EMBRACING PAPERLESS TRADE

BEST PRACTICE GUIDE ON ELECTRONIC CONTRACTING

International Federation of Freight Forwarders Associations

The global voice of freight logistics

FIATA INTERNATIONAL FEDERATION OF FREIGHT FORWARDERS ASSOCIATIONS

FIATA is a non-governmental, membership-based organisation representing freight forwarders in some 150 countries. FIATA is a reference source on international policies and regulations governing the freight forwarding and logistics industry. FIATA works at the international level to represent service providers who operate in trade logistics and supply chain management. Through its FIATA documents and forms, congress, training and publications, and engagement with relevant international organisations, it promotes trade facilitation and best practices among the freight forwarding community.

Founded in Vienna, Austria, on 1926, FIATA owes its name to its French acronym (*Fédération Internationale des Associations de Transitaires et Assimilés*) and is known as 'the global voice of freight logistics'. FIATA is headquartered in Geneva, Switzerland.

DISCLAIMER

For further information about the activities of the FIATA Advisory Body on Legal Matters or to make comments about this guide, please contact the FIATA Headquarters at **legal@fiata.org**

Photos: Marharyta Marko from iStock (front cover); Vitali Michkou from Dreamstime (back cover)

CONTENTS

1. INTRODUCTION

1.1 Electronic contracting is no longer merely an option

It is increasingly common for freight forwarders to conduct their relations with clients/providers, including the conclusion of contracts, partly or wholly by electronic or digital means. This may be for a variety of reasons:

- *In relations with contractors* (e.g. carriers or other service providers or subcontractors): this may be something already "imposed" by service providers.
- *In relations with clients* (including shippers and consignees): this is in principle a decision that is rather under the forwarder's control, but is likely to be an important commercial factor to remain competitive.

In other words, electronic contracting is no longer an option, and companies should be prepared for this if they want to remain competitive. Various considerations come into play when conducting legal relations through digital means. From a legal point of view, the relevant point is whether contracts concluded and/or performed through digital means are valid, binding and enforceable.

1.2 What this best practice guide covers

This best practice guide has been developed by FIATA's Advisory Body on Legal Matters to provide best practices when contracting by electronic means throughout the process. It takes into account various practices around the world from a global perspective and provides practical tips to consider when using electronic contracts.

It should be noted that this best practice guide does not address electronic negotiable trade documents, such as negotiable bills of lading, which are subject to a number of other unique considerations.

This best practice guide should not be construed as legal advice in any way and freight forwarders are advised to seek their own independent legal advice and contact their local freight forwarding association for guidance, in accordance with their own local context.

2. WHAT IS ELECTRONIC CONTRACTING?

2.1 Electronic contracts

An **electronic contract** is a legally binding agreement between two or more parties that is formed and executed using electronic means. Often, it will be exchanged between the parties via email, online forms, or other electronic contracting platforms.

2.2 Signature and authentication: Electronic vs digital signatures

Electronic contracts are generally executed through the use of **electronic signatures**, which provide an electronic indication of a person's intent to agree to the content of a document or a set of data to which the signature relates. This can include typing one's name into a document, using a mouse or other pointing device to sign your name on a touch screen, or using a software programme that creates an electronic image of a signature. Electronic signatures are typically considered legally binding in most jurisdictions, but they may not provide the same level of security and authenticity as a digital signature.

In order to ensure greater security and authenticity, a **digital signature** may be used instead. A digital signature uses **Public Key Infrastructure (PKI)** technology to ensure the authenticity and integrity of the signature. PKI uses a pair of public and private keys to encrypt and decrypt the signature, thus providing a unique fingerprint. The private key is used to create the signature, and the public key is used to verify it. The process of signing a document with a digital signature includes the use of a certificate-based digital ID, which serves as a proof of identity for the signer. Digital signatures offer a higher level of security and are considered to be more tamper-proof than electronic signatures. They can be used as a seal, evidencing that the document has not been altered and is not subject to forgery.

3. BENEFITS OF ELECTRONIC CONTRACTING

There are several benefits to using electronic contracts, which have the potential to provide greater convenience, efficiency and security in the contracting process:

1. **Convenience:** Electronic contracts can be created, signed, and stored electronically, which means that they can be completed and executed quickly and easily, without the need for physical signatures or the printing and mailing of paper documents.

2. **Reduction in operational costs:** Electronic contracts can save time and money by eliminating the need for printing, mailing, and storing physical documents. They also reduce the need for travel and in-person meetings.

