Sicherheitsvorkehrung beim Versand von Rechnungen per E-Mail

DS-GVO Art. 5 Abs. 2, 24, 32, 82 Abs. 1, Abs. 3 BGB §§ 242, 254, 278, 62 Abs. 2, 631

OLG Schleswig, Urteil vom 18.12.2024 – 12 U 9/24 (LG Kiel); rechtskräftig

Leitsätze

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 E-Mail versandte Rechnung unbefugt verändert worden ist, führt nicht zur Erfüllung der Zahlungsverpflichtung iSv § 362 Abs. 2 BGB.

2. Dem Kunden kann allerdings ein Schadensersatzanspruch in Höhe der auf das Drittkonto getätigten Überweisung zustehen, den er der Klageforderung des Werkunternehmers unter dem Gesichtspunkt der Dolo-agit-Einwendung gem. § 242 BGB entgegenhalten kann.

3. Ein solcher Schadensersatzanspruch kann aus Art. 82 DS-GVO resultieren.

4. Art. 82 Abs. 2 DS-GVO – der die in Art. 82 Abs. 1 DS-GVO grundsätzlich normierte Haftungsregelung präzisiert – hat drei Voraussetzungen für die Entstehung eines Schadensersatzanspruchs, nämlich – erstens eine Verarbeitung personenbezogener Daten iSd Art. 5 Abs. 1 lit. a Var. 1, 6 Abs. 1 UAbs. 1 lit. a, 7 DS-GVO iVm Art. 4 Nr. 1 und 2 DS-GVO unter schuldhaftem Verstoß gegen die Bestimmungen der DS-GVO, – zweitens einen der betroffenen Person entstandenen Schaden und - drittens einen Kausalzusammenhang zwischen der rechtswidrigen Verarbeitung und diesem Schaden (vgl. EuGH Urt. v. 25.1.2024 – C-687/21 [= ZD 2024, 334] Rn. 58; EuGH Urt. v. 4.5.2023 – C-300/21 [= ZD 2023, 446] Rn. 36 mAnm Mekat/Ligocki).

5. Ein Verstoß gegen die Vorschriften der DS-GVO durch den Verantwortlichen kann in diesem Zusammenhang nicht schon allein deswegen angenommen werden, weil ein unbefugter Zugriff auf personenbezogene Daten durch Dritte iSv Art. 4 Nr. 10 DS-GVO stattgefunden hat (vgl. EuGH Urt. v. 25.1.2024 – C-687/21 [= ZD 2024, 334] Rn. 45; EuGH Urt. v. 14.12.2023 – C-340/21 [= ZD 2024, 150 mAnm Ligocki/Sosna] Rn. 22 ff., 31-39).

6. Umgekehrt ist nach der Rechtsprechung des EuGH der Verantwortliche aber auch nicht gem. Art. 82 Abs. 3 DS-GVO von seiner nach Art. 82 Abs. 1 und 2 DS-GVO 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 Urt. v. 14.12.2023 – C-340/21 [= ZD 2024, 150 mAnm Ligocki/ Sosna] Rn. 65 ff., 74).

7. Vielmehr hat der Verantwortliche die Möglichkeit, aber auch die Verpflichtung, nach dem in Art. 5 Abs. 2 DS-GVO formulierten und in Art. 24 DS-GVO konkretisierten Grundsatz seiner Rechenschaftspflicht darzulegen und zu beweisen, dass die von ihm getroffenen Sicherheitsmaßnahmen geeignet waren, um die personenbezogenen Daten entsprechend dem von der DS-GVO verlangten Sicherheitsniveau vor dem Zugriff Unbefugter zu schützen (vgl. EuGH Urt. v. 25.1.2024 – C-687/21 [= ZD 2024, 334] Rn. 40ff.; ebenso EuGH Urt. v. 14.12.2023 – C-340/21 [= ZD 2024, 150 mAnm Ligocki/Sosna] Rn. 48 ff., 57).

8. Der EuGH hat die Anforderungen des Art. 32 DS-GVO 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 Urt. v. 14.12. 2023 – C-340/21 [= ZD 2024, 150 mAnm Ligocki/Sosna] Rn. 40 ff., 47).

