BRANDI
RECHTSANWÄLTE

LEGAL AND TECHNICAL REQUIREMENTS FOR

SENDING INVOICES ELECTRONICALLY

Information on data protection I June 2025

Introduction

With the Growth Opportunities Act (Federal Law Gazette I 2024 No. 108), the VAT regulations for issuing invoices in the B2B sector have been revised. All sales that occur and are invoiced from 1 January 2025 on are affected. Under the old legal situation, there was already a legal obligation to issue an invoice for a service to another entrepreneur within six months of the service being performed if the transaction was not tax-exempt under Section 4 Nos. 8 to 29 UStG. Since 1 January 2025, the legislator has obliged entrepreneurs in the B2B sector to issue invoices as electronic invoices (hereinafter: e-invoices). Until 31 December 2024, this term also covered the sending of invoices by email (with a PDF attachment if necessary), the provision of the invoice in an online portal for downloading, the transmission by electronic data interchange (EDI) and the transmission of invoices by fax. The term electronic invoice or e-invoice has now been given a stricter definition in Section 14 (1) (3) UStG. According to this, an e-invoice is an invoice that is issued, transmitted and received in a structured electronic format and enables electronic processing. However, if invoices are sent in an electronic format that does not fulfil these requirements, for example as a PDF attachment by email or on paper by letter, they are not e-invoices as defined above, but "other invoices" within the meaning of Section 14 (1) (4) UStG.

The following article will analyse the implications of these changes for companies and the security requirements that electronic invoicing must now meet.

The obligation to issue invoices electronically in the B2B sector

Entrepreneurs are authorised to issue an invoice if they carry out a delivery or other service in return for payment in Germany as part of their business, Section 14 (2) (1) UStG. The obligation to issue an e-invoice in the B2B area follows from Section 14 (3) (2) UStG. This obligation does not affect – at least for the time being – sales to entrepreneurs abroad and to end consumers. As before, the authenticity of the origin of the invoice, the integrity of its content and its legibility must be guaranteed for both e-invoices and other invoices in accordance with Section 14 (3) (1) UStG. Entrepreneurs therefore remain responsible for ensuring that the identity of the invoice issuer remains secure and that the information required under the UStG is not (subsequently) changed. The way in which these objectives are to be achieved is left to the entrepreneurs' discretion by the law, Section 14 (3) (4) UStG. Any internal control procedures that can create a reliable audit trail between the invoice and the service should be permitted, Section 14 (3) (5) UStG. When transmitting an e-invoice, the authenticity of the origin and the integrity of the content are deemed to be guaranteed if a qualified electronic signature or an authorised EDI procedure is used, in accordance with Section 14 (3) (6) UStG. At least for e-invoices within the meaning of Section 14 (1) (3) UStG, the UStG is therefore no longer limited to a specific technology, but is formulated in a technology-open manner. However, the UStG does not contain a comparable provision for "other invoices" within the meaning of Section 14 (1) (4) UStG.

The electronic transmission of an e-invoice with a qualified electronic signature in accordance with Section 14 (3) (6) no. 1 UStG

The legislator also refrains from defining the term "qualified electronic signature" in Section 14 (3) (6) no. 1 UStG, so that the definition in the eIDAS Regulation (Electronic Transactions Regulation) must be used (see BT-Drs. 18/12494, p. 49). An "electronic signature" is data in electronic form which is attached to or logically associated with other electronic data and which the signatory uses to sign, Art. 3 No. 10 eIDAS Regulation. A "qualified electronic signature" is an "advanced electronic signature" that has been created by a qualified electronic signature creation device and is based on a qualified certificate for electronic signatures in accordance with Art. 3 No. 12 eIDAS Regulation. The requirements for an "advanced electronic signature" in accordance with Art. 3 No. 11 eIDAS Regulation in turn follow from Art. 26 (1) eIDAS Regulation. According to this, an advanced electronic signature must be clearly attributable to the signatory, enable the signatory to be identified, have been created using electronic signature creation data that the signatory can use with a high degree of confidence under his sole control, and be linked to the data signed in this way in such a way that any subsequent modification of the data can be recognised. In order for an advanced electronic signature to fulfil the further requirements for a "qualified electronic signature" within the meaning of Art. 3 No. 12 eIDAS Regulation, a qualified certificate issued by a qualified trust service provider is required. An overview of qualified trust service providers can be found on the website of the European Commission (Trusted EU lists).

