BRANDI
RECHTSANWÄLTE

RECHTLICHE UND TECHNISCHE ANFORDERUNGEN AN DEN ELEKTRONISCHEN

VERSAND VON RECHNUNGEN

Informationen zum Datenschutz I Juni 2025

English version

Einleitung

Mit dem Wachstumschancengesetz (BGBl. I 2024 Nr. 108) sind die umsatzsteuerrechtlichen Regelungen zur Ausstellung von Rechnungen im B2B-Bereich neu gefasst worden. Betroffen sind alle Umsätze, die ab dem 01.01.2025 anfallen und abgerechnet werden. Bereits nach der alten Rechtslage bestand die Rechtspflicht, für eine Leistung an einen anderen Unternehmer eine Rechnung innerhalb von sechs Monaten nach Ausführung der Leistung auszustellen, wenn der Umsatz nicht ausnahmsweise nach § 4 Nr. 8 bis 29 UStG steuerfrei war. Seit dem 1. Januar 2025 ist neu, dass der Gesetzgeber Unternehmer im B2B-Bereich verpflichtet, die Rechnungen als elektronische Rechnungen (im Folgenden: E-Rechnung) auszustellen. Vor diesem Begriff waren noch bis zum 31.12.2024 auch der Rechnungsversand per E-Mail (ggf. mit PDF-Anhang), die Bereitstellung der Rechnung in einem Onlineportal zum Download, die Übermittlung per elektronischem Datenaustausch (engl. Electronic Data Interchange bzw. EDI) sowie die Rechnungsübermittlung per Fax erfasst. Nunmehr hat der Begriff der elektronischen Rechnung bzw. E-Rechnung eine strengere Definition in § 14 Abs. 1 S. 3 UStG erfahren. Danach ist eine E-Rechnung eine Rechnung, die in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen wird und eine elektronische Verarbeitung ermöglicht. Werden Rechnungen hingegen in einem elektronischen Format, das diesen Anforderungen nicht genügt, beispielsweise als PDF-Anhang per E-Mail, oder auf Papier per Brief übermittelt, handelt es sich nicht um E-Rechnungen im oben genannten Sinne, sondern um „sonstige Rechnungen“ im Sinne des § 14 Abs. 1 S. 4 UStG. Im nachfolgenden Beitrag soll aufgeschlüsselt werden, welche Implikationen sich aus diesen Änderungen für Unternehmen ergeben und welchen Sicherheitsanforderungen der elektronische Versand von Rechnungen nunmehr genügen muss.

Die Verpflichtung zur elektronischen Rechnungsstellung im B2B-Bereich

Unternehmer sind berechtigt eine Rechnung auszustellen, wenn sie im Inland im Rahmen Ihres Unternehmens eine Lieferung oder eine sonstige Leistung gegen Entgelt ausführen, § 14 Abs. 2 S. 1 UStG. Die Verpflichtung zur Ausstellung einer E-Rechnung im B2B-Bereich folgt aus § 14 Abs. 3 S. 2 UStG. Von dieser Verpflichtung unberührt bleiben – zumindest vorerst – Umsätze an Unternehmer im Ausland sowie an Endverbraucher. Wie bisher auch müssen gemäß § 14 Abs. 3 S. 1 UStG sowohl für E-Rechnungen wie auch für sonstige Rechnungen die Echtheit der Herkunft der Rechnung, die Unversehrtheit ihres Inhalts und ihre Lesbarkeit gewährleistet sein. Unternehmer bleiben damit dafür verantwortlich, dass die Sicherheit der Identität des Rechnungsausstellers gewahrt bleibt sowie die nach dem UStG erforderlichen Angaben nicht (nachträglich) geändert werden. Die Art und Weise, wie diese Ziele zu erreichen sind, stellt das Gesetz den Unternehmern frei, § 14 Abs. 3 S. 4 UStG. Jegliche innerbetriebliche Kontrollverfahren, die einen verlässlichen Prüfpfad zwischen Rechnung und Leistung schaffen können, sollen zulässig sein, § 14 Abs. 3 S. 5 UStG. Bei der Übermittlung einer E-Rechnung gelten gem. § 14 Abs. 3 S. 6 UStG die Echtheit der Herkunft und die Unversehrtheit des Inhalts als gewährleistet, wenn eine qualifizierte elektronische Signatur oder ein zulässiges EDI-Verfahren verwendet werden. Jedenfalls für E-Rechnungen im Sinne des § 14 Abs. 1 S. 3 UStG ist das UStG mithin nicht mehr auf eine bestimmte Technologie festgelegt, sondern insoweit technologieoffen formuliert. Eine vergleichbare Bestimmung für „sonstige Rechnungen“ im Sinne des § 14 Abs. 1 S. 4 UStG ergibt sich aus dem UStG hingegen nicht.