9. Nach Ansicht des Senats ist danach eine reine Transportverschlüsselung beim Versand von geschäftlichen E-Mails 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 iSd DS-GVO darstellen. Vielmehr ist die End-to-End-Verschlüsselung zurzeit das Mittel der Wahl.

10. Gem. Art. 82 Abs. 3 DS-GVO wird der Verantwortliche von der Haftung befreit, wenn er in keinerlei Hinsicht für den schadensverursachenden Umstand verantwortlich ist. Verantwortung ist dabei das Verschulden iSd deutschen Rechtsterminologie und nicht die datenschutzrechtliche Verantwortung (LG Mainz Urt. v. 12.11.2021 – 3 O 12/20 [= ZD 2022, 163] Rn. 73; Wolff/Brink, BeckOK Datenschutzrecht/Quaas, 50. Ed. 1.8.2024, Art. 82 DS-GVO Rn. 17 und 17.2; Geissler/Ströbel NJW 2019, 3414 (3415)). Das Verschulden wird nach dem Wortlaut der Norm grundsätzlich vermutet.

11. Ist bei dem Versand von geschäftlichen E-Mails 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 Urt. v. 14.12.2023 – C-340/21 [= ZD 2024, 150 mAnm Ligocki/Sosna] Rn. 72).

12. Ein Mitverschulden des Kunden iSv § 254 BGB kann aus Abweichungen der E-Mail – hier einer angehängten Rechnung – von früheren Rechnungen resultieren und obliegt einer Prüfung im Einzelfall.

Sachverhalt

Die Parteien streiten darüber, ob die Kl. (erneut) die Zahlung ihrer Werklohnforderung durch die Bekl. verlangen kann, nachdem der Überweisungsbetrag nach Manipulation der Rechnung durch kriminell handelnde Dritte dem Konto eines Unbekannten gutgeschrieben wurde.

Hinsichtlich des weiteren Sachverhalts wird Bezug genommen auf den Tatbestand des landgerichtlichen Urteils.

Das LG hat der Klage stattgegeben. Der Kl. stehe gegen die Bekl. ein Anspruch auf Zahlung der ausstehenden Vergütung iHv 15.385,78 EUR zu.

Zwischen den Parteien sei unstreitig, dass sie einen Werkvertrag iSd § 631 BGB in Form eines Bauvertrags abgeschlossen hätten, die Kl. ihre vertraglich geschuldeten Werkleistungen erbracht habe und infolge getätigter Abschlagszahlungen gem. § 641 Abs. 1 S. 1 BGB noch eine von der Bekl. geschuldete Vergütung iHv 15.385,78 EUR nach Stellung einer Schlussrechnung am

26.9.2022 sowie durch Abnahme des Werks am 12.1.2023 fällig gewesen sei.

Unstreitig sei ebenso, dass seitens der Bekl. in Bezug auf jene Schlussrechnung eine skontogeminderte Zahlung iHv 14.924,20 EUR auf das Konto eines Dritten erfolgt sei. Allerdings sei durch diese Zahlung der Anspruch der Kl. auf verbleibende Vergütung ihrer Leistung nicht gem. § 362 BGB erloschen.

Aus den Gründen

47 Die zulässige Berufung ist begründet. Die Kl. hat keinen Anspruch auf (erneute) Zahlung des vereinbarten Werklohns durch die Bekl., ebenso wenig auf Zahlung außergerichtlicher Rechtsanwaltsgebühren.

48 1. Zwischen den Parteien ist unstreitig ein Werkvertrag iSd § 631 BGB in Form eines Bauvertrags zustande gekommen. Die Kl. hat ihre vertraglich geschuldeten Werkleistungen erbracht und infolge getätigter Abschlagszahlungen war gem. § 641 Abs. 1 S. 1 BGB noch eine Vergütung iHv 15.385,78 EUR nach Stellung einer Schlussrechnung am 26.9.2022 von der Bekl. geschuldet, sowie nach Abnahme des Werks am 12.1.2023 fällig.

