# LEGAL READINESS ASSESSMENT GUIDE

Cross-border paperless trade has great potential not only to grow trade competitiveness, but also to address new challenges associated with cross-border e-commerce and the rise of the digital economy. The Interim Intergovernmental Steering Group on Cross-border Paperless Trade Facilitation and its Legal and Technical Working Groups have developed Legal and Technical Readiness Checklists as part of their support for the implementation of the substantive provisions of the Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific. This readiness assessment guide will facilitate self-assessments of legal and technical readiness FOR cross-border paperless trade. The guide contains explanatory notes, good practices, references and other relevant information to assist users to conduct self-assessment using the checklists.

The readiness assessment guide is available at: https://readiness.digitalizetrade.org/

## Contents

# Introduction to the checklist

1. The checklist serves to identify potential legal gaps and highlight what may need to be done to ensure the laws support engagement in cross-border paperless trade, as envisaged in the Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific, which was adopted by the Economic and Social Commission for Asia and the Pacific (ESCAP) in 2016.
2. It should be noted that the checklist is not intended to assess the readiness of a country to join the Framework Agreement. This treaty contemplates that its parties ensure that their legal systems support the use of electronic communications and gradually adapt their laws for the purpose of cross-border paperless trade. It is not necessary for Governments to modernize their laws before ratifying or acceding to the Agreement.[1] Paperless trade implementation is a work in progress, and the Agreement is a tool meant to support such progress regardless of the level of readiness of a country.
3. In line with the substantive provisions of the Framework Agreement, the checklist organizes legal issues into four major parts as follows: (a) electronic transactions and signatures law; (b) laws regarding paperless trade systems; (c) cross-border aspects; and (d) other considerations. Each part is divided into sections. In each part and section of the checklist, key legal issues are highlighted, and a list of focus questions is proposed.
4. The checklist is intended for use by all stakeholders involved in paperless trade facilitation and not only for legal specialists. While it includes references to legal concepts, it does so in general terms in order to reach a broad audience. Each question should be seen as the starting point for a broader reflection on the state of the law in the given area.
5. The term "law" should be understood to include statutes, regulations, administrative measures and any other binding rules. All questions about national laws can be applied to subnational laws as appropriate. In completing the checklist, it is recommended that the user indicate, where possible, the legal authority for the answers, for example the statute, regulation or other rule relevant to the answers. Some relevant obligations may arise through contracts as well.
6. A number of examples of country reports on readiness assessments for cross-border paperless trade carried out by ESCAP are also available online.[2] In addition, a general introduction on legal issues related to cross-border paperless trade may be found in the ESCAP publication *Electronic Single Window Legal Issues: A Capacity-Building Guide*.[3]

**I. Electronic transactions and signature law**

1. Part I of the checklist is focused on laws related to electronic transactions and electronic signatures. These concerns are addressed either directly or indirectly in articles 5, 6 and 7 of the Framework Agreement. In particular, the first three principles included in article 5 (on general principles) represent the principles guiding the legislative texts on electronic commerce prepared by the United Nations Commission on International Trade Law (UNCITRAL) and, as such, are an expression of international consensus.[4] Approximately

[1] Detailed information on the Framework Agreement, including an explanatory note and answers to frequently asked questions, is available at www.unescap.org/resources/framework-agreement-facilitation-cross-border-paperless-trade-asia-and-pacific.

[2] Available at www.unescap.org/resources/readiness-assessments-cross-border-paperless-trade.

[3] ST/ESCAP/2636.

[4] The Framework Agreement contains the internationally recognized criteria for these laws, such as non-discrimination of the use of electronic communications (the laws apply in the same way, or with the same effect, to paper and electronic documents), technological neutrality (the laws do not specify what technology to use to achieve the legal effect) and functional equivalence (electronic documents have the same practical or legal effect as their paper equivalents, even if they have different characteristics).

half of the Governments in Asia and the Pacific have adopted at least one UNCITRAL text on electronic commerce.[5]

2. In order to promote interoperability, to the extent possible similar rules should apply to electronic communications exchanged among commercial operators and between commercial operators and public authorities. In the paperless trade facilitation environment, this means that trade-related data exchanged in commercial documents may be reused for submission to single windows. This should ensure high data quality with respect to its origin, integrity, accuracy, completeness and other characteristics.

***Related provisions of the Framework Agreement:***

- Article 5 on general principles.
- Article 6 on the national policy framework, enabling domestic legal environment and paperless trade committee.
- Article 7 on the facilitation of cross-border paperless trade and development of single-window systems (more specific questions on the single window appear below in part II).

**II. Laws regarding paperless trade system**

1. Part II of the checklist is focused on laws related to implementing and developing a paperless trade system (including but not limited to a single window system). These matters relate in particular to articles 6 and 7 of the Framework Agreement. The wide scope of article 6 can encompass several aspects of creating an enabling national policy framework for paperless trade. In article 7, parties are specifically encouraged to implement and develop a cross-border paperless trade system, in particular a single window. Accordingly, in part B, issues related to the implementation of a single window and/or other paperless trade system(s) are covered first. Part II also includes questions on end-user agreements, service-level agreements and memorandums of understanding on paperless trade.

***Related provisions of the Framework Agreement:***

- Article 6 on the national policy framework, enabling domestic legal environment and paperless trade committee.
- Article 7 on the facilitation of cross-border paperless trade and development of single-window systems.

**III. Cross-border aspects**

1. Part III of the checklist is focused on the cross-border aspects of paperless trade, which directly relate to the ultimate goal of the Framework Agreement. Certain cross-border aspects are already raised in part I as they relate to general matters that may be relevant to paperless trade facilitation. The questions in part III are specific to cross-border paperless trade facilitation. They are inspired by the Agreement, in particular article 8 on cross-border mutual recognition of trade-related data and documents in electronic form; article 9 on international standards for exchange of trade-related data and documents in electronic form; and article 10 on the relation to other legal instruments enabling cross-border paperless trade.
2. A key issue in achieving seamless cross-border paperless trade is the legal recognition of trade-related data and documents of one country by the authorities of another. Recognition involves attributing a legal status to electronic messages exchanged across borders. A variety of legal mechanisms may achieve that goal. Some of them will apply to certain types of transactions (for instance, business-to-business or business-to-government transactions), while other legal mechanisms will apply only to specific types of documents or data sets, or to specific types of trust services (for example, electronic signatures). Some legal mechanisms will establish legal recognition in a technology-neutral manner, or

[5] For a list of UNCITRAL texts on electronic commerce, see part C.

without regard for the method or technology used, while others will do so in a technology-specific manner. With respect to legal form, some mechanisms are treaty-based and therefore may be directly legally binding. Other mechanisms favour the harmonization of legal systems through the adoption of uniform laws, while still others are based on bilateral or regional agreements or memorandums of understanding and similar technical arrangements.

3. In article 8 of the Framework Agreement, the mutual legal recognition of trade-related data and documents in electronic form is promoted and the notion of substantially equivalent level of reliability is used to indicate that mutual legal recognition can be based on the general principle of technology neutrality. However, no specific legal recognition mechanism is established. Rather, the expression of this criterion is left open to various options. Accordingly, many of the questions in part III are aimed at identifying which laws and technical arrangements may contribute to achieving mutual legal recognition. The scope of the questions also extends to include the broader focus of articles 9 and 10 on laws and other relevant agreements that prohibit, restrict or facilitate cross-border data flows for paperless trade and any related activity. An indicative list of relevant international instruments is provided at the end of part III for ease of reference.

***Related provisions of the Framework Agreement:***

- Article 8 on cross-border mutual recognition of trade-related data and documents in electronic form.
- Article 9 on international standards for exchange of trade-related data and documents in electronic form.
- Article 10 on relation to other legal instruments enabling cross-border paperless trade.

**IV. Other considerations**

1. For paperless trade to be conducted in the best possible manner, the Framework Agreement requires parties to create an enabling national legal framework (article 6) and remove all legal barriers. It is therefore recommended that the parties aim to build a national policy framework to implement the Agreement that addresses all the pertinent legal issues and is consistent with international legal instruments and standards for cross-border electronic data and document exchange. Besides the topics specifically addressed in substantive provisions of the Agreement, parties may also wish to deal with related issues, such as data ownership, liability, dispute settlement, electronic payment and competition, which in some cases may have been addressed in other legal agreements (see article 10). These matters may affect the effective operation of single window and other paperless trade systems, particularly in the cross-border environment.
2. These legal issues may be addressed in different sets or sources of legal rules. Therefore, there is no one-size-fits-all solution or approach. The legal framework, action plan and capacity-building programmes may and should be customized at the national level, depending on the various levels of awareness and preparedness of different member States, as already envisaged in article 6, 12 and 14 of the Framework Agreement. The list of legal issues in part IV is not exhaustive, and other relevant issues may emerge.