3. **Increased security:** Electronic contracts can be designed with built-in security features, such as encryption and digital signatures, which provide a higher security level and help to protect against fraud and tampering.

4. **Reduction in errors:** Electronic contracts can be designed to include built-in validation and error-checking, which can help to reduce errors and improve the accuracy of the information contained in the contract.

5. **Increased accessibility:** Electronic contracts can be stored and accessed electronically, which makes them more easily accessible and searchable, and allows for faster retrieval and review.

4. LEGAL RECOGNITION OF ELECTRONIC CONTRACTING AROUND THE WORLD

4.1 Frameworks recognising electronic contracting at the global level

Electronic contracting is recognised at the global level through a number of laws and regulations that have been put in place to ensure the legal validity and enforceability of electronic contracts and electronic signatures. At the international level, notable ones include:

UNCITRAL Model Law on Electronic Commerce (1996) (MLEC)

Adopted in 1996, the MLEC aims to enable the commercial use of modern means of communication and storage of information. It contains the first formulation of the three fundamental principles of technology neutrality, non-discrimination and functional equivalence in electronic media for paper-based concepts such as "writing", "signature" and "original". It also establishes rules for the formation and validity of contracts concluded electronically and for the attribution and retention of data messages.

Legislation based on or influenced by the Model Law has been adopted in 83 States and a total of 164 jurisdictions.

The text of the MLEC and the list of enacting states is available on the UNCITRAL website.

UNCITRAL Model Law on Electronic Signatures (2001) (MLES)

Adopted in 2001, the MLES aims at bringing additional legal certainty to the use of electronic signatures. It establishes criteria of technical reliability for the equivalence between electronic and hand-written signatures.

It follows a technology-neutral "two tier" approach, which avoids favouring the use of any specific software, method or product while attaching legal presumptions to more secure

signatures. In addition, it establishes rules for assessing the possible liability of signatories, relying parties and trusted service providers intervening in the signature process.

Legislation based on or influenced by the Model Law has been adopted in 38 States and a total of 39 jurisdictions.

The text of the MLES and the list of enacting states is available on the UNCITRAL website.

United Nations Convention on the Use of Electronic Communications in International Contracts (2005)

Adopted in 2005, the **United Nations Convention on the Use of Electronic Communications in International Contracts or "Electronic Communications Convention", or ECC** builds up on and updates the provisions of previous UNCITRAL texts. It aims at enhancing legal certainty and commercial predictability where electronic communications are used across borders by, among others:

- validating the legal status of cross-border electronic exchanges;
- preventing medium and technology discrimination;
- enabling the use of electronic communications in other treaties (e.g., NYC, CISG).

The text of the Convention and the list of enacting states is available on the UNCITRAL website.

4.2 Challenges to electronic contracting

At present, there continues to be a *lack of harmonisation at the international level regarding the recognition of electronic contracts*. While electronic contracts are recognised and legally binding in many jurisdictions around the world, the laws and regulations governing electronic contracting and their requirements can vary from country to country. Some countries have specific laws and regulations in place to govern electronic contracting, while others may rely on more general contract laws.

In the same way, specific requirements and standards for electronic and digital signatures can differ, including the level of security and authenticity that is required for an electronic or digital signature to be legally binding and enforceable.

It is also worth noting that there may be some challenges with cross-border electronic contracting, such as issues with the recognition and enforcement of electronic signatures, and the jurisdiction in which disputes will be resolved. Freight forwarders seeking to use electronic contracts are advised to consider these factors when drafting and executing electronic contracts that involve parties from multiple jurisdictions, and to seek independent legal advice as necessary.

4.3 Jurisdictional examples

Please note that the below information constitutes examples only, and should not be relied upon. Readers are advised to conduct their own research and due diligence to ensure that the information is correct and up-to-date.

Australia

Australia has legally recognised eSignature since 1999 with the Electronic Transactions Act. The Act recognises electronic signing as an important way to promote business and the economy in Australia. On 23 February 2022, the Corporations Amendment (Meetings and Documents) Bill 2021 (the Bill) became law, permanently amending the Corporations Act 2001 to allow companies to execute documents (including deeds) by electronic means on a permanent basis, extending a temporary measure that was introduced during the COVID-19 pandemic.

Chile

There are particular laws governing contracting on the internet and the electronic signatures in Chile, such as the Law on Electronic Documents, Electronic Signature and Electronic Signature Certification Services Law No. 19.799, dated April 12th, 2002 ("Electronic Signature Law") and Law No. 21,180, on Digital Transformation of the State ("Digital Transformation Law"). Consequently, acts and contracts concluded by electronic means are deemed as concluded in writing for all legal purposes.