49 Unstreitig ist ebenso, dass seitens der Bekl. in Bezug auf jene Schlussrechnung eine skontogeminderte Zahlung iHv 14.924,20 EUR auf das Konto eines Dritten erfolgt ist. Allerdings ist die Forderung der Kl. dadurch nicht erfüllt iSv § 362 Abs. 2 BGB. Insoweit folgt der Senat dem LG. ...

52 2. Anders als das LG meint, steht der Bekl. allerdings ein Schadensersatzanspruch in Höhe der auf das Drittkonto getätigten Überweisung des streitgegenständlichen Betrags zu, den die Bekl. der Klagforderung unter dem Gesichtspunkt der Doloagit-Einwendung gem. § 242 BGB entgegenhalten kann.

53 a) Ein solcher Anspruch resultiert vorliegend jedenfalls aus Art. 82 DS-GVO.

54 Die DS-GVO verlangt von Unternehmen, sensible Daten gegen Datenschutzverletzungen zu sichern. Sensible Daten sind zB 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 DS-GVO 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 DS-GVO eröffnet einen direkten eigenen deliktischen Schadensersatzanspruch mit Verschuldensvermutung, wobei der Verantwortliche nach Absatz 3 den Entlastungsbeweis führen kann. ...

62 (1) Vorliegend hat nach Ansicht des Senats die Kl. – anders als das LG meint – im Zuge der Verarbeitung der personenbezogenen Daten der Bekl. bei Versand der streitgegenständlichen E-Mail mit Anhang gegen die Grundsätze der Art. 5, 24 und 32 DS-GVO verstoßen. ...

65 (cc) Vielmehr hat der Verantwortliche die Möglichkeit, aber auch die Verpflichtung, nach dem in Art. 5 Abs. 2 DS-GVO formulierten und in Art. 24 DS-GVO konkretisierten Grundsatz seiner Rechenschaftspflicht darzulegen und zu beweisen, dass die von ihm getroffenen Sicherheitsmaßnahmen geeignet waren, um die personenbezogenen Daten entsprechend dem von der DS-GVO verlangten Sicherheitsniveau vor dem Zugriff Unbefugter zu schützen (vgl. EuGH Urt. v. 25.1.2024 – C-687/21 [= ZD 2024, 334] Rn. 40ff.; ebenso EuGH Urt. v. 14.12.2023 – C-340/21 [= ZD 2024, 150 mAnm Ligocki/Sosna = MMR 2024, 231 mAnm Kohl/Rothkegel] Rn. 48 ff., 57). Das ist der Kl. vorliegend nicht gelungen, da der Senat die Transportverschlüsselung, die sie beim Versand der streitgegenständlichen E-Mail – von der Bekl. bestritten – verwendet haben

will (in Form von SMTP über TLS), nicht für ausreichend und damit auch nicht für „geeignet" iSd DS-GVO hält. Es kann damit auch dahinstehen, ob eine solche Transportverschlüsselung tatsächlich erfolgt ist. Das von der Kl. zum Beweis dafür und für die Frage, ob eine Transportverschlüsselung dem üblichen Sicherungsmaß entspricht oder sogar darüber hinausgeht, angebotene Sachverständigengutachten ist insoweit nicht einzuholen.

66 (aaa) Der Senat verkennt dabei nicht, dass es konkrete gesetzliche Anforderungen an eine Verschlüsselung von E-Mails nicht gibt.

67 Auch in der DS-GVO ist eine Verschlüsselung nicht zwingend vorgeschrieben. Sie wird jedoch mehrfach im Text der Verordnung erwähnt, jedes Mal als Empfehlung. In Art. 32 DS-GVO 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 u.a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten gehören. Da die DS-GVO die Verschlüsselung jedoch nicht zwingend vorschreibt, bietet sie keine Klarheit darüber, wann die Verschlüsselung verwendet werden sollte und welche Standards dabei angewendet werden müssen.

68 Nach der „Orientierungshilfe des Arbeitskreises Technische und organisatorische Datenschutzfragen vom 27.5.2021", 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, 25 und 32 Abs. 1 DS-GVO 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 insb. 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_verschluesselung.pdf).