Related provisions of the Framework Agreement:

- Article 6 on the national policy framework, enabling domestic legal environment and paperless trade committee.
- Article 10 on the relation to other legal instruments enabling cross-border paperless trade.
- Article 12 on the action plan.
- Article 14 on capacity-building.

# I. Electronic transactions and signature law

## I.A. Electronic transactions law: general principles

This section is aimed at identifying the general features of electronic transactions law, including whether they implement internationally recognized general principles.

### I.A.1 What is the legal status of electronic transactions?

Electronic transactions are transactions of a commercial or non-commercial nature that take place through electronic means, i.e. by exchanging data messages. "Data message" means information generated, sent, received or stored by electronic, optical or similar means (*Model Law on Electronic Commerce 1996* - MLEC Article 2(a)). Examples of electronic means include e-mail, messaging, electronic data interchange (EDI), short message system (SMS) and fax.

National law may accord full or partial legal validity to electronic transactions. This may happen because of a law, regulation or other written legislative text, through judicial decisions or by application of general legal principles.

Article 5 of the MLEC establishes legal recognition on the basis of the principle of non-discrimination against the use of electronic means.

> *5. Legal recognition of data messages*
>
> *Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.*

Legislation based on the same approach as the uniform model may differ in the language used.

See section 8(1) of the *Electronic Transactions Act 1999* (Cth) of Australia.

> *8. Validity of electronic transactions*
>
> *1) For the purposes of a law of the Commonwealth, a transaction is not invalid because it took place wholly or partly by means of one or more electronic communications.*

Other laws take a different approach, recognizing only those electronic transactions that comply with certain requirements.

See section 4 of Nepal's Ordinance No. 32 of the year 2061 B.S. [2005 A.D.], An Ordinance to provide the provisions for Electronic Transactions.

> *4. Legal recognition of electronic record*
>
> *Where the law in force requires any information, documents, records or any other matters to be kept in written or printed typewritten form, then, if such information, documents, records or the matters are maintained in an electronic form by fulfilling the procedures as stipulated in this Ordinance or the Rules made hereunder, such electronic record shall also have legal validity.*

### I.A.2 If an electronic transactions law exists, is it based on uniform models?

In several countries, legislation dealing with electronic transactions (often called Electronic Transactions, Electronic Commerce or Electronic Signatures Law) is based on uniform law, i.e. on model legislation that has been prepared by an international body. Uniform law, which may include international standards with or without direct legal effect, can be global or regional. The United Nations Commission on International Trade Law (UNCITRAL) Model Laws are examples of global uniform law.

Adoption of model laws indicates the desire of the country to harmonize its laws with those of other countries, which facilitates cross-border electronic exchanges. UNCITRAL legal texts on electronic transactions such as the MLEC and the *Model Law on Electronic Signatures 2001* (MLES) are examples of laws that are being widely adopted by countries to achieve global harmonization.

### I.A.3 What are the conditions, if any, for the legal recognition of electronic transactions?

Laws on electronic transactions may be neutral or specific about the electronic technology to be used in order for them to be recognized as legally valid. "Technology neutral" laws do not prescribe or favour the use of any particular technology, method or product for electronic transaction.

In contrast, "technology specific" laws recognize only those electronic transactions that use a specific technology, method or product – for instance, transactions signed with public key infrastructure (PKI) based digital signatures, or PKI-based digital signatures originating in the country of origin or from service providers that are licensed by an oversight authority.

Normally, technology neutral laws do not contain an explicit label with this characterization. Rather, it is the whole law that is drafted in a technology neutral manner.

See Article 3 of the MLES for an example of technology neutral uniform law provision dealing with electronic signatures.

> *3. Equal treatment of signature technologies*
>
> *Nothing in this Law, except Article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in Article 6, paragraph 1, or otherwise meets the requirements of applicable law.*

Technology specific requirements may apply to all types of electronic transactions.

Alternatively, technology specific requirements may apply only to some transactions, such as those exchanged in a certain field (for example, banking) or with certain participants (for example, government and other public agencies). Such requirements may be imposed because security or reliability are considered especially important. In those cases, there may be a law of general application that enables the use of information in electronic form under technology neutral standards, while electronic transactions in certain fields or with special form requirements need to use specified technology.

Article 3 of the *Digital Signature Act 1999* of the Republic of Korea deals with the legal effect of a digital signature.

> *3. Effect, etc. of digital signature*
>
> *(1) In cases where a signature, signature and seal, or name and seal is, under other Acts and subordinate statutes, required to be affixed on a paper-based document or letter, it shall be deemed that such requirements are satisfied if there is a certified digital signature affixed on an electronic message.*

Paragraph 3 of the same Act introduces an exception to accommodate party autonomy.

> *(3) A digital signature other than a certified digital signature shall have such an effect of a signature, signature and seal, or name and seal, as is agreed between the parties concerned.*

### I.A.4 Does the law establish functional equivalence between paper documents and electronic communications?

The law may adopt a "functional equivalence" approach to give electronic communications the same legal effect as paper-based documents. The principle of functional equivalence establishes that, when certain conditions are met, the legal value of electronic communications is equivalent to that of paper-based documents because they satisfy the same policy function as the paper. This approach allows a legal system not to alter its traditional rules about paper-based documents. It also avoids creating a special legal regime for electronic communications (a so-called "dual regime" approach).

UNCITRAL texts rely on a functional equivalence approach to determine how the purposes and functions of paper-based documents can be fulfilled by electronic communications. For example, Article 6(1) of the MLEC provides the requirement of a document "in writing", which aims at making the information contained in that document available beyond the moment of the transaction.

*6. Writing*

*Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.*

### I.A.5 What is the legal status of electronic contracts?

Some national laws contain provisions on the legal status of contracts made and performed by electronic means. These provisions aim to ensure that the electronic form of a contract is not in itself a reason to invalidate it. Other legal systems have decided that validating electronic communications will validate contracts in electronic form without mentioning them specifically.

See for instance section 11 of the *Electronic Transactions Act 2010 (Cap. 88)* of Singapore that recognises the legal validity of electronic communications in concluding contracts.

*11. Formation and validity of contracts*

*1. For the avoidance of doubt, it is declared that in the context of the formation of contracts, an offer and the acceptance of an offer may be expressed by means of electronic communications.*

*2. Where an electronic communication is used in the formation of a contract, that contract shall not be denied validity or enforceability solely on the ground that an electronic communication was used for that purpose.*

Moreover, laws can contain other provisions that do not modify the general law of contract but clarify how it can be applied in a digital environment. For instance, they can determine the time of dispatch and receipt of offer, acceptance and other contract-related communications, or they can confirm the validity of the use of automated agents in contract formation and performance. This is the approach taken in UNCITRAL texts, where the rules on electronic contracts are found especially in the MLEC and the *Convention on the Use of Electronic Communications in International Contracts 2005* (ECC).

For instance, section 14(a) of the Australian *Electronic Transactions Act 1999* (Cth), based on article 10(2) of the ECC, specifies the time of receipt of an electronic communication.

*14(a). Time of receipt*

*(1) For the purposes of a law of the Commonwealth, unless otherwise agreed between the originator and the addressee of an electronic communication:*

*(a) the time of receipt of the electronic communication is the time when the electronic communication becomes capable of being retrieved by the addressee at an electronic address designated by the addressee; or*

*(b) the time of receipt of the electronic communication at another electronic address of the addressee is the time when both:*

*(i) the electronic communication has become capable of being retrieved by the addressee at that address; and*

*(ii) the addressee has become aware that the electronic communication has been sent to that address.*

Section 15 of the *Electronic Transactions Act 2010 (Cap. 88)* of Singapore adopts verbatim Article 12 of the ECC, which provides legal validity to a contract formed by automated message systems.

*15. Use of automated message systems for contract formation*

*A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.*

As a general rule, therefore, provisions on electronic contracts do not alter the substantive law of contract, whether the law is technology neutral or technology specific.