Die elektronische Übermittlung einer E-Rechnung mit einer qualifizierten elektronischen Signatur gem. § 14 Abs. 3 S. 6 Nr. 1 UStG

Ebenso verzichtet der Gesetzgeber darauf, den Begriff der „qualifizierten elektronischen Signatur“ in § 14 Abs. 3 S. 6 Nr. 1 UStG zu definieren, sodass auf die Definition in der eIDAS-Verordnung (Elektronische-Transaktionen-VO) zurückgegriffen werden muss (vgl. BT-Drs. 18/12494, S. 49). Unter einer „elektronischen Signatur“ versteht man Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet, Art. 3 Nr. 10 eIDAS-VO. Eine „qualifizierte elektronische Signatur“ ist gemäß Art. 3 Nr. 12 eIDAS-VO eine „fortgeschrittene elektronische Signatur“, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht. Die Anforderungen an eine „fortgeschrittene elektronische Signatur“ folgen gem. Art. 3 Nr. 11 eIDAS-VO wiederum aus Art. 26 Abs. 1 eIDAS-VO. Danach muss eine fortgeschrittene elektronische Signatur eindeutig dem Unterzeichner zugeordnet werden können, seine Identifizierung ermöglichen, unter Verwendung elektronischer Signaturerstellungsdaten erstellt worden sein, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann, und so mit den auf diese Weise unterzeichneten Daten verbunden sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Damit eine fortgeschrittene elektronische Signatur auch die weite-

ren Voraussetzungen für eine „qualifizierte elektronische Signatur" i.S.d. Art. 3 Nr. 12 eIDAS-VO erfüllen kann, bedarf es eines durch einen qualifizierten Vertrauensdiensteanbieter ausgestellten qualifizierten Zertifikates. Eine Übersicht qualifizierter Vertrauensdiensteanbieter findet sich auf der Webseite der Europäischen Kommission (Vertrauenswürdige EU-Listen).

Die elektronische Übermittlung einer E-Rechnung mit Hilfe von EDI-Verfahren gem. § 14 Abs. 3 S. 6 Nr. 2 UStG

Abweichend von § 14 Abs. 1 und 2 UStG kann eine Rechnung bis zum 31.12.2027 für einen nach dem 31.12.2026 und vor dem 01.01.2028 ausgeführten Umsatz vorbehaltlich der Zustimmung des Empfängers in einem elektronischen Format, das nicht § 14 Absatz 1 Satz 6 UStG entspricht, ausgestellt werden, wenn diese mittels elektronischem Datenaustausch (EDI) nach Artikel 2 der Empfehlung 94/820/EG der Kommission vom 19. Oktober 1994 über die rechtlichen Aspekte des elektronischen Datenaustausches (ABl. L 338 vom 28.12.1994, S. 98) übermittelt wird, § 27 Abs. 38 S. 1 Nr. 3 UStG.