69 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 E-Mails – genießt. Es ist daher zur Überzeugung des Senats auch verpflichtet, diesen Schutz durch entsprechende Maßnahmen so weit wie möglich zu gewährleisten.

70 Der EuGH hat die Anforderungen des Art. 32 DS-GVO 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 Urt. v. 14.12.2023 – C-340/21 Rn. 40 ff., 47).

71 (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 Kl. ausgeschlossen, geschäftliche E-Mails mit personenbezogenen Daten völlig ohne jede Verschlüsselung zu versenden. ...

74 (ccc) Nach Ansicht des Senats ist danach eine Transportverschlüsselung beim Versand von geschäftlichen E-Mails mit personenbezogenen Daten zwischen Unternehmer und Kunden jedenfalls bei dem hier bestehenden hohen finanziellen Risiko durch Verfälschung der angehängten Rechnung der Kl. für den Kunden nicht ausreichend und kann keinen „geeigneten" Schutz iSd DS-GVO darstellen. Vielmehr ist die End-to-End-Verschlüsselung zurzeit das Mittel der Wahl.

75 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 E-Mails zB 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 E-Mail mit der Rechnung der Kl. im Anhang sind die persönlichen Daten der Bekl. als Privatkundin wie Name und Adresse und die Tatsache, dass die Bekl. einen Werkvertrag abgeschlossen hat, nicht in dem Maße tiefgreifend persönlich. Der Zugriff durch einen unbefugten Dritten darauf führte aber im konkreten Fall iVm der ebenfalls „gehackten" und unberechtigt veränderten Kontoverbindung der Kl. dazu, dass die Bekl. auf ein falsches Konto gezahlt hat und - wie die Ausführungen unter 1. zeigen – den Werklohn nunmehr erneut zahlen soll, sodass ihr ein massiver finanzieller Schaden von über 15.000 EUR entstanden ist. Dass Kunden von Unternehmen bei einem Datenhacking solche Vermögenseinbußen drohen, ist ein Risiko, das dem Versand von Rechnungen per E-Mail immanent ist, von der Kl. bei ihrer Planung zur E-Mail-Sicherheit erkannt werden musste und bei ihren Überlegungen zu Schutzmaßnahmen beim Versand von Rechnungen per E-Mail mit einzubeziehen war. Anders, als das LG meint, kommt es darauf, dass bei der Kl. 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 E-Mail verlangt von einem Unternehmen wie der Kl. eine entsprechende Voraussicht und ein entsprechendes proaktives Handeln.

76 Der Senat verkennt dabei nicht, dass die hier für einen E-Mail-Versand mit angehängter Rechnung verlangte End-to-End-Verschlüsselung für ein Unternehmen wie die Kl. einen gewissen technischen Aufwand erfordert, der sich möglicherweise nicht darauf beschränkt, in dem benutzten Standard-E-Mail-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 E-Mails 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 Kl. 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 Kl. 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 E-Mail-Verschlüsselung unter Nennung verschiedener E-Mail-Tools, die eine solche Verschlüsselung ermöglichen (s. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/E-Mail-Verschluesselung/E-Mail-Verschluesselung-in-der-Praxis/e-mail-verschlues selung-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 Kl. nach entsprechendem Hinweis des Senats in der mündlichen Verhandlung, welche Schutzmaßnahmen er erwarte, nicht vorgetragen.

77 Soweit dieser zu erwartende hohe Standard zum Schutz der personenbezogenen Daten beim Versand von E-Mails 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. ...

82 (2) Der Bekl. ist unstreitig ein Schaden entstanden, der in dem – wie oben dargestellt – mangels Erfüllung erneut zu zahlenden Werklohn liegt.

83 (3) Dieser von der Bekl. geltend gemachte Schaden ist auch eine kausale Folge des Verstoßes gegen die DS-GVO.

84 Da nach den obigen Darlegungen die Kl. bei Versand ihrer E-Mail mit der angehängten Rechnung kein ausreichendes Schutzniveau zur Sicherung der personenbezogenen Daten der Bekl. eingehalten hat, obliegt ihr der Beweis dafür, dass der der Bekl. entstandene Schaden nicht durch ihr Fehlverhalten entstanden ist (EuGH Urt. v. 14.12.2023 – C-340/21 Rn. 72). Dies ist ihr vorliegend nicht gelungen.