See Article 9 of the ECC for a technology neutral provision dealing with a form requirement of an electronic contract.

> *9. Form requirement*
>
> *1. Nothing in this Convention requires a communication or a contract to be made or evidenced in any particular form.*

For an example of technology specific legislative provision, see rule 3 of the *Electronic Transactions Rules 2064* (2007) of Nepal, complementing section 4 of the *Ordinance No. 32 of 2005*.

> *3. To certify electronic record*
>
> *(1) A person intending to certify the electronic record or the information kept in electronic form by digital signature may certify such record or information by fulfilling the following procedures:*
>
> > *(a) by creating hash result by the use of hash function by means of software contained in one's computer, and*
> >
> > *(b) by creating a digital signature from the result under Clause (a) by the use of private key of the person affixing the digital signature by means of software.*
>
> *(2) Any electronic record certified by digital signature created under Sub-rule (1) and the digital signature certifying such record shall be deemed to be a legally recognized electronic record and digital signature.*

### I.A.6 Are there special rules for the use of electronic communications in paperless trade?

By definition, trade is paperless if electronic communications are used, so no special rules may be thought to be required for trade once electronic communications themselves are validated. However, a large part of paperless trade involves public entities, whether customs authorities or other regulatory agencies protecting the integrity of the national economy and environment. As noted, electronic communications exchanged with public entities may be subject to special requirements.

Accordingly, States may decide to apply general electronic transactions law (ETL) also to paperless trade or may decide to establish a special legal regime for it. The first approach has the advantage of facilitating the exchange of information between private and public sectors, promoting technical as well as legal interoperability. The second approach may be seen as more secure and better suited for the management of a border operations such as a "single window".

Often, States decide to introduce safeguards in addition to the general ETL applying to paperless trade. It is then important to minimize occasions in which the special requirements hinder the flow of trade-related data.

For instance, section 25 of the *Electronic Transactions Act 2010 (Cap. 88)* of Singapore extends the application of the Act to the use of electronic records by public agencies in that country. Note subsection (2), with relatively restrictive provisions for some cases.

> *25. Acceptance of electronic filing and issue of documents*
>
> *1) Any public agency that, pursuant to any written law —*
> *a) accepts the filing of documents, or obtains information in any form;*
> *b) requires that documents be created or retained;*
> *c) requires documents, records or information to be provided or retained in their original form;*
> *d) issues any permit, licence or approval; or*
> *e) requires payment of any fee, charge or other amount by any method and manner of payment,*

*may, notwithstanding anything to the contrary in such written law, carry out that function by means of electronic records or in electronic form.*

*2) In any case where a public agency decides to perform any of the functions in subsection (1) by means of electronic records or in electronic form, the public agency may specify —*

*a) the manner and format in which such electronic records shall be filed, created, retained, issued or provided;*

*b) where such electronic records have to be signed, the type of electronic signature required (including, if applicable, a requirement that the sender use a particular type of secure electronic signature);*

*c) the manner and format in which such signature shall be affixed to the electronic record, and the identity of or criteria that shall be met by any specified security procedure provider used by the person filing the document;*

*d) such control processes and procedures as may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; and*

*e) any other required attributes for electronic records or payments that are currently specified for corresponding paper documents.*

The provision is operationalised in the Singapore *Customs Act 2004 (Cap. 70)*.

*86. Computer service*

*(1) The Director-General may establish and operate a computer service and make provision for any manifest, return, list, statement, declaration, direction, notice, permit, receipt or other document required or authorised by this Act to be made, served or submitted by electronic transmission (referred to in this Act as an electronic notice).*

*96. Declarations to give a full and true account*

*(1) The declarations referred to in sections 37, 59 and 80 shall, unless the Director-General allows under subsection (2), be made and submitted by an electronic notice in accordance with section 86 and such declaration shall give a full and true account of such particulars as are required by the Director-General.*

It is also important to bear in mind the relevant provisions of evidence law. (Electronic evidence is discussed below in part I.E.4.) In the case of Singapore, those are found in the *Evidence Act 1997 (Cap. 97)*.

For information on other States, see the Asia-Pacific Economic Cooperation (APEC) publication *Review on Regulations and Policies for E-Port and Single Window in APEC Economies* (2016), available at http://www.apmenet.org/wp-content/uploads/2016/07/Review-on-Regulations-and-Policies-for-E-Port-and-Single-Window-in-APEC-Economies.pdf

### I.A.7 In particular, are there special rules for the use of trade-related data and documents in electronic form such as certificates of origin, invoices and phytosanitary certificates?

Even if the law has a technology neutral approach that applies to both private and public sector, special requirements may arise for the use in electronic form of certain types of commercial and trade-related documents.

In particular, the law, including administrative regulations, may set out special requirements for the submission to a single window of documents that are particularly relevant for paperless trade such as manifests, certificates of origin, invoices and phytosanitary certificates. The special requirements may apply to certain kinds of documents only when they will be exchanged across borders.

### I.A.8 Are there special rules for the use of electronic transferable records such as bills of lading?

Certain commercial documents are transferable, i.e. they incorporate the entitlement to the delivery of goods that they describe (for example, bills of lading, warehouse receipt) or the payment of money (for example, checks,

promissory notes). Bills of lading are particularly relevant for paperless trade facilitation and for logistics. Other transferable documents relate to financing and are relevant for national trade platforms.

Because of their need for special features, notably non-duplication and control ("possession" when on paper), the law requires special rules for their use in electronic form. UNCITRAL has prepared the *Model Law on Electronic Transferable Records 2017* (MLETR) to deal with those documents in line with UNCITRAL principles of technology neutrality and functional equivalence.

In certain jurisdictions, special legal regimes exist to enable the use of specific types of electronic transferable records. For example, Article 862 of the revised *Commercial Act 2016* of Republic of Korea gives legal validity to electronic bills of lading complying with certain requirements.

> *862. Electronic bills of lading*
>
> *1. A carrier may issue an electronic bill of lading by means of registration with the registry agency designated by the Ministry of Justice with the consent of a consignor or charterer in lieu of issuance of a bill of lading referred to in Article 852 or 855. In such cases, an electronic bill of lading shall have the same legal effect as bills of lading referred to in Articles 852 and 855.*

The related Regulation on the Implementation of the Provisions of the Commercial Act Regarding Electronic Bills of Lading provides details on how electronic bills of lading should be managed and on the requirements by which a registry agency may be licensed.

## I.B. Electronic signatures and trust services

Electronic signatures serve to identify the originator of an electronic communication and ascertain their intention with respect to that communication. Certain types of electronic signatures, namely digital signatures based on public key infrastructure certificates, may provide additional information, for instance on the integrity of the data message and on timestamping.

Many laws deal with the legal recognition of electronic signatures and set out requirements to be met so that an electronic signature may be considered legally equivalent to a handwritten signature. This reflects the importance given to signatures in business practices. However, legislative approaches may vary significantly, in particular with respect to technology neutrality and the status of service providers.

Trust services are electronic services that provide assurance on the quality of data. Trust services are often used to establish confidence in the use of electronic communications.

### I.B.1 Does the law address how electronic signatures, including for identification, authorization and authentication, are added in an electronic environment? Does it require the use of a specific technology or method for electronic signatures or is it technology neutral?

(a) The law may mandate the use of a specific technology for electronic signatures. A technology specific approach spells out how electronic signatures must be created and often authenticated (certified) to be valid. The purpose of this approach is generally to ensure reliability or security of the performance of the "function", especially the identification of the signatory but also the link between the signatory and the information. Thus, the law may require the use of PKI-based digital certificates. In that case, the law may also specify which providers of PKI signing data and supporting services (notably issuing certificates) are recognized and establish an oversight regime (certification, accreditation, licensing or monopoly) for them.

Article 2 of the Law of the Republic of Armenia on *Electronic Document and Electronic Signature 2004*, defines an electronic signature by reference to the use of cryptographic techniques.

> *2. Definitions*
>
> *"electronic digital signature" means obtained signature-creation data and a cryptographic data modification of the given electronic document presented in a unique sequence of symbols in electronic*

*form, which is attached to or logically associated with an electronic document and which is used to identify the signatory, as well as to protect the electronic document from forgery and distortion.*

In case of technology specific electronic signature law, please provide details of the required characteristics. Often this is a digital signature supported by a PKI-based certificate issued by a trusted third party, sometimes a public authority. Those details may be contained in implementing regulations and may vary with the type of document or transaction.