The electronic transmission of an e-invoice using EDI procedures in accordance with Section 14 (3) (6) no. 2 UStG

By way of derogation from Section 14 (1) and (2) UStG, an invoice may be issued until December 31, 2027 for a transaction carried out after December 31, 2026 and before January 1, 2028, subject to

the recipient's consent, in an electronic format that does not comply with Section 14 (1) (6) UStG if it is transmitted by means of electronic data interchange (EDI) in accordance with Article 2 of Commission Recommendation 94/820/EC of October 19, 1994 on the legal aspects of electronic data interchange (OJ L 338, 28.12.1994, p. 983 UStG), Section 27 (38) (1) no. 1 no. 3 UStG.
The prerequisite for the recognition of invoices transmitted using the EDI procedure is that there is an agreement between the invoice issuer and the invoice recipient regarding the electronic data exchange in accordance with Article 2 of the aforementioned Commission Recommendation of 19 October 1994, which provides for the use of procedures that guarantee the authenticity of the origin and the integrity of the data, clause 14.4 (9) UStAE (Value Added Tax Application Decree). The annex to the Commission Recommendation of 19 October 1994 also contains a corresponding EDI model agreement, Article 6 of which contains security procedures for verifying origin and integrity, which are listed in more detail in the technical annex.

Data protection requirements for the electronic dispatch of invoices in the B2C sector

In contrast to electronic business transactions with other companies, data protection regulations must be observed in addition to VAT regulations when dealing with end customers. In particular due to the risk of manipulation of electronically sent invoices by criminally acting third parties, the question must be asked as to which technical and organisational measures must be established before invoices can also be sent electronically to end customers.
If and insofar as personal data is processed, Art. 32 (1) GDPR sets out certain requirements in this context and formulates a standard of care for the responsible parties. Accordingly, controllers and processors must take appropriate technical and organisational measures to ensure a level of protection appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. This open formulation provides guidance, but does not allow the conclusion to be drawn as to which specific security measures must be implemented in detail when sending invoices electronically in the B2C sector. In the absence of supreme court rulings, this question has also been assessed differently by different courts in the past.

OLG Schlesweig, judgement of 18.12.2024 – Ref.: 12 U 9/24: End-to-end encryption is currently the method of choice

Strict requirements have been formulated in particular by the Higher Regional Court of Schleswig in its judgement of 18 December 2024 (Ref.: 12 U 9/24). The plaintiff, which operates a building services company, had agreed a construction contract with the defendant in October 2021, under which the plaintiff was commissioned to install heating systems in a semi-detached house. After carrying out the planned installation work, the plaintiff invoiced the defendant for the services rendered in three instalments. The invoices were each attached to an email as a PDF file and sent to the plaintiff. The defendant sent the first two instalment invoices to the bank details of the plaintiff indicated on the invoices. However, the email with the third instalment invoice in the amount of EUR 15,385.78, which was also the final invoice, was intercepted and manipulated by a third party in an unexplained manner. In contrast to the previous invoices, it therefore contained the account details of an unknown third party at a foreign neo- or online bank. With the exception of the IBAN, the colour design had also been significantly changed and, in contrast to the previous invoices, the QR code, the seal, the details of the managing director, the tax number and the watermark in the background of the invoice text were missing in the bank details section. Nevertheless, this did not prevent the defendant from transferring the invoice amount to the account of the unknown third party listed in the third instalment invoice. The plaintiff, on the other hand, was unable to register receipt of payment on her account, so that she filed a claim for payment after enquiring with the plaintiff. The parties therefore disputed whether the plaintiff could demand (renewed) payment of its claim for payment for work in the amount of EUR 15,385.78 from the defendant after the transfer amount was credited to the account of an unknown party following manipulation of the invoice by third parties acting criminally. In this context, the plaintiff argued in particular that it had transport-encrypted all e-mails via SMTP (Simple Mail Transfer Protocol) using TLS (Transport Layer Security) and thus sufficiently secured them. Furthermore, she had her computer systems checked after becoming aware of the manipulation and no security vulnerability had been found in her email accounts. In her opinion, the manipulation must therefore have occurred in the sphere of the defendant. On the other hand, she had not used end-to-end encryption (E2E) which would have encrypted the data itself (in our case the emails) instead of the connection before it was sent from the sender to the recipient. However, this would have required both the plaintiff and the defendant to set up end-to-end encryption and exchange the respective key pair.
While the Regional Court of Kiel therefore ruled in favour of the plaintiff at first instance and ordered the defendant to make a new payment (Regional Court of Kiel, judgement of 29.12.2023 – 9 O 110/23), the Higher Regional Court of Schleswig overturned the Regional Court judgement on the grounds that the defendant was entitled to a claim for damages in the amount of the transfer made to the third-party account under Art. 82 (1) GDPR as a result of the lack of end-to-end encryption, which it could hold against the plaintiff's claim. In any case, this should apply if there are high financial risks on the part of the customer due to falsification of the invoice. Therefore, the defendant did not have to pay again in the case in dispute. The Higher Regional Court of Schleswig did not take into account the fact that the personal data of the customer contained in the specific invoice (name, address, customer of the plaintiff, outstanding invoice for a work service) can probably be qualified as low-risk under data protection law and that the IBAN was a date of the company that had been changed, which does not fall within the material scope of the GDPR. In this respect, the Higher Regional Court of Schleswig instead allowed it to suffice that the unauthorised manipulation of the plaintiff's account details also enabled unauthorised access to the defendant's data.
The court interpreted Art. 32 GDPR to mean that, of the currently possible and commonly used encryption methods for sending emails, both point-to-point or transport encryption (e.g. SMTP via TLS) and end-to-end encryption could be considered, but there is a risk with the former that cyber criminals could carry out a "man-in-the-middle attack", which is designed for the various nodes on the web between the servers of the email providers of the sender and recipient, and could therefore intercept, copy or change data (e.g. emails) without their knowledge. A "man-in-the-middle attack" – which the court seems to assume without further justification – can only be countered with end-to-end encryption. In this context, the Higher Regional Court of Schleswig emphasises that, unlike transport encryption, end-to-end encryption does not encrypt the individual sections of the sending channel, but the emails themselves. According to the Higher Regional Court of Schleswig, emails encrypted in this way can only be read in plain text if the sender and recipient have the necessary key. Without this key, however, neither the email providers involved nor potential attackers could read or manipulate the emails en route. For the court, it is therefore clear that only end-to-end encryption can fulfil the three objectives of encryption on the internet (confidentiality, authenticity, integrity). According to the legal opinion of the Higher Regional Court of Schleswig, in light of the generally known and widely publicised