85 Unstreitig ist bei der von der Kl. (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 E-Mail ist definitionsgemäß nur auf dem Transport verschlüsselt. Einen Beweis dafür, dass im konkreten Fall der Zugriff nicht im Bereich der Kl., sondern erst im Bereich der Bekl. bzw. des Zeugen A. erfolgt ist, hat die Kl., 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 Ausforschungsbeweis handeln würde. Auch die bei dem Zeugen A. vorhandenen Schutzmaßnahmen sind aus diesem Grund nicht weiter aufzuklären.

86 IÜ wäre der Kl. – selbst wenn der unbefugte Zugriff im Bereich des Zeugen A. und nicht schon im Bereich der Kl. erfolgt sein sollte – weiterhin anzulasten, dass sie einen solchen Zugriff durch den von ihr gewählten Versand der Daten per E-Mail le-

diglich mit Transportverschlüsselung und damit mit unzureichender Sicherung erst ermöglicht hätte, denn auch bei einem von der Kl. angesprochenen Datenhacking im Bereich des Zeugen A. wäre die streitgegenständliche E-Mail samt Anhang aufgrund der End-to-End-Verschlüsseluung wegen des eigenen erforderlichen Schlüssels bei Einhaltung entsprechender Standards auch auf

dem Server/Computer des Zeugen jedenfalls ganz weitgehend geschützt gewesen.

87 (4) Ein Mitverschulden an der Schadensentstehung gem. § 254 BGB trifft die Bekl. nicht.

88 Anders als das LG meint, oblag der Bekl. 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 Kl. 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 Bekl. noch dem Zeugen A. bei oberflächlicher Betrachtung auffallen mussten. Etwas anderes folgt auch nicht daraus, dass die Bekl. 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 Bekl. nicht vorgeworfen werden, dass sie vor der Überweisung des offenen Werklohns keine Rücksprache mit der Kl. genommen hat. ...

Anmerkung

Das Datenschutzrecht hat inzwischen an den Gerichten und in der Anwaltschaft vermehrt Beachtung gefunden. Dennoch fällt es vielen schwer, das Datenschutzrecht als Ausfluss des Datenschutzgrundrechts iRd risikobasierten Ansatzes der DS-GVO einzuordnen. Weiterhin sind aufgrund des technischen Fortschritts und der komplexen Sachverhalte vertiefte Kenntnisse über IT-Systeme und IT-Sicherheit notwendig, um den Sachverhalt datenschutzrechtlich vorzutragen oder zu beurteilen.

Daher werden der Urteilsbesprechung eine Einordnung des technischen und rechtlichen Hintergrunds – hier insb. Art. 32 DS-GVO – sowie die zum Verständnis notwendige Tatsachenfeststellung der Ausgangsinstanz vorangestellt.

1. Technischer Hintergrund

Grundlage des Verfahrens war, dass der Anhang einer E-Mail, genauer eine Rechnung im PDF-Format, verändert wurde. Die ausschlaggebende Änderung in der Rechnung lag in der Veränderung der dort angegebenen IBAN des rechnungausstellenden Unternehmens.

Diese Art des Betrugs ist in den letzten Jahren verstärkt aufgetreten. Beim „Business-E-Mail-Compromise"-Scam werden Rechnungen von den Betrügern abgefangen und die IBAN in den Rechnungen geändert. Dies geschieht entweder bereits beim Versender vor dem Versand der E-Mail oder beim Empfänger nach dem Eingang.

Hierbei haben sich vier übliche Szenarien herauskristallisiert:

- Die Angreifer verschaffen sich Zugriff auf das IT-System des Rechnungsversenders. Dann wird die Rechnungsvorlage bereits im System geändert, sodass die IBAN bei keiner Rechnung der Realität entspricht.