(b) Alternatively, the law may be technology neutral and recognize all types of electronic signatures. Exceptions may be made for specific types of documents or transactions. For example, section 10 of the *Electronic Transactions Act 1999* (Cth) of Australia.

*10. Requirement for a signature*

*(1) If, under a law of the Commonwealth, the signature of a person is required, that requirement is taken to have been met in relation to an electronic communication if:*

*(a) in all cases—a method is used to identify the person and to indicate the person's intention in respect of the information communicated; and*

*(b) in all cases—the method used was either:*

*i. as reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or*

*ii. proven in fact to have fulfilled the functions described in paragraph (a), by itself or together with further evidence; and*

*I if the signature is required to be given to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that the method used as mentioned in paragraph (a) be in accordance with particular information technology requirements—the entity's requirement has been met; and*

*(d) if the signature is required to be given to a person who is neither a Commonwealth entity nor a person acting on behalf of a Commonwealth entity—the person to whom the signature is required to be given consents to that requirement being met by way of the use of the method mentioned in paragraph (a).*

(c) Often the law takes an intermediate approach, called "two-tier" or "hybrid": all authentication methods may be recognized as having legal value, if they meet certain requirements, and 2) certain technologies offering higher levels of security (usually digital signatures issued by a recognized certifying authority) have a stronger legal status, typically associated with presumptions of origin and integrity.

Section 226 of the *Contract and Commercial Law Act 2017* of New Zealand is a technology neutral provision on electronic signatures based on the functional equivalence approach.

*226. Legal requirement for signature*

*(1) A legal requirement for a signature other than a witness's signature is met by means of an electronic signature if the electronic signature—*

*(a) adequately identifies the signatory and adequately indicates the signatory's approval of the information to which the signature relates; and*

*(b) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required.*

*(2) However, a legal requirement for a signature that relates to information legally required to be given to a person is met by means of an electronic signature only if that person consents to receiving the electronic signature.*

Section 228 of the same Act sets in a technology neutral manner the requirements to presume the reliability of the electronic signature

*228. Presumption about reliability of electronic signatures*

*(1) For the purposes of sections 226 and 227, it is presumed that an electronic signature is as reliable as is appropriate if—*

*(a) the means of creating the electronic signature is linked to the signatory and to no other person; and*

*(b) the means of creating the electronic signature was under the control of the signatory and of no other person; and*

*(c) any alteration to the electronic signature made after the time of signing is detectable; and*

*(d) where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.*

*(2) Subsection (1) does not prevent any person from proving on other grounds or by other means that an electronic signature—*

*(a) is as reliable as is appropriate; or*

*(b) is not as reliable as is appropriate.*

### I.B.2 Does the law adopt a functional equivalence approach for electronic signatures?

In line with the general application of the functional equivalence principles, the law may set the conditions under which an electronic signature is considered equivalent to a handwritten one. If a functional equivalence approach is adopted, an electronic signature must normally identify the signatory and to indicate the signatory's intention in respect of the information signed. For example, Article 9 of the MLETR.

*9. Signature*

*Where the law requires or permits a signature of a person, that requirement is met by an electronic transferable record if a reliable method is used to identify that person and to indicate that person's intention in respect of the information contained in the electronic transferable record.*

### I.B.3 Is the law based on international standards?

Many jurisdictions have based their electronic signature laws on uniform models.

UNCITRAL legal texts, especially the MLES, provide a set of provisions on electronic signatures based on the principles of technology neutrality and functional equivalence. Other regional models exist, for instance the European Union *Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC* (eIDAS Regulation), and certain influential national laws.

This question gives an opportunity to identify those international standards and describe significant variations that national law has made from its international sources.

### I.B.4 Does the law recognize foreign electronic signatures?

A foreign electronic signature is an electronic signature that is issued or applied outside the jurisdiction where its legal recognition is sought. It may also contain other foreign elements, such as relying on a PKI-based certificate generated abroad.

In certain jurisdictions, the law recognizes only national electronic signatures. In many cases, this outcome may be implicit since the law does not contain any provision on foreign electronic signatures. However, silence on foreign electronic signatures does not necessarily mean that they are invalid.

Other jurisdictions may have laws, regulations, policies or agreements to provide legal recognition to foreign electronic signatures.

The law may attribute to a certain body the possibility of recognizing electronic signatures, or certain types of them, based on general guidelines. See for instance the *Information Technology Act 2000* (No. 21 of 2000) of India.

> *19. Recognition of foreign certifying authorities*
>
> *19(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.*
>
> *89. Power of controller to make regulations*
>
> *89(1) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.*
>
> *(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely: […] (b) the conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority under sub-section (1) of section 19;*

Alternatively, technology neutral electronic transactions may apply the same standards to validate the use of domestic and foreign electronic signatures. In other words, when it comes to assessing the validity of the signature, the foreign element is disregarded.

In that line, Article 12 of the MLES provides for a test of substantial equivalence between the reliability levels offered by the signatures in question in different locations. The Article offers legal effect to a foreign electronic signature if that signature offers a substantially equivalent level of reliability to an electronic signature issued in the enacting State.

> *12. Recognition of foreign certificates and electronic signatures*
>
> 1. *In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:*
>  a) *To the geographic location where the certificate is issued or the electronic signature created or used; or*
>  b) *To the geographic location of the place of business of the issuer or signatory.*
> 2. *A certificate issued outside [the enacting State] shall have the same legal effect in [the enacting State] as a certificate issued in [the enacting State] if it offers a substantially equivalent level of reliability.*
> 3. *An electronic signature created or used outside [the enacting State] shall have the same legal effect in [the enacting State] as an electronic signature created or used in[the enacting State] if it offers a substantially equivalent level of reliability.*
> 4. *In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be had to recognized international standards and to any other relevant factors.*
> 5. *Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.*

Legal recognition of foreign signatures may also be provided by treaty or by a regional instrument. Article 9(3) of the ECC has this effect when electronic signatures are used in commercial exchanges since the ECC is a treaty that binds its States parties. The eIDAS Regulation has the same effect within the European Union.

Similar to what happens with domestic electronic signatures, the legal recognition of foreign electronic signatures, or certain types of them, used for electronic exchanges within a particular sector (such as banks) or among particular participants (such as public agencies) may be determined either by special laws (such as customs laws) or by other legal instruments.

Finally, the law may allow for parties to a commercial transaction to agree on the conditions for the recognition of foreign signatures. This is often allowed on the basis of general legal principles rather than specific provisions in the law. The Pan Asian E-Commerce Alliance (PAA) PKI Mutual Recognition Framework is a contractual mechanism used by PAA participants to achieve mutual legal recognition of foreign digital certificates. Contractual mechanisms operate within the limits of mandatory legal provisions that may be applicable.

#### I.B.5 Are there special rules for the use of electronic signatures in paperless trade?

If laws on paperless trade are enacted, they may contain special provisions. An example of such law could be the legal regime for the operation of the electronic single window.

#### I.B.6 Does the law deal with trust services?

Trust services are electronic services that provide assurance of the quality of data. Electronic signatures may be considered one type of trust service but, because of their importance, they are discussed separately. Other common trust services include assurance of integrity of the message and of the date and time at which certain functions were performed ("timestamping"). Often these services are provided with PKI technology by the same provider that issues PKI-based certificates for digital signatures. Other trust services include electronic registered delivery services, website authentication and archiving services.

The law may contain general rules on the legal status of some or all trust services. It may also mandate the use of certain trust services for certain types of transactions.

Special provisions on the use of trust services may also be found in law relating to paperless trade.

## I.C. Privacy and data protection

Privacy and data protection are important elements of the legal landscape of electronic commerce as they may impose conditions to data transfer between the parties. This section is aimed at identifying laws relating to privacy and data protection, with special attention to those relevant to paperless trade.

#### I.C.1 Is there a law on privacy and data protection? If so, what are its features? Is it based on international standards?

Privacy and data protection are notions that may differ depending on regions and contexts. For the purposes of the checklist, privacy and data protection law is the law that sets the condition for the collection of, access to, use and transfer of data as well as for data storage and preservation. Often, that law establishes a dedicated authority for its enforcement.