Voraussetzung für die Anerkennung von im EDI-Verfahren übermittelten Rechnungen ist, dass über den elektronischen Datenaustausch eine Vereinbarung zwischen dem Rechnungsaussteller und dem Rechnungsempfänger nach Artikel 2 der zuvor benannten Kommissionsempfehlung vom 19. Oktober 1994 besteht, in der der Einsatz von Verfahren vorgesehen ist, die die Echtheit der Herkunft und die Unversehrtheit der Daten gewährleisten, Klausel 14.4 Abs. 9 UStAE (Umsatzsteuer-Anwendungserlass). Im Anhang zu der Kommissionsempfehlung vom 19. Oktober 1994 findet sich auch eine entsprechende EDI-Mustervereinbarung, die in ihrem Art. 6 Sicherheitsverfahren zur Überprüfung des Ursprungs und der Integrität enthält, die im technischen Anhang näher aufgeführt sind.

Datenschutzrechtliche Anforderungen an den elektronischen Versand von Rechnungen im B2C-Bereich

Gegenüber Endkunden sind anders als im elektronischen Geschäftsverkehr gegenüber anderen Unternehmen neben umsatzsteuerrechtlichen auch datenschutzrechtliche Bestimmungen zu beachten. Insbesondere wegen des Risikos einer Manipulation von elektronisch versandten Rechnungen durch kriminell handelnde Dritte ist die Frage zu stellen, welche technischen und organisatorischen Maßnahmen zu etablieren sind, bevor Rechnungen auch gegenüber Endkunden auf elektronischem Wege versandt werden können.

Mit Art. 32 Abs. 1 DSGVO werden, wenn und soweit personenbezogene Daten verarbeitet werden, in diesem Zusammenhang sowohl gewisse Voraussetzungen aufgestellt, als auch ein Sorgfaltsmaßstab für die verantwortlichen Stellen formuliert. Danach haben Verantwortliche und Auftragsverarbeiter unter der Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese offene Formulierung bietet Orientierung, erlaubt aber nicht den Schluss, welche konkreten Sicherheitsmaßnahmen im Einzelnen beim elektronischen Versand von Rechnungen im B2C-Bereich zu implementieren sind. Mangels höchstrichterlicher Rechtsprechung ist diese Frage in der Vergangenheit von unterschiedlichen Gerichten auch durchaus unterschiedlich bewertet worden.

OLG Schleswig, Urteil vom 18.12.2024 – Az.: 12 U 9/24: Ende-zu-Ende-Verschlüsselung sei zurzeit das Mittel der Wahl