hacking possibilities, the rapid increase in hacker attacks known to the courts and the far-reaching financial consequences for individual customers in individual cases, only end-to-end encryption offers "suitable" protection within the meaning of the GDPR. The Higher Regional Court of Schleswig also requires the necessary technical and financial effort from a medium-sized craft business. Finally, if no correspondingly high standard of protection of personal data can be ensured when sending emails with attached invoices, it would still be possible to send invoices by post "as always".

However, the Higher Regional Court of Schleswig fails to recognise that even end-to-end encryption could not have prevented the manipulation of the invoice it described if the manipulation was not the result of a technically complex "man-in-the-middle attack", but simply the result of the recipient's mailbox possibly being compromised. If criminal third parties have access to the end customer's inbox (a so-called "business email compromise" attack), end-to-end encryption does not regularly prevent the manipulation of an email. In view of the fact that – contrary to the erroneous assumption by the Higher Regional Court of Schleswig – even in the event of a proven data protection breach, it is not the controller but the data subject as the claimant who must demonstrate and prove the causal link between the breach and the damage that has occurred as required by Art. 82 (1) GDPR, this risk does not constitute an argument against the electronic sending of invoices in the B2C sector anyway.

OLG Karlsruhe, judgement of 27.7.2023 – 19 U 83/22: The necessary safety precautions are determined by the justified safety expectations, taking into account reasonableness

The Higher Regional Court of Karlsruhe, in its decision of 27 July 2023 (case no.: 19 U 83/22), formulated a more successful standard of care for the electronic sending of invoices. The facts of the case are essentially comparable to those in the previous judgement of the Higher Regional Court of Schleswig, but, in contrast to the latter, the case takes place exclusively in the B2B sector. Both the plaintiff and the defendant are therefore entrepreneurs, so that the Higher Regional Court of Karlsruhe assumes in its decision that no personal data is processed and that the material scope of application of the GDPR is not opened (Art. 2 (1) GDPR).

In its reasoning, however, the court states that – contrary to what the Mosbach Regional Court judgement of 24 May 2022 (Ref.: 1 O 271/21) assumed at first instance – Art. 32 (1) GDPR does not necessarily require the use of end-to-end encryption anyway, but that end-to-end encryption only has to be "taken into account in the consideration of the necessary measures" and is only a "must" in cases where the breach of confidentiality poses a high risk to the rights and freedoms of the natural persons concerned and cannot be averted in any other way. In all other cases, the standard of care when sending e-mails in the course of business, in particular with regard to the type and scope of the necessary security precautions, must be based on the legitimate security expectations of the relevant public, taking into account reasonableness, unless the parties have expressly agreed otherwise. In the case at issue, however, the defendant itself had not assumed that the encryption of PDF files in business transactions (with the exception of the exchange of particularly sensitive data such as trade or business secrets) was customary. Finally, no passwords were exchanged between the contracting parties, nor did the file in dispute give the impression that it was particularly secured by encryption. Although the BSI recommends end-to-end encryption for emails, it also stated that this has only been used very rarely to date and is therefore not to be expected due to the lack of a corresponding general security expectation on the part of the public. On the other hand, transport encryption is common and is also regularly set up as standard with the usual email providers. It is therefore not only to be expected of every responsible body, but is also to be expected in electronic business transactions.

Conclusion

The electronic sending of invoices does not necessarily require end-to-end encryption or other specific security measures. Rather, Art. 32 (1) GDPR also permits other "appropriate" technical and organisational measures. In addition to secure email encryption, digital signatures can also be used alongside transport encryption, for example. In addition, customers should always be made aware of the possibility that invoices may be manipulated. Only if and insofar as there are high risks to the rights and freedoms of natural persons will the data controller be expected to choose additional security measures. In addition to end-to-end encryption, alternative transmission channels such as a secure customer portal can also be considered. In the B2B sector, it is also possible to contractually agree on a certain security standard for electronic business transactions. This is also regularly recommended. Habib Majuno

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Habib Majuno
Research Associate

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