The content of privacy and data protection laws may vary significantly. States may take inspiration from international standards. At the global level, the Organization for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013* offer a set of relevant principles. At the regional level, the Asia-Pacific Economic Cooperation (APEC) *Privacy Framework 2015* also contains relevant principles that can be implemented through the APEC Cross-Border Privacy Rules (CBPR) System.

Privacy and data protection laws often protect a specific set of data, referred to as personal data, personal information or personally identifiable information. This set of data may include data relevant for paperless trade.

### I.C.2 Does domestic law address the transfer of data abroad?

Privacy law may deal with the transfer of data (including data used in paperless trade) overseas. Often, exporting data is allowed only on the condition that the destination country provides equal data protection. Section 26 of Singapore *Personal Data Protection Act 2012* makes this kind of rule very clear.

> *26. Transfer of personal data outside Singapore*
>
> *1. An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisation provide a standard of protection to personal data so transferred that is comparable to the protection under this Act.*

While *Personal Data Protection Act 2012* is a baseline privacy legislation, it does not supersede other existing statues dealing with the protection of personal data such as the *Banking Act 2008 (Cap. 19)*. Instead, it works in conjunction with them.

Section 26 of the *Personal Data Protection Act 2012*, Regulation 9 of the *Personal Data Protection Regulations 2014* and Paragraph 19 of *the Personal Data Protection Commission* jointly provide a wide range of legal bases and mechanisms for transferring personal data to a country or territory outside Singapore. These measures include the use of contractual agreements to ensure that the recipient overseas is bound legally to provide a comparable standard of protection. The use of a contractual arrangement (bilaterally or regionally) is consistent with Article 7 of the Association of Southeast Asian Nations (ASEAN) *Protocol to Establish and Implement ASEAN Single Window* (ASW) *2015* ("Legal Framework"), to which Singapore is a party.

PART III to VI, Regulation 9(1)(a) and (b) of the *Personal Data Protection Regulations 2014* sets out the requirements for transferring personal data outside Singapore and what constitutes a "legally enforceable obligation" that provides a standard of protection that is at least comparable to the protection under the *Personal Data Protection Act 2012* to personal data transferred overseas pursuant to section 26.

Privacy and data protection in cross-border data transfer may also be governed by industry-specific agreements. For example, the privacy regime in the financial sector may be enforced by a delegated authority that regulates financial institutions and enforces the obligation under the laws governing financial transactions.

In some cases, laws are enacted to permit data flows from commercially significant partners. The European Union Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data – known as the General Data Protection Regulation, or "GDPR" – establishes a system for the transfer of data outside the European Union that may require such legislative action.

### I.C.3 Do international agreements contain provisions relevant to privacy and data protection?

Cross-border provisions on privacy and data protection may also be contained in international agreements such as the electronic commerce chapters of free trade agreements. These provisions, which aim to ensure a level of legal uniformity, require States to develop privacy and data protection laws accordingly and may refer to international principles and guidelines. For example, Article 14.8 of the Comprehensive and Progressive Agreement for Trans-Specific Partnership (CPTPP).

> *14.8. Personal information protection*
>
> *1. … each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies.*
> *[…]*

5. *Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangement to promote compatibility between them.*

International agreements may be bilateral or multilateral, of general application or sector specific.

### I.C.4. Does the law require data localization? If so, does it apply to paperless trade?

The law may prescribe "data localization", i.e. collection, processing and storage of data, or of certain types of data, in a particular jurisdiction. This may be done for security or other reasons. Data localization requirements may also be agreed upon in contracts. Data localization may significantly affect the design and operation of an information system; for instance, it may in practice impede the use of certain technology such as cloud computing.

Provisions on data localization may be found also in free trade agreements (FTA). However, in that case the provisions normally aim to limit the ability of states to require data localization, as this is seen as an obstacle to dataflows. For example, Article 14.13 of the CPTPP.

*14.13. Location of computing facilities*

1. *The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.*
2. *No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.*
3. *Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.*

### I.C.5 Is there any special rules on privacy and data protection for paperless trade?

The notions of data integrity and data protection are usually used in different context. Data integrity has more to do with individual records: do I have a valid PKI certificate giving me assurance that this record has not been tampered with? Data protection has to do with protecting a database: do I have multifactor authentication to access my office email? Privacy is about limits to transfer data. As noted above (I.C.1), general privacy and data protection law could regulate all aspects of protecting personal information, including in paperless trade. However, sector specific laws (such as on banking or customs) may take precedence over general privacy laws. Contractual agreements (for example, with a single window operator) may also be relevant.

### I.C.6 Does the law protect the confidentiality of commercial information in electronic form?

Commercial and trade-related documents may contain information, such as undisclosed know-how and trade secrets, that is confidential. Such information may be useful, for example, for marketing, supply-chain management or manufacturing purposes.

Confidentiality protects information from unauthorized access, use or disclosure that could be prejudicial to businesses' interest. General laws on commercial confidentiality may apply to information in any form, including electronic. Specific laws on confidentiality of electronic information may also exist.

In Singapore, section 28 of the *Electronic Transaction Act 2010 (Cap. 88)* imposes confidentiality obligations where information is obtained in the performance of duties or exercise of powers under the Act.

> *28. Obligation of confidentiality*
>
> *1. No person shall disclose any information which has been obtained by him in the performance of his duties or the exercise of his powers under this Act, unless such disclosure is made –*
>
> *a. With the permission of the person from whom the information was obtained or, where the information is the confidential information of a third person, with the permission of the third person;*
>
> *b. For the purpose of the administration or enforcement of this Act;*
>
> *c. For the purpose of assisting any public officer or officer of any other statutory board in the investigation or prosecution of any offence under any any written law;*
>
> *d. Or in compliance with the requirement of any court or the provision of any written law.*
>
> *2. For the purposes of this section, the reference to a person disclosing any information includes his permitting any other person to have access to any electronic record, book, register, correspondence, information, document or other material which has been obtained by him in the performance of his duties or the exercise of his powers under this Act.*
>
> *3. Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both.*

Moreover, specific provisions may apply to certain instances, for example, disclosure of information submitted to an electronic single window. Australia has adopted a provision for protecting confidential information submitted in accordance with the *Customs Act 1901* (Cth) from unauthorized disclosure, including information whose disclosure could prejudice the competitive position of the person providing the information.

> *233BABAF. Using information held by the Commonwealth*
>
> *1. A person commits an offence if:*
>
> *a. the person obtains information; and*
>
> *b. the information is restricted information;*
>
> *c. the person uses the information to commit an offence against a law of Commonwealth, a State or a Territory.*
>
> *Penalty: Imprisonment for 2 years or 120 penalty uses, or both.*
>
> *4. In this section:*
>
> *restricted information means information:*
>
> *a) held in a computer owned, leased or operated by the Commonwealth for use for the purpose of the Customs Act: and*
>
> *b) to which access is restricted by an access control system associated with a function of the computer.*

Liability for disclosure of confidential information may arise from statutory or contractual provisions. Either civil or criminal liability is possible, or both.

### I.C.7 Are there provisions on cybercrimes that are applicable to paperless trade?

Many countries have established general penalties against abusive access or alteration and other misuse of the information stored, communicated, or processed by a computer system or network. General cybercrime law could apply also to unauthorized access to information held in paperless trade systems.

In some cases, dedicated provisions may exist. Articles 30 to 33 of the *Electronic Trade Facilitation Act 2015* of the Republic of Korea impose criminal sanctions for various abuses of the information of an electronic trade infrastructure business entity, which is an entity designated to manage an information system that "intermediates, keeps and certifies electronic trade documents by systematically interlinking traders with trade-related agencies through information and communications networks".