Strenge Anforderungen sind insbesondere vom OLG Schlesweig in seinem Urteil vom 18.12.2024 (Az.: 12 U 9/24) formuliert worden. Die Klägerin, die ein Unternehmen für Haustechnik betreibt, hatte sich im Oktober 2021 mit der Beklagten über einen Bauvertrag geeinigt, in dessen Rahmen die Klägerin mit der Installation von Heizungsanlagen in einem Doppelhaus beauftragt wurde. Nach Durchführung der geplanten Intallationsarbeiten rechnete die Klägerin die erbrachten Leistungen gegenüber der Beklagten in drei Abschlagszahlungen ab. Die Rechnungen wurden jeweils als PDF-Datei einer E-Mail anbei gehängt und an die Klägerin versandt. Die Beklagte wies die ersten beiden Abschlagsrechnungen an die auf den Rechnungen angegebenen Bankverbindungen der Klägerin an. Die E-Mail mit der dritten Abschlagsrechnung in Höhe von 15.385,78 EUR die zugleich die Schlussrechnung darstellte, ist jedoch auf ungeklärte Weise von einem Dritten abgefangen und manipuliert worden. Abweichend von den vorherigen Rechnungen enthielt sie daher die Kontoverbindung eines unbekannten Dritten bei einer ausländischen Neo- bzw. Onlinebank. Mit Ausnahme der IBAN war außerdem auch die farbliche Gestaltung erheblich verändert worden und im Abschnitt der Bankverbindung fehlten im Unterschied zu den vorherigen Rechnungen der QR-Code, das Siegel, die Angaben zum Geschäftsführer, die Steuernummer sowie das Wasserzeichen im Hintergrund des Rechnungstextes. Dies hielt die Beklagte trotzdem nicht davon ab, den Rechnungsbetrag auf das in der dritten Abschlagsrechnung aufgeführte Konto des unbekannten Dritten zu überweisen. Die Klägerin konnte auf ihrem Konto dahingegen keinen Zahlungseingang verzeichnen, sodass Sie nach Rückfrage bei der Klägerin auf Zahlung klagte. Die Parteien stritten also darüber, ob die Klägerin die (erneute) Zahlung ihrer Werklohnforderung in Höhe von 15.385,78 EUR von der Beklagten verlangen kann, nachdem der Überweisungsbetrag nach Manipulation der Rechnung durch kriminell handelnde Dritte dem Konto eines Unbekannten gutgeschrieben wurde. In diesem Rahmen brachte die Klägerin insbesondere vor, dass sie sämtliche E-Mails per SMTP (Simple Mail Transfer Protocol) über TLS (Transport Layer Security) transportverschlüsselt und damit ausreichend abgesichert habe. Ferner habe sie nach Bekanntwerden der Manipulation ihre Computersysteme überprüfen lassen, wobei keine Sicherheitslücke in ihren E-Mail-Accounts festgestellt worden sei. Ihrer Ansicht nach müsse sich die Manipulation daher in der Sphäre der Beklagten ereignet haben. Dahingegen habe sie keine Ende-zu-Ende-Verschlüsselung (E2E) eingesetzt, die statt der Verbindung die Daten selbst (in unserem Fall die E-Mails) verschlüsselt hätte, bevor diese von der Senderin an die Empfängerin versandt werden. Dazu hätte allerdings sowohl auf Seiten der Klägerin wie auf Seiten der Beklagten die Ende-zu-Ende-Verschlüsselung eingerichtet und das jeweilige Schlüsselpaar ausgetauscht werden müssen. Während in der Instanz das Landgericht Kiel daher noch zu Gunsten der Klägerin entschieden und die Beklagte zu einer erneuten Zahlung verurteilt hatte (LG Kiel, Urt. v. 29.12.2023 – 9 O 110/23), hob das OLG Schleswig das landgerichtliche Urteil mit der Begründung auf, dass der Beklagten in Folge der fehlenden Ende-zu-Ende-Verschlüsselung ein Schadensersatzanspruch in Höhe der auf das Drittkonto getätigten Überweisung aus Art. 82 Abs. 1 DSGVO zustehe, den sie dem Anspruch der Klägerin entgegenhalten könne. Jedenfalls solle dies dann gelten, wenn durch Verfälschung der Rechnung hohe finanzielle Risiken auf Seiten des Kunden bestünden. Daher müsse die Beklagte im streitgegenständlichen Fall nicht erneut zahlen. Dabei ließ das OLG Schleswig unberücksichtigt, dass die in der konkreten Rechnung enthaltenen personenbezogene Daten des Kunden (Name, Anschrift, Kunde der Klägerin, offene Rechnung über eine Werkleistung) datenschutzrechtlich wohl als risikoarm zu qualifizieren sind und mit der IBAN ein Datum des Unternehmens verändert worden war, das gerade nicht in den sachlichen Anwendungsbereich der DSGVO fällt. Insoweit hat das OLG Schleswig stattdessen ausreichen lassen, dass bei der unbefugten Manipulation der Kontoverbindung der Klägerin gleichzeitig auch unbefugt auf die Daten der Beklagten zugegriffen werden konnte.