- Die Angreifer verschaffen sich Zugang zum E-Mail-Postfach des Mitarbeiters, der die Rechnungen versendet. Sie fügen im Postfach Regeln ein, die die Mail mit der Originalrechnung automatisiert an einen anderen Ort verschieben. Dort ändern die Angreifer die Rechnung und senden diese dann über den Account des Mitarbeiters zum Rechnungsempfänger.

- Die Angreifer verschaffen sich Zugang zum E-Mail-Postfach des Rechnungsempfängers. Sie führen Regeln ein, die die Mails sofort aus dem Posteingang an einen anderen Ordner verschieben. Dort verändern die Angreifer die Rechnung und verschieben die geänderte Rechnung

wieder in den Posteingang oder versenden sie erneut unter einer ähnlich lautenden E-Mail-Adresse an den Empfänger.

Eine weitere Form ist die vollständig irreale Rechnung, die die Angreifer ohne Zugriff auf die Postfächer von einer Domain versenden, die der Domain des Rechnungsstellers stark ähnelt.

2. Zwischenergebnis

Um bei einer veränderten Mail richtig vorzutragen, muss technisch festgestellt werden, ob und bei welchem Kommunikationspartner der Angriff stattfand – entweder auf der Versender- oder der Empfängerseite. Dies ist essenziell für die rechtliche Einordnung eines Verstoßes gegen Art. 32 DS-GVO.

Das OLG stützte seine Entscheidung allerdings auf keines dieser „normalen" Szenarien, sondern nahm eine „Man in the Middle"-Attacke an. Bei dieser Attacke steht der Angreifer zwischen den Kommunikationspartnern und kontrolliert den Datenverkehr beim TK-Dienstleister. Diese Attacken sind bei E-Mails schwer zu realisieren, da der Angreifer die E-Mail im TK-Netz abfangen, verändern und wieder unbemerkt einspeisen muss. Dies erfordert extrem hohen technischen Aufwand. Daneben stellt sich bei diesen Angriffen die rechtliche Frage, welches Verschulden das TK-Unternehmen trifft.

3. Rechtlicher Hintergrund Art. 32 DS-GVO

Das OLG Schleswig stellte im Urteil rechtlich darauf ab, dass im unverschlüsselten Versand einer Rechnung per E-Mail ein Verstoß gegen Art. 32 DS-GVO liegt. Art. 32 DS-GVO konkretisiert Art. 25 DS-GVO und legt den Maßstab des Schutzes personenbezogener Daten durch entsprechende technische und organisatorische Maßnahmen iRd risikobasierten Ansatzes fest. Dafür müssen angemessene technische und organisatorische Maßnahmen ergriffen werden, insb. im Hinblick auf die Schwere des Risikos der Verarbeitung in Bezug auf die konkret verarbeiteten personenbezogenen Daten. Je sensibler die Daten sind, desto höhere Sicherungsmaßnahmen sind erforderlich.

4. Tatsachenfeststellungen

Vor dem LG Kiel (Urt. v. 29.12.2023 – 9 O 110/23) als Ausgangsinstanz stritten die Parteien darüber, ob sich der auf Zahlung des Werklohns verklagte Auftraggeber ggü. dem klagenden Werkunternehmer auf Erfüllung bzw. die Verletzung einer Nebenpflicht aus dem Werkvertrag berufen kann, wenn der Auftraggeber auf eine verfälschte Abschlussrechnung, die er per unverschlüsselter Mail erhielt, an einen unbekannten Dritten zahlte.

Der Bekl. hatte vor der Abschlussrechnung bereits auf zwei unverschlüsselt per E-Mail versandte Teilrechnungen gezahlt. Hinsichtlich des Versands bzw. des Empfangs der E-Mail stellte die Kammer im unstrittigen Sachverhalt fest: „Die streitgegenständliche dritte Abschlagsrechnung, zugleich Schlussrechnung, vom 26.9.2022 über den Betrag von 15.385,78 EUR sandte die Kl. ebenfalls als Anlage im pdf-Format nebst Aufmaß an den Zeugen. Bei diesem ging unter seinem E-Mail-Account am 27.9.2031 um 2:09 Uhr eine E-Mail ein, der u.a. eine unstreitig manipulierte Rechnung im pdf-Format beigefügt war."