*30. (Penalty Provisions)*

*(1) Any of the following persons shall be punished by imprisonment with labor for not more than ten years or by a fine not exceeding 100 million won:*

*1. A person who forges or alters any electronic trade document recorded in the computer files of an electronic trade infrastructure business entity, a person sending or receiving electronic trade document, a trader, or a trade-related agency, or any trade information entered in their database, or uses any forged or altered electronic trade document or trade information, in violation of Article 20 (1);*

*2. A person who has a certificate under Article 17 (1) issued by means of information processing, etc. after entering false information or improper orders in a computer or any other information processing device of an electronic trade infrastructure business entity, in violation of Article 20 (2).*

*(2) A person who attempts to commit a crime as described in paragraph (1) shall be punished.*

*31. (Penalty Provisions)*

*Any of the following persons shall be punished by imprisonment with labor for not more than five years or by a fine not exceeding 50 million won:*

*1. A person who conducts the business affairs provided for in Article 6 (2) 1 through 3 without having been designated as an electronic trade infrastructure business entity, in violation of Article 6 (3);*

*2. A person who damages any electronic document recorded in the computer files of an electronic trade infrastructure business entity, a person sending or receiving electronic trade document, a trader, or a trade-related agency, or any trade information entered in their database, or infringes on their business secret, in violation of Article 20 (3);*

*3. A person who divulges or abuses any confidential information pertaining to electronic trade documents or trade information that he/she has become aware of in conducting business, in violation of Article 20 (4);*

*4. An electronic trade infrastructure business entity who fails to keep electronic documents or databases for three years, in violation of Article 20 (5).*

*32. (Penalty Provisions)*

*A person who conducts business affairs falling under any subparagraph of Article 12 (1) by means of electronic documents without using electronic trade infrastructure in violation of the proviso to Article 12 (1) shall be punished by a fine not exceeding 20 million won.*

*33. (Joint Penalty Provisions)*

*If the representative of a corporation, or an agent, or employee of, or any other person employed, by the corporation or an individual commits any violation falling under any of Articles 30 through 32 in conducting business affairs of the corporation or individual, not only*

*shall such violator be punished, but also the corporation or individual shall be punished by a fine referred to in the relevant provisions: Provided, That this shall not apply to cases where such corporation or individual has not negligent in giving due attention and supervision concerning the relevant duties in order to prevent such offence.*

## I.D. Data sharing

Paperless trade systems are often built around the notion of a single window for customs operations, which involves collecting trade-related data and documents and sharing them among participants. This process raises delicate issues. Besides general rules on privacy, data protection and data retention, specific legal texts may address data sharing, especially among public entities.

### I.D.1 Are there agreements or policies for collecting, accessing, using and sharing data among government agencies participating in a paperless trade system?

Electronic facilities such as single windows aim at sharing information between traders and government and among government entities. In many cases, the right of a public body to obtain information is set in the law.

The use of electronic means for information collection and sharing may require additional safeguards. Hence, besides the general privacy and data protection law, a country may have laws or regulations governing collection, access, use and sharing of data among government agencies. These actions may be governed by a general public sector privacy statute. Often, however, such rules apply to specific contexts, such as single windows for customs operations or similar facilities relevant to paperless trade. These interactions may also be managed through Memoranda of Understanding (MoUs).

Moreover, the law may designate the conditions under which dedicated systems for exchange of trade-related information may be established and operated in an efficient and secure manner. For example, the *Electronic Trade Facilitation Act 2015* of the Republic of Korea (discussed in I.C.7).

The conditions on and limits to collecting and sharing data among government agencies may vary significantly, especially if a general privacy and data protection law does not exist or does not apply to those agencies. For instance, one common and important rule limits data sharing for purposes other than those for which it was originally collected. It is therefore important to describe the main elements of the regime in place.

## I.E. Data retention and electronic evidence

The legal effect of electronic records often depends on their evidentiary value, i.e. the ability to use those records before a court to substantiate a legal claim. This section is aimed at clarifying which retention and evidence rules apply.

### I.E.1 Does the law establish general requirements for data retention, including a minimum and maximum retention period? Do they apply to electronically-stored data?

Data retention laws aim to ensure storage of data in a manner that allows its future use, including use as evidence in the context of dispute resolution and (criminal and administrative) law enforcement. The period for which the information should be retained is usually set by other laws, for instance those on the limitation of actions due to the passing of time. That period may be different for different functions of the document (for example, as evidence of a contract or as the basis for taxation).

The ETLs may contain a general rule on data retention. Article 10 of the MLEC sets criteria for the retention of electronic data, including the format in which data is to be stored.

*10. Retention of data messages*

*1. Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:*

*a) the information contained therein is accessible so as to be usable for subsequent reference; and*

*b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and*

*c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.*

Evidence law may contain additional requirements (see I.E.4).

The law may also set specific retention requirements for trade-related information. For instance, Article 5 of the *Framework Act on Electronic Documents and Transactions 2016* of the Republic of Korea provides general requirements for retention of electronic documents, including trade documents.

*5. Storage of electronic documents*

*1. Where an electronic document meets the following requirements, the storage of such electronic document may take the place of the storage of the document provided for in the relevant statutes:*

*a. that the content of the electronic document shall be available for public perusal;*

*b. that the electronic document shall be kept in the same form as when prepared, transmitted, or received or in a form reproducible same as the aforementioned form;*

*c. where matters concerning an originator, an addressee, and the time of transmission or receipt of the electronic document are included therein, such matters shall remain therein.*

Article 16 of *Electronic Trade Facilitation Act 2015* of the Republic of Korea gives legal recognition to electronic documents kept in the national trading platform by reference to the *Framework Act on Electronic Documents and Transactions 2016* and the *Digital Signatures Act 1999.*

*16. Validity of electronic trade documents kept by electronic trade infrastructure business entities*

*1. Where an electronic trade infrastructure business entity keeps electronic trade documents, such electronic trade documents shall be deemed to have been kept pursuant to Article 5 (1) of the Framework Act on Electronic Documents and Transactions.*

*2. Where an electronic trade infrastructure business entity intends to use its digital signature in order to keep electronic trade documents, it shall use its certified digital signature under subparagraph 3 of Article 2 of the Digital Signature Act.*

The retention period for electronic records may also be specified for some purposes by specialized laws. For example, in Australia, data submitted for the purpose of customs operations needs to be retained in the single window for five years pursuant to section 126DC of the *Customs Act 1901* (Cth).

*126DC. Records of certain electronic communication*

*1. The Comptroller-General of Customs must keep a record of each electronic communication made as required or permitted by this Act. The Comptroller-General of Customs must keep the record for 5 years after the communication is made.*

Additional requirements relevant for data retention may be contained in privacy and data protection law. Those requirements normally align with other obligations to retain information, for instance by not requiring destruction of information that may have legal value.

### I.E.2 Does the law require or favour the use of specific trust services or service providers for data retention?

The law may require the use of specific trust services or trust service providers for data retention. The law may also mandate the use of specific technical standards or of technology such as PKI certificates that ensure the integrity of a data message from a certain point in time. Those requirements may be of general application or apply to specific areas and business sectors. Satisfaction of those requirements may be a condition for legal recognition of stored data or could introduce a legal presumption of validity for a given purpose.

For instance, Article 31-6 of the *Framework Act on Electronic Documents and Transactions 2016* of the Republic of Korea indicates that storage of data in an electronic document centre designated under Article 31-2 of the same Act is presumed to comply with the general storage requirements contained in Article 5 of that Act (see above).

> *31-6. Effect of storage through authorized electronic document centers*
>
> *Where an authorized electronic document center stores electronic documents, such electronic documents shall be deemed stored under Article 5 (1) or (2).*

Specific requirements for data retention of trade-related documents may be found in the technical specifications of the facilities used for trade facilitation. In turn, those specifications normally comply with the requirements for data retention set in general law, unless an exception is specified.

### I.E.3 Do data custodians, such as data centres, assume liability for loss or damage to electronically stored information? Is such liability contractual, statutory or both?

Agreements with trust service providers offering data storage services may define the liability of those providers in case of loss or other damage to stored data. Those agreements often contain clauses limiting liability.

Moreover, the liability of the trust service providers may be limited by statute, in general terms or with respect to the use of specific service providers, or of specific technologies or solutions. The law may also define other elements of the liability regime such as the allocation of the burden of proof.

For instance, Article 31-16 of the *Framework Act on Electronic Documents and Transactions 2016* of the Republic of Korea indicates that, in case of loss arising from storage of electronic documents, a certified electronic document centre operator shall compensate the user who has suffered the loss unless the operator can prove that the loss did not arise from its negligence or wilful misconduct. This provision has the effect of reversing the ordinary rule on burden of proof, which requires that the person who has suffered the loss should prove the negligence or wilful misconduct of the operator.

> *31-16. Liability for compensation and purchasing insurance*
>
> *1. When a certified electronic document centre has inflicted a loss on a user in connection with the storage of electronic documents, etc., it shall compensate the user for such loss: provided, that where the certified electronic document centre has proved that there is no intention or negligence on its part, this shall not apply.*

The liability regime under contract law aims usually at providing monetary compensation. It does not affect the application of administrative and criminal sanctions.