Den Art. 32 DSGVO legte das Gericht dahingehend aus, dass unter den aktuell möglichen und gebräuchlichen Verschlüsselungsmethoden für den Email-Versand zwar grundsätzlich sowohl die Punkt-zu-Punkt bzw. Transportverschlüsselung (z.B. SMTP über TLS) als auch die Ende-zu-Ende-Verschlüsselung in Betracht kämen, bei ersterem aber die Gefahr bestünde, dass Internetkriminelle einen „Man-in-the-Middle-Angriff" durchführten, der auf die unterschiedliche Knotenpunkte im Web zwischen den Servern der E-Mail-Anbieter von Versender und Empfänger angelegt sei, und damit ohne deren Wissen Daten (z.B. E-Mails) abfangen, kopieren oder verändern könnten. Einem „Man-in-the-Middle-Angriff" – von dem das Gericht ohne nähere Begründung auszugehen scheint – könne man nur mit einer Ende-zu-Ende-Verschlüsselung begegnen. Das OLG Schleswig hebt in diesem Rahmen hervor, dass anders als bei der Transportverschlüsselung bei der Ende-zu-Ende-Verschlüsselung nicht die einzelnen Abschnitte des Versandkanals, sondern die E-Mails selbst verschlüsselt seien. Derart verschlüsselte E-Mails könnten – so das OLG Schleswig – nur im Klartext gelesen werden, wenn Sender und Empfänger über den notwendigen Schlüssel verfügen. Ohne diesen Schlüssel könnten dahingegen weder die beteiligten E-Mail-Anbieter noch potentielle Angreifer die E-Mails unterwegs lesen oder manipulieren. Für das Gericht steht damit fest, dass nur die Ende-zu-Ende-Verschlüsselung die drei Ziele der Verschlüsselung im Internet (Vertraulichkeit, Authentizität, Integrität) wahren könne. Nach der Rechtsauffassung des OLG Schleswig biete vor dem Hintergrund der allgemein bekannten und vielfältig veröffentlichten Hackermöglichkeiten, des gerichtsbekannt rasanten Anstiegs von Hackerangriffen und der im Einzelfall weitreichenden finanziellen Folgen für den einzelnen Kunden, nur die Ende-zu-Ende-Verschlüsselung einen „geeigneten" Schutz im Sinne der DSGVO. Den dafür erforderlichen technischen und finanziellen Aufwand verlangt das OLG Schleswig auch von einem mittelständischen Handwerksbetrieb. Schließlich bestünde nach wie vor, soweit kein entsprechend hoher Standard zum Schutz der personenbezogenen Daten beim Versand von Emails mit angehängten Rechnungen sichergestellt werden könne, die Möglichkeit „wie eh und je" Rechnungen per Post zu versenden.

Das OLG Schleswig verkennt dabei allerdings, dass auch eine Ende-zu-Ende-Verschlüsselung die von ihm dargestellte Manipulation der Rechnung nicht hätte verhindern können, wenn die Manipulation nicht das Ergebnis eines technisch komplexen „Man-in-the-Middle-Angriffs", sondern schlichtweg Folge des womöglich kompromittierten Postkorbs des Empfängers gewesen war. Haben kriminelle Dritte Zugriff auf den Postkorb des Endkunden (sog. „Business-E-Mail-Compromise"-Angriff), verhindert regelmäßig auch die Ende-zu-Ende-Verschlüsselung nicht die Manipulation einer E-Mail. Vor dem Hintergrund, dass – anders als vom OLG Schleswig irrig angenommen – selbst bei einem nachgewiesenen Datenschutzverstoß nicht der Verantwortliche, sondern die betroffene Person als Anspruchsteller den von Art. 82 Abs. 1 DSGVO geforderten Kausalzusammenhang zwischen dem Verstoß und dem eingetretenen Schaden darlegen und beweisen muss, stellt dieses Risiko ohnehin kein Argument gegen den elektronischen Versand von Rechnungen im B2C-Bereich dar.

OLG Karlsruhe, Urteil vom 27.7.2023 – 19 U 83/22: Die erforderlichen Sicherheitsvorkehrungen bestimmen sich nach den berechtigten Sicherheitserwartungen unter Berücksichtigung der Zumutbarkeit

Einen gelungeneren Sorgfaltsmaßstab für den elektronischen Versand von Rechnungen formuliert das OLG Karlsruhe in seiner Entscheidung vom 27.07.2023 (Az.: 19 U 83/22). Der Sachverhalt ist dabei im Wesentlichen mit demjenigen im vorherigen Urteil des OLG Schleswigs vergleichbar, spielt sich aber abweichend von diesem ausschließlich im B2B-Bereich ab. Sowohl der Kläger wie auch der Beklagte sind also Unternehmer, sodass das OLG Karlsruhe in seiner Entscheidung davon ausgeht, dass keine personenbezogenen Daten verarbeitet werden und der sachliche Anwendungsbereich der DSGVO nicht eröffnet ist (Art. 2 Abs. 1 DSGVO).