Damit stellte das LG Kiel fest, dass eine Mail mit der Originalrechnung versandt wurde und eine Mail mit einer verfälschten Rechnung im Posteingang des Bauleiters des Bekl. (Zeuge) einging.

Die Kl. trug – strittig – vor, sie „selbst habe nach dem Vorfall ihre Computersysteme überprüfen lassen, wobei keine Sicherheitslücke ihres E-Mail-Accounts habe festgestellt werden können. Die Rechnungen der Kl. seien per SMTP (Simple Mail Transfer Protocol) über TLS (Transport Layer Security) verschlüsselt gewesen."

Auch strittig trug die Kl. vor, der vom Bekl. beauftragte Bauleiter – bei dem die Mail einging – „habe nach dem Vorfall wohl aus Sicherheitsgründen seinen ursprünglich genutzten E-Mail-Provider gewechselt, da die Manipulation in seinem Verantwortungsbereich stattgefunden haben müsse."

Der Bekl. trug strittig vor, „der Zeuge habe von der Kl. die manipulierten Unterlagen ... und nicht die unbearbeitete Originalrechnung ... zugesandt bekommen."

Im Verfahrensgang führt das OLG Schleswig ergänzend aus: „das strafrechtliche Verfahren gegen Herrn B. wegen Abfangens von Daten, Betrug und Geldwäsche beim Amtsgericht Y. zum dortigen Az. ... 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 Bekl. die Rechnung habe zukommen lassen und sein E-Mail-Konto nach der streitgegenständlichen Manipulation von ... zu yyy gewechselt haben solle."

Damit war in beiden Instanzen strittig, ob es sich um eine „Man in the Middle" - oder die in 1. genannte dritte Variante – genauer: das kompromittierte Mailpostfach des Empfängers – gehandelt hat. Offen bleibt im Urteil des OLG Schleswig allerdings, wie es trotz des strittigen Sachverhalts zur Feststellung kam, dass es sich um einen „Man in the Middle"-Angriff handelte.

5. Technische und rechtliche Einordnung

Prozessual machte der Bekl. eine Einwendung und eine Einrede geltend. So erhob er wegen der erfolgten Überweisung die Einwendung der Erfüllung iSv § 362 Abs. 1 BGB. Zudem machte er die Dolo-agit-Einrede aus § 242 BGB geltend und begründete dies damit, dass der Kl. mit dem unverschlüsselten Versand eine Nebenpflicht verletzt habe. Daher habe die Darlegungs- und Beweislast für die Tatsachen, die begründen, dass durch die Überweisung an einen Dritten Erfüllung eingetreten war bzw. die mangelhafte IT-Sicherheit beim Mailversand zur Überweisung führte, beim Bekl. gelegen.

Dieser Argumentation folgte das OLG Schleswig und führte aus: „[ist] eine reine Transportverschlüsselung beim Versand von geschäftlichen E-Mails mit personenbezogenen Daten zwischen Unternehmer und Kunden jedenfalls bei dem hier bestehenden hohen finanziellen Risiko durch Verfälschung der angehängten Rechnung der Kl. für den Kunden nicht ausreichend und kann keinen geeigneten Schutz iSd DS-GVO darstellen. Vielmehr ist die End-to-End-Verschlüsselung zurzeit das Mittel der Wahl." und urteilte darauf, dass der Versand ohne End-to-End-Verschlüsselung einen Datenschutzverstoß iSd Art. 82 DS-GVO darstelle und die fehlende End-to-End-Verschlüsselung kausal für den Schaden – hier die Zahlung an den Dritten – sei. Der Bekl. habe daher aus Art. 82 DS-GVO einen Anspruch auf Schadensersatz in Höhe des überwiesenen Betrages.

Diese Rechtsansicht geht aus verschiedenen Gründen fehl.

a) Risikobewertung des Art. 32 DS-GVO

Der Senat verkennt, dass die sich auf der Rechnung befindlichen personenbezogenen Daten – Name, Anschrift und der Auftrag – in der datenschutzrechtlichen Bewertung auf einer niedrigen Risikostufe einzuordnen sind, da die DS-GVO der informationellen Selbstbestimmung und nicht dem sicheren Rechtsverkehr dienen soll. Weiter wurde nur die IBAN des Unternehmens verändert, also ein Datum, das gerade nicht der DS-GVO unterfällt.