The Electronic Signature Law recognises two electronic signatures: the electronic signature and the advanced electronic signature. The electronic signature is defined as any 'sound, symbol or electronic process that allows the recipient of an electronic document

to at least formally identify its author'. On the other hand, advanced electronic signature is defined as one 'created using means controlled exclusively by the holder so that it is linked to it and to the data to which it refers, allowing the detection of any alterations, the verification of the identity of the holder and the prevention of the repudiation of its integrity and authorship'. This signature must be certified by a registered third party.

China

China has legally recognised eSignatures since 2004 with The PRC Electronic Signature Law. Under this act, eSignatures are viewed as the same level of validity as pen and paper signatures when the appropriate requirements are taken. The Civil Law provides that a contract could be concluded orally or in written form, and the written form would come into effect once it's signed with signatures or sealed with company stamps. In practice, it is highly recommended that the contract is both signed by the legal representative or authorised representative of the company and sealed with the company stamp.

Electronic signatures are available with different commercial platforms. The company's stamp, which normally must be registered with the police, could also be registered electronically with a few platforms from the government, to ensure electronic stamps are effective. In this way, parties can sign electronic contracts with the same legal effect as a written one.

United Kingdom

Effective as of September 2019, UK Law Commission has confirmed that electronic signatures can be used to execute documents, including where there is a statutory requirement for a signature. This means that, in most cases, electronic signatures can be used as a viable alternative to handwritten ones (effective September 2019).

EU Member States

Electronic signatures were first recognised in European legislation through the Directive 1999/93/EC on a Community framework for electronic signatures, adopted in 1999.

Since 1 July 2016, electronic signatures in the EU are governed by the Electronic Identification and Trust Services (eIDAS) Regulation. eIDAS provides a predictable regulatory environment directly applicable to all EU Member States to enable secure and

seamless electronic interactions between businesses, citizens and public authorities. The eIDAS Regulation defines three levels of electronic signature: "simple" electronic signature, advanced electronic signature and qualified electronic signature. The requirements of each level build on the requirements of the level below it, such that a qualified electronic signature meets the most requirements and a "simple" electronic signature the least. While different levels of electronic signatures may be appropriate in different contexts, only qualified electronic signatures are explicitly recognised to have the equivalent legal effect of hand-written signatures all over the EU.

United States of America

The Uniform Electronic Transactions Act, 1999 (UETA) and the Electronic Signatures in Global and National Commerce Act of 2000 (E-SIGN Act) govern and provide legislation that aids in making electronic contracts and electronic signatures valid, admissible and enforceable. The regulations also stipulate that no document will be denied effectiveness only on the basis that it has been entered into electronically.

UETA provides a legal framework for conducting electronic transactions and recognises the validity and enforceability of electronic signatures and records. E-SIGN Act establishes the legal equivalence of electronic signatures with handwritten signatures and ensures the validity and enforceability of electronic contracts and records in interstate and foreign commerce.

While UETA is applicable at the state level, E-SIGN is a federal law that supersedes state laws where they may conflict. Consequently, E-SIGN provides consistent rules and standards for electronic transactions throughout the United States, harmonising the legal landscape across different jurisdictions.

There are four major requirements for an electronic signature to be recognised as valid under U.S. law: (1) Intent to sign; (2) Consent to do business electronically; (3) Association of signature with the record; and (4) Record retention.

However, not all documents are legally valid in the US when signed with the electronic signature, as outlined by the National Telecommunications Information Administration (NTIA). Documents that cannot be signed electronically include, inter alia: wills and testamentary trusts court orders or official court documents, and documents legally required to transport hazardous materials, pesticides or other toxic substance.

South Africa

The governing law in South Africa relating to the use of electronic signatures and records is the South African common law and the Electronic Communications and Transactions Act 25 of 2002 (hereafter "ECT Act").

The ECT Act distinguishes between an:

- "Electronic signature" ("ES"), which means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature (i.e., any digital or scanned (often also referred to as "unsecured") signatures), and
- "Advanced electronic signature" ("AES"), which means an electronic signature that results from a process which has been accredited by the South African .za Domain Name Authority.

Generally, no special formalities are required for the conclusion of an enforceable contract in South Africa and most contracts are not required to be in a written form, or to be signed. Therefore, contracting parties are responsible for determining the formalities that will be applied to a contract, including whether it will be executed with electronic signatures.

