rechnungen betreffend die Farbe, Angaben zum Geschäftsführer, fehlenden QR-Code der Bankverbindung und fehlendes Siegel stellen geringfügige äußere Abweichungen dar, die weder der Beklagten noch dem Zeugen A. bei oberflächlicher Betrachtung auffallen mussten. Etwas anderes folgt auch nicht daraus, dass die Beklagte erkannt hat, dass die Kontoverbindung verändert war. Angesichts der Tatsache, dass im Geschäftsleben die Kontoverbindung eines Unternehmens aus diversen Gründen geändert wird, kann einer privaten Kundin wie der Beklagten nicht vorgeworfen werden, dass sie vor der Überweisung des offenen Werklohns keine Rücksprache mit der Klägerin genommen hat.

- 105 b) Ob die Klägerin daneben auch gem. § 280 Abs. 1 BGB aus einer Nebenpflichtverletzung haftet, weil sie die Vermögensinteressen der Beklagten nicht hinreichend geschützt hat, kann vorliegend offen bleiben.
- 106 Zwar könnte in dem fehlenden Schutzniveau für den Versand von Emails auch eine verschuldete Nebenpflichtverletzung des zwischen den Parteien bestehenden Werkvertrags liegen. Da die Darlegungs- und ggf. Beweislast für einen solchen Schadensersatzanspruch jedoch hinsichtlich der Kausalität dieser Pflichtverletzung für den eingetretenen Schaden – anders als bei Art. 82 DSGVO – bei der Beklagten als derjenigen liegt, die den Anspruch geltend macht, was weitere Prüfungen nach sich ziehen würde, und der Beklagten ein Schadensersatzanspruch bereits nach Art. 82 DSGVO zuzusprechen ist (s. oben a)), kann diese Frage offen bleiben.
- 107 3. Nachdem der Anspruch der Klägerin auf erneute Zahlung des Werklohns abzuweisen ist, besteht auch kein Anspruch auf vorgerichtliche Rechtsanwaltskosten gem. § 280 Abs. 2, 286 Abs. 3 BGB.
- 108 4. Die prozessualen Nebenentscheidungen beruhen auf § 91 Abs. 1, 101 Abs. 1, 708 Nr. 10, 711 ZPO.
- 109 Die Revision wird gemäß § 544 Abs. 2 Nr. 1 ZPO zugelassen. Die Frage, welches Schutzniveau vom Verarbeiter gem. Art. 24, 32 DSGVO beim Versand geschäftlicher Emails mit personenbezogenen Daten, insbesondere mit angehängten Rechnungen, einzuhalten ist, ist höchstrichterlich noch nicht geklärt.