Zusammenfassend ist bei einer streng datenschutzrechtlichen Betrachtung festzuhalten, dass nicht das evidente widerrechtliche Zugriffnehmen der Angreifer auf die personenbezogenen Daten des Auftraggebers, sondern vielmehr die Änderung eines nicht personenbezogenen Datums des Werkunternehmers zum Schaden geführt hat. Das Risiko iSd Art. 32 DS-GVO ergab sich dementsprechend gerade nicht aus der Verarbeitung der personenbezogenen Daten des Bestellers, sodass die Bezugnahme auf diese Daten – als mit einem hohen Risiko behaftet – fehlgeht.

So würde mit dieser Argumentation bei dem Diebstahl eines wertvollen Pakets die unberechtigte Kenntnisnahme von Name und Adresse der natürlichen Person auf dem Empfängerschild oder im Paket als Datenschutzverstoß und nicht die unzureichende Sicherung der Ware als Verstoß gegen den Transportvertrag den Schadensersatz auslösen.

b) Fehlende Verschlüsselung nicht unbedingt kausal

Wie in 1. ausgeführt gibt es neben der unwahrscheinlichen Variante des „Man in the Middle"-Angriffs vier Varianten des „Business-E-Mail-Compromise"-Angriffs, und aus technischer Sicht hätte bei zwei Varianten eine Verschlüsselung den Angriff nicht verhindern können.

So findet in der

- Variante 1 die Veränderung der Rechnung bereits vor dem Versand statt, sodass der Empfänger auch bei einer verschlüsselten Mail eine falsche Rechnung erhalten hätte und in der
- Variante 4 kann – sofern automatisches Entschlüsseln im Mailprogramm eingestellt ist – die Mail nach dem Empfang noch verändert werden.

Aus technischer Sicht wäre für ein sachgerechtes Urteil die Fragestellung: „Welches IT-System war kompromittiert?" Grundlage der Entscheidung und nicht die Verschlüsselung der Mail.

c) Darlegungs- und Beweislast bei Kausalität

Hinsichtlich der Darlegungs- und Beweislast in Bezug auf die Kausalität nimmt das OLG Schleswig abschließend rechtsirrig an, dass diese bei einem nachgewiesenen Datenschutzverstoß beim Verantwortlichen liegt.

Dazu führt das OLG aus, dass, da „die Kl. bei Versand ihrer E-Mail kein ausreichendes Schutzniveau zur Sicherung der personenbezogenen Daten der Bekl. eingehalten habe, ihr der Beweis obliege, dass der der Bekl. entstandene Schaden nicht durch ihr Fehlverhalten entstanden ist (EuGH Urt. v. 14.12.2023 – C-340/21 Rn. 72)."

Diese Rechtsansicht steht allerdings diametral zur vom OLG Schleswig genannten Rspr. des EuGH, da der EuGH in Rn. 72 nicht auf die Darlegungs- und Beweislast bei der Kausalität, sondern die Verschuldensregelung des Art. 82 Abs. 3 DS-GVO – genauer: die Möglichkeit der Enthaftung des Verantwortlichen, wenn er „nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist" – referenziert.

6. Ergebnis

Das vorliegende Urteil kann gerade im Hinblick auf die unvollständigen Feststellungen im strittigen Sachverhalt sowie aufgrund der fehlenden rechtlichen Wertungen bei der Kausalität für ähnlich gelagerte Sachverhalte herangezogen werden.

RA Bernhard Veeck, LL.M., bytelaw, Frankfurt/M.

Anm. d. Red.:

Der Volltext ist abrufbar unter: BeckRS 2024, 39951. Vgl. ferner EuGH ZD 2024, 334; EuGH ZD

2023, 446 mAnm Mekat/Ligocki; EuGH ZD 2024, 150 mAnm Ligocki/Sosna = MMR 2024, 231 mAnm Kohl/Rothkegel und LG Mainz ZD 2022, 163.