5. SELECTING A PROVIDER OF AN ELECTRONIC CONTRACT SYSTEM

Freight forwarders wishing to use an electronic contracting system are advised to carefully evaluate the features, security, and compliance of the service provider before making a decision. Important considerations may include:

1. **Ensuring adequate security:** The system should be secure and compliant with industry standards for data encryption, access controls, and electronic signature security.

2. **Ensuring legal compliance:** The system should be compliant with relevant laws and regulations related to electronic contracts.

3. **Considering usability and scalability:** The electronic contract system should be user-friendly, and should integrate well with any existing systems and processes used within the company. In addition, the system should be capable of accommodating the company's growth and any potential increase in the volume of contracts.

4. **Considering fair data ownership:** Freight forwarders should understand the rights and responsibilities of data ownership associated with the platform, as well as how the data may be used or analysed, particularly in case of termination of the service or data migration.

5. **Ensuring appropriate audit trails:** The provider should offer detailed audit trails and version control to ensure the integrity of the contract process.

6. **Ensuring appropriate storage measures within the system:** The platform should have appropriate storage measures commensurate to the needs of the company. It is important to conduct a holistic review of the system's policies and procedures to understand their data storage practices, and whether the measures for storage, encryption and backups are sufficient. This should include certifications such as SOC 2, ISO 27001, or HIPAA compliance that demonstrate the system's adherence to industry standards for data security, as well as appropriate policies demonstrating compliance with relevant data protection regulations.

6. PRACTICAL CONSIDERATIONS WHEN USING ELECTRONIC CONTRACTING METHODS

6.1 Establish clear internal contracting procedures and protocols

Clear contracting procedures or protocols should be established that not only ensure compliance with applicable laws or regulations, but also reflect the priorities of the parties or the forwarder, the proper contractual conditions, and that ensure collecting all needed and relevant expressions of consent. FIATA has previously published a Best Practice Guide on Contract Management that sets out general considerations in the contracting process, and it is recommended that freight forwarders equally take into account these considerations for electronic contracts.

However, it is worth noting that in addition to the regular contracting protocols for paper contracts, electronic contracts require specific protocols, including, for example, the authorisation process to use electronic signatures and/or stamps, and safeguarding measures to enter into the platforms. These include:

1. **Establishing a secure system for electronic signatures and document storage.** This is important to ensure the authenticity and integrity of the electronic contract. Measures may include:
    a. using secure servers and cloud storage systems, together with strong encryption to protect the contracts from unauthorised access and tampering;
    b. implementing access controls to ensure that only authorised individuals can access and view the electronic contracts;
    c. regularly backing up the electronic contracts in a separate and secure location;
    d. keeping the system updated with the latest security measures, and ensuring a regular audit to identify any vulnerabilities in the system;

e. have a business continuity plan in place of any security breaches or system failures.

2. **Developing clear policies and procedures for creating and executing electronic contracts.** In many instances, the possibilities for concluding an electronic contract may mean that employees within a company may unwittingly enter into a legally binding contract without realising it, for example by clicking through an online form or typing their name electronically.

   It is therefore recommended that clear guidelines are established for what constitutes a legally binding electronic signature, as well as clear authority levels to clarify who within the company is permitted to conclude contracts on the company's behalf. **Freight forwarders may wish to add a sentence to the contract stating that the person signing represents that it has the necessary authority to execute the contract.**

3. **Ensuring that all parties involved in the electronic contract are aware of and agree to the terms and conditions of the contract.** This includes providing clear and conspicuous notice of the terms and obtaining affirmative consent from all parties.

4. **Auditing and monitoring the electronic contracting process.** This should ensure compliance with internal policies and procedures, as well as applicable laws and regulations.

5. **Having a plan in place for the management of electronic records** including retention, archival, and destruction policies and procedures, and ensuring this is communicated across the company.

6.2 Understand how electronic contracting is recognised legally in the jurisdictions of the signing parties

Given the varying approaches to electronic contracting around the world, it is crucial to determine if electronic contracting is legally recognised in the jurisdictions of the signing parties, and what requirements may be involved for such recognition.

A review of the laws and regulations of the relevant jurisdictions should be conducted to see if they have laws specifically addressing electronic contracting, or if they have adopted any international conventions or agreements that recognise electronic contracting, such as those listed in the preceding sections. In the event that the results are inconclusive, it

may also be useful to look at court cases in the relevant jurisdictions that have dealt with electronic contracting to see how they have been treated.