Das Gericht führt in seiner Begründung allerdings aus, dass – anders als noch vom LG Mosbach mit Urteil vom 24.05.2022 (Az.: 1 O 271/21) erstinstanzlich angenommen – der Art. 32 Abs. 1 DSGVO ohnehin nicht zwingend die Verwendung einer Ende-zu-Ende-Verschlüsselung voraussetze, sondern eine Ende-zu-Ende-Verschlüsselung insoweit nur „in der Abwägung der notwendigen Maßnahmen berücksichtigt" werden müsse und allenfalls in den Fällen ein „Muss" darstelle, in denen der Bruch der Vertraulichkeit ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen berge und nicht anders abgewendet werden könne. In allen anderen Fällen müsse sich der Sorgfaltsmaßstab beim Versand von E-Mails im geschäftlichen Verkehr, insbesondere hinsichtlich Art und Umfang der erforderlichen Sicherheitsvorkehrungen, soweit hierzu von den Parteien keine ausdrücklichen Vereinbarungen getroffen worden seien, an den berechtigten Sicherheitserwartungen der maßgeblichen Verkehrskreise unter Berücksichtigung der Zumutbarkeit orientieren. Im streitgegenständlichen Fall habe die Beklagte aber schon selbst nicht angenommen, dass eine Verschlüsselung von PDF-Dateien im geschäftlichen Verkehr (ausgenommen vom Austausch besonders sensibler Daten wie Betriebs- oder Geschäftsgeheimnisse) üblich sei. Schließlich seien zwischen den Vertragsparteien auch weder etwaige Passwörter ausgetauscht worden, noch habe die streitgegenständliche Datei den Eindruck erweckt, dass sie durch eine Verschlüsselung besonders gesichert sei. Das BSI empfehle für E-Mails zwar die Ende-zu-Ende-Verschlüsselung, äußerte aber gleichzeitig die Einschätzung, dass diese bisher nur sehr selten eingesetzt werde und damit mangels der entsprechenden allgemeinen Sicherheitserwartung des Verkehrs auch nicht zu erwarten sei. Dahingegen ist eine Transportverschlüsselung üblich und regelmäßig auch als Standard bei den üblichen E-Mail-Providern eingerichtet. Sie ist mithin jeder verantwortlichen Stelle nicht nur zuzumuten, sondern wird im elektronischen Geschäftsverkehr zu erwarten sein.

Fazit

Der elektronische Versand von Rechnungen setzt nicht zwingend eine Ende-zu-Ende-Verschlüsselung oder andere spezifische Sicherheitsmaßnahmen voraus. Vielmehr lässt Art. 32 Abs. 1 DSGVO auch andere „geeignete" technische und organisatorische Maßnahmen zu. Neben einer sicheren E-Mail-Verschlüsselung, können neben einer Transportverschlüsselung beispielsweise auch digitale Signaturen zum Einsatz kommen. Hinzukommt, dass Kunden immer auf die Möglichkeit, dass Rechnungen manipuliert sein können, aufmerksam gemacht werden sollten. Nur wenn und soweit hohe Risiken für die Rechte und Freiheiten natürlicher Personen bestehen, wird von der datenschutzrechtlich verantwortlichen Stelle die Wahl weiterer Sicherheitsmaßnahmen zu erwarten sein. Neben einer Ende-zu-Ende-Verschlüsselung kann dabei allerdings auch an alternative Übertragungswege wie ein sicheres Kundenportal gedacht werden. Im B2B-Bereich besteht darüber hinaus die Möglichkeit sich bereits vertraglich auf einen bestimmten Sicherheitsstandard im elektronischen Geschäftsverkehr zu einigen. Regelmäßig ist dies auch zu empfehlen. Habib Majuno

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Habib Majuno
Wissenschaftlicher Mitarbeiter

T +49 521 96535 - 890
F +49 521 96535 - 113
E habib.majuno@brandi.net