The liability issues related to operations of cross-border paperless trade systems, including single window, will be discussed in IV.B.

### I.E.4 Is electronic evidence admissible in judicial and other proceedings?

The ETLs may provide at a general level for the admissibility of data messages as evidence in legal proceedings and for their evidential value. The evidential value of the data messages may depend on whether they are generated, retained or communicated in a reliable manner.

Article 9(1) of the MLEC extends the principle of non-discrimination against electronic means to the admissibility and evidentiary value of data messages.

> *9. Admissibility and evidential weight of data message*
>
> *1. In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:*
> *a. on the sole ground that it is a data message; or,*
> *b. if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.*

Article 9(2) of the MLEC sets general conditions regarding when data messages shall be given due evidential weight.

> *9. Admissibility and evidential weight of data message*
>
> *2. Information in the form of data message shall be given due evidential weight. In assessing the evidential weight of data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.*

Additional rules are often inserted in evidence laws. Those rules may contain presumptions or specify how evidence should be taken. For example, section 161 of the Australian *Evidence Act 1995* (Cth).

> *161. Electronic communications*
>
> *(1) If a document purports to contain a record of an electronic communication other than one referred to in section 162, it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that the communication:*
>
> *(a) was sent or made in the form of electronic communication that appears from the document to have been the form by which it was sent or made; and*
>
> *(b) was sent or made by or on behalf of the person by or on whose behalf it appears from the document to have been sent or made; and*
>
> *(c) was sent or made on the day on which, at the time at which and from the place from which it appears from the document to have been sent or made; and*
>
> *(d) was received at the destination to which it appears from the document to have been sent; and*
>
> *(e) if it appears from the document that the sending of the communication concluded at a particular time—was received at that destination at that time.*
>
> *(2) A provision of subsection (1) does not apply if:*
>
> *(a) the proceeding relates to a contract; and*
>
> *(b) all the parties to the proceeding are parties to the contract; and*
>
> *(c) the provision is inconsistent with a term of the contract.*

*Also, see section 116A of the Evidence Act 1997 (Cap. 97)* (Singapore), *See original text for illustrations.*

*116A. Presumptions in relation to electronic records*

*(1) Unless evidence sufficient to raise doubt about the presumption is adduced, where a device or process is one that, or is of a kind that, if properly used, ordinarily produces or accurately communicates an electronic record, the court shall presume that in producing or communicating that electronic record on the occasion in question, the device or process produced or accurately communicated the electronic record.*

*(2) Unless evidence to the contrary is adduced, the court shall presume that any electronic record generated, recorded or stored is authentic if it is established that the electronic record was generated, recorded or stored in the usual and ordinary course of business by a person who was not a party to the proceedings on the occasion in question and who did not generate, record or store it under the control of the party seeking to introduce the electronic record.*

*(3) Unless evidence to the contrary is adduced, where an electronic record was generated, recorded or stored by a party who is adverse in interest to the party seeking to adduce the evidence, the court shall presume that the electronic record is authentic in relation to the authentication issues arising from the generation, recording or storage of that electronic record.*

*[(4)]*

*(5) The Minister may make regulations providing for a process by which a document may be recorded or stored through the use of an imaging system, including providing for the appointment of one or more persons or organisations to certify these systems and their use, and for any matters incidental thereto, and an "approved process" in subsection (6) means a process that has been approved in accordance with the provisions of such regulations.*

*(6) Where an electronic record was recorded or stored from a document produced pursuant to an approved process, the court shall presume, unless evidence to the contrary is adduced, that the electronic record accurately reproduces that document.*

*[(7)]*

Finally, laws governing paperless trade may have dedicated provisions on evidence. For example, section 126DC of the Australian *Customs Act 1901* (Cth) makes provision for the evidentiary value of electronic records stored in the single window system.

*126DC. Records of certain electronic communications*

*(1) The Comptroller-General of Customs must keep a record of each electronic communication made as required or permitted by this Act. The Comptroller-General of Customs must keep the record for 5 years after the communication is made.*

*Note: It does not matter whether the communication is made to the Department or by the Department or a Collector.*

*Evidentiary value of the record*

*(2) The record kept is admissible in proceedings under this Act.*

*(3) In proceedings under this Act, the record is prima facie evidence that a particular person made the statements in the communication, if the record purports to be a record of an electronic communication that:*

*(a) was made to the Department; and*

*(b) met the information technology requirements that the Comptroller-General of Customs has determined under section 126DA have to be met to satisfy a requirement that the person's signature be given to the Department in connection with information in the communication.*

*(4) In proceedings under this Act, the record is prima facie evidence that the Department or a Collector made the statements in the communication, if the record purports to be a record of an electronic communication that was made by the Department or a Collector.*

**I.E.5 Is electronic evidence that is generated, stored or collected abroad admissible? If so, under which conditions?**

Evidence law seldom has specific rules on the admissibility of evidence generated or stored abroad.

The law may refer to the intrinsic evidentiary value of the data message without discriminating due to foreign elements, akin to what happens with paper-based documents. In that case, the evidentiary value of domestic and foreign data messages will be assessed on the same criteria. Recognition the evidentiary value of foreign data messages may also be possible on the basis of bilateral or multilateral treaties.

On the other hand, the law may set national requirements for the admissibility of electronic evidence that bar the recognition of foreign evidence. This may happen in particular if special evidentiary weight is given to digital signatures that are subject to national regulation. See the discussion of cross-border recognition of electronic signatures in part I.B.4.

# II. Laws regarding paperless trade system

## II.A. Establishment of a paperless trade system

The establishment and operation of a paperless trade system often requires a set of dedicated laws and regulations. This section is aimed at identifying those laws and regulations as well as the basic features of governance of the paperless trade systems.

A country may aim to set up a paperless trade system pursuant to various trade agreements such the Trade Facilitation Agreement (TFA) of the World Trade Organization (WTO) but may not yet have one. In that case, it is important to establish a legal basis for the implementation and operation of the paperless trade system. In other cases, the paperless trade system may be still at the planning and development stage, or a pilot project. In such instances, the legal readiness checklist may be read as an introduction to various legal issues that need to be addressed to operate a paperless trade system and as a tool to identify legal gaps.

The legal readiness checklist refers, where possible, to international legal standards, such as UNCITRAL texts, to facilitate the achievement of cross-border legal recognition and technical interoperability. In addition to international legal standards, a country may need to adopt multilateral, regional (such as ASW) or bilateral agreements to enable cross-border operation of its paperless trade system.

**II.A.1 Does a dedicated paperless trade system, such as a single window, exist? If so, what legal instruments are used to establish and operate it? How do these instruments define the rights and obligations of the participants?**

Many countries have established dedicated systems for the exchange of trade-related information in electronic form (here referred to as a "paperless trade system"). Most of them will refer to this system as a "single window". However, single window may describe very different platforms, systems and environments, including outside the paperless trade context. United Nations Economic Commission for Europe (UNECE) Recommendation No. 33 contains a definition of single window for trade purposes.

*"a facility that allows parties involved in trade and transport to lodge standardized information and documents with a single entry point to fulfill all import, export, and transit-related regulatory requirements." "If information is electronic, then individual data elements should only be submitted once"*

Most trade single windows are built around the notion of submission of information from traders to regulatory agencies such as customs. However, the paperless trade environment may be more comprehensive (such as the TradeTrust system of Singapore that deals with both Business to Business - B2B and Business to Government - B2G exchanges); in the latter case, reference is made to a "national trade platform".

Paperless trade systems, including single windows, require enabling laws and regulations. This question focuses on those laws and regulations that authorize establishment and operation of a paperless trade system. These laws also generally define the rights and obligations of all participants (such as importers, exporters, licensees, and licensing agencies) or some smaller sub-set of those participants. They may also specify if the system operator may be liable for its operations, and limitations of such liability. Alternatively, the liability of the system operator may be based on general rules.

Article 1(5) of the *Electronic Trade Facilitation Act 2015* of the Republic of Korea is an example of law establishing a paperless trade system (called "electronic trade infrastructure").

*1(5). Purpose*

*The term "electronic trade infrastructure" means an information system that intermediates, keeps and certifies electronic trade documents by systematically interlinking traders with trade-related agencies through information and communications networks.*

In Australia, section 126D of the *Customs Act 1901* (Cth) explicitly empowers the Comptroller-General of Customs to establish and operate the integrated cargo system (ICS).

*126D. Comptroller-General of Customs to maintain information system*

*The Comptroller-General of Customs must establish and maintain such information systems as are necessary to enable persons to communicate electronically with the Department.*

Section 126DB of the *Customs Act 1901* (Cth) imposes the burden of proof on the traders who allege the misfunction of or failure to comply with official information technology requirements, or who say they have officially reported the failure.

*126DB. Authentication of certain electronic communications*

*An electronic communication that is made to the Department and is required or permitted by this Act is taken to be made by a particular person, even though the person did not authorise the communication, if:*

*(a) the communication meets the information technology requirements that the Comptroller-General of Customs has determined under section 126DA have to be met to satisfy a requirement that the person's signature be given to the Department in connection with information in the communication; and*

*(b) the person did not notify the Department of a breach of security relating to those information technology requirements before the communication;*

*unless the person provides evidence to the contrary.*

Important additional terms and conditions relating to paperless trade systems may be included in contractual agreements such as "end-user agreements" and "service-level agreements".

### II.A.2 Which government agencies participate in the paperless trade system? On what legal basis?

A paperless trade system may deal only with B2G exchanges (single window) or include also B2B exchanges (national trade platform). While the goal of a single window is to link all relevant public agencies, countries may

implement it in phases, typically starting with those that are more often involved in import/export transactions. Additional government agencies may join the system at each subsequent phase.

The pace of expansion of the single window is set in legal and policy documents, which often also contain the basis for information-sharing. In the absence of a framework document, coordination between government agencies participating in the single window may be achieved with MoUs.

> *For example, Armenia's single window system aims to offer mainly customs-related services at the initial stage and to later integrate import/export permit issuing agencies. The Presidential Decree of Uzbekistan No. UP-5582 about "additional measures for enhancement of customs administration and increase in efficiency of activities of bodies of the State Customs Service of the Republic of Uzbekistan" of 24 November 2018 requires that a single window be made available on customs terminals for all of the following functions: customs, banking, logistics, laboratory, phytosanitary, veterinary, sanitary, epidemiological ecological, certifications and other services.*

#### II.A.3 Is there a central body tasked with setting up and managing the paperless trade system?

Often, a public entity is tasked with coordinating the design and implementation of the paperless trade system. If the paperless trade system is planned to be implemented in phases, that entity is responsible for coordinating the implementation of each phase.

The customs authority is often considered well suited to take the lead role as it often receives information on paper at the border posts. Private or semi-private entities may also be tasked with coordination functions, for instance when the paperless trade system is funded as a public-private partnership. In the latter case, special rules may address sharing data originating from law enforcement agencies or other agencies with the power to compel disclosure of information to them.

The coordinating agency may operate in consultation with a national coordinating committee, which may include private sector representatives.

The central coordinating body and related entities may have a dedicated budget for their activities. The availability of that budget may be particularly relevant when setting up the paperless trade system. Moreover, the operation of the paperless trade system may be self-funded (i.e. by fees from users) or rely on other financial support (or a combination of the two).

## II.B. Quality of information exchanged with the paperless trade system

The main function of the paperless trade system, including the single window, is to facilitate the exchange of trade-related data and documents in electronic form. The information is originally submitted on paper or electronically by commercial operators that have a duty to make complete and correct statements. Moreover, in an electronic environment, there could be special procedures to attribute the declarations originating from the various participants. Electronic signatures may play a significant role in the attribution of the declarations.

#### II.B.1 Does the law on the substantive requirements of trade-related data and documents also apply to paperless trade?

The verification of the compliance of import/export operations with the law is based on the declarations of the traders or of their agents, such as customs brokers. Accordingly, laws and regulations on customs operations require the submission of accurate trade-related information, including with respect to its attribution. At a minimum, the normal rule is that information submitted should be complete, accurate and up to date. This is intended to permit customs and other law enforcement agencies to carry out their functions, to ensure compliance with regulations and to investigate allegations of non-compliance.

The use of electronic means normally does not alter the substantive content of the information to be provided. In other words, substantive information requirements do not change depending on the medium used (paper or

electronic). The duties of the entity filing the information is in principle the same in all cases. It is therefore important to identify any such difference and its justification.

**II.B.2 Are there specific rules for the exchange of trade-related data and documents in electronic form?**

Specific rules are sometimes needed to adapt paper-based procedures for submission of information to paperless trade. As a result, one sees not only the general rules on the use of electronic communications, but also special rules dealing with controls over data input processing, responsibility for data transmission and processing, and audit trails and recording mechanisms.

Often, customs laws are designed to operate in a paper-based environment and later adapted to paperless trade. In other cases, only electronic submissions are possible. For example, section 96 of the Singapore *Customs Act 2004 (Cap. 70)* makes the use of electronic communications mandatory and imposes the standards for accuracy and completeness that apply to documents on paper.

> *96. Declaration to give a full and true account*
>
> *1. The declaration referred to in sections 37 (declaration), 59 (removal of dutiable goods from Customs control) and 80 (declaration by claimant) shall, unless the Director-General allows under subsection (2), be made and submitted by an electronic notice in accordance with section 86 (computer service) and such declaration shall give a full and trust account of such particulars as are required by the Director-General.*
> *2. The Director-General may, in his discretion and subject to such conditions as he may impose, allow any declaration referred in sections 37, 59 and 80 to be made on a form determined by the Director-General.*
> *3. Such declaration shall –*
> *a. Give a full and true account of the particulars for which provision is made in the form; and*
> *b. Be in duplicate or in such other number of copies as the person to whom the declaration is required to be made may direct.*

If a country does not have laws expressly directed at paperless trade, it may have laws and regulations of general application that apply as well to paperless trade and that enable – among other things – submission and processing of electronic information and ensure its integrity and security.

A critical element of these rules when applied to paperless trade is the identification of the source of the information, i.e. its attribution. As noted above (section II.B.1), attribution is critical for law enforcement as well as normal commercial relations. On paper, attribution is carried out with signatures and seals on the sheet containing the information. In an electronic environment, attribution is often achieved with electronic signatures, which, in some cases, may also provide assurance of the integrity of the data message. Other metadata and textual content may also help show attribution of an electronic document.

The paperless trade system may rely on the general rules on electronic signatures or may specify its own rules. In both instances, these rules may be technology neutral or technology specific (see section I.B).

## II.C. Service-level agreements and memorandums of understanding

A number of legal texts, such as service-level agreements, memorandums of understanding, end-user agreements and other contractual agreements, are relevant to the operation of a paperless trade system. These legal texts define the obligations of the participants in the paperless trade system. For instance, service-level agreements define the obligations of the service provider with respect to the availability of the system, response time, processing time and other technical requirements that are critical to define to ensure the availability and smooth operation of the system.

**II.C.1 Are there service-level agreements or memorandums of understanding governing paperless trade operations? If so, who are the parties and what is the legal authority for concluding these agreements?**

A service-level agreement (SLA) is a contract between the provider and the user of a service that identifies the services covered by the contract and the minimum level of service expected under the contract. This is usually done by specifying performance standards, including the methods by which their achievement is measured. The SLA is legally binding, unlike a service level objective, which describes a goal in service delivery and may not bind the service provider.

In the paperless trade context, the term SLA may refer to a contract between the paperless trade system operator and its service providers (for example, a cloud computing service provider; a trust service provider). It may also refer to a contract between a paperless trade system operator, for example, the operator of a national single window that is a private entity, and a client public entity (for example, customs as the agency with coordinating responsibilities for the paperless trade system). The SLA is governed by contract law, including with respect to liability and its limitations. Like all contracts, the SLA is subject to laws of mandatory application, including any special regulation on paperless trade. As noted above, the SLA aims at specifying the expected quality of service by establishing performance benchmarks. It may also contain contingency plans and procedures.

The relationship between a public operator of a national single window (for example, customs) and other public entities participating in the paperless trade system (for example, Ministry of Agriculture) may be regulated under a MoU or other administrative law instrument, notably with respect to information exchange among government agencies.

The SLA is distinct from an "end-user agreement", which is a contract between the paperless trade system operator and the users of the system (usually, private sector actors such as traders, freight forwarders