Importantly, freight forwarders are advised to seek their own legal advice to ensure that they have an accurate understanding of the situation and its implications for the specific case at hand. Adopting a choice of law clause referring to a jurisdiction with favourable treatment towards electronic contracting may, upon appropriate legal advice, be a sensible measure to ensure greater certainty.

6.3 Ensure adequate insurance coverage

Due diligence should be a fundamental component of a freight forwarders' approach to this area of risk. The selection of reputable providers for e-signature software is critical.

It would be prudent to ensure that sufficient liability insurance is in place to cover risks associated with all contractual arrangements. For contractual e-signatures, ensuring your liability insurer is aware of your systems, controls and providers could serve to satisfy any concerns they might have regarding this area of risk.

6.4 Take appropriate cybersecurity measures

When using electronic contracts, cybersecurity measures should be taken to protect the contracts and the sensitive information they contain, as well as to ensure compliance with relevant data protection requirements. FIATA has previously published a Prevention of Cybercrime Best Practice Guide which may provide some useful information. Practical measures may include:

1. **Encryption:** Strong encryption is recommended to protect the contracts and any sensitive information they contain. This helps to ensure that the contracts cannot be read or modified without the proper authorisation.
2. **Firewalls:** An up-to-date firewall should be used to protect the electronic contract system from unauthorised access and cyber-attacks.
3. **Multi-factor authentication:** Multi-factor authentication to ensure that only authorised users can access the electronic contract system.

4. **Vulnerability management:** Regular security scans should be conducted to monitor the electronic contract system for vulnerabilities and patch or update as needed.
5. **Employee training:** Provide regular cybersecurity training to employees to ensure they understand how to identify and prevent potential security threats.
6. **Reviewing third-party contracts:** Reviewing any third-party contracts and service providers to ensure they have adequate security measures in place.

7. SPECIAL CONSIDERATIONS WHEN SIGNING AN ELECTRONIC CONTRACT

7.1 Situations where a stamp is usually required

Where a stamp would usually be required for a contract, there are several methods that may constitute a valid electronic signature, depending on the laws and regulations of the jurisdictions concerned. Some are listed below:

1. **Digital signature:** As noted in the foregoing sections, digital signatures are a specific type of electronic signature that use encryption and digital certificates to verify the identity of the signer. In many countries, digital signatures are recognised as a legally binding substitute for a stamp.

2. **Tamper-evident seal:** Some electronic signature software can add a tamper-evident seal to the document, which is a visual representation of the signature that can be used to detect if the document has been modified after it was signed, and may be considered in some countries in place of a stamp.

3. **Notary service:** Many countries have notary services that can provide an electronic notarisation service which can be legally equivalent to a traditional wet-ink signature.

It is important to check the laws and regulations of the specific country or jurisdiction where the contract is being executed to ensure that the electronic signature method used is legally binding and recognised as a substitute for a stamp.

7.2 Email signatures

An email signature is a way to add personal or organisational information at the end of an email message. It is not considered to be an electronic signature for the purposes of contracting, as it does not provide the same level of security and authentication as a digital signature.

8. QUICK CHECKLIST

- ☐ Ensure that electronic contracts are recognised by the jurisdictions of the signing parties and any applicable laws;
- ☐ Ensure that electronic signatures are recognised by the jurisdictions of the signing parties, and understand the legal requirements for an electronic signature to be recognised;
- ☐ Choose a reliable system provider and clearly define their responsibilities and liabilities;
- ☐ Establish internal control systems for the use of electronic signatures and electronic stamps within the organisation;
- ☐ Purchase insurance for the use of electronic contracts and the risks arising thereof;
- ☐ Take appropriate cybersecurity measures;
- ☐ To the extent possible, establish clear contracting procedures or protocols that not only ensure compliance with applicable laws or regulations, but also reflect the priorities of the parties or the forwarder, the proper contractual conditions, and that ensure the collection of all needed and relevant expressions of consent;
- ☐ Implement tools that ensure the proper monitoring, storage and audit trail of all contracts concluded electronically and their status;
- ☐ Ensure continuous employee learning and training;
- ☐ Check/track any related regulations updates in your region.

International Federation of Freight Forwarders Associations

The global voice of freight logistics

Rue Kléberg 6 | 1201 Geneva | Switzerland
Tel.: +41 22 715 45 45 | info@fiata.org | www.fiata.org

Design: Services Concept Sàrl, Geneva
Layout: Svitlana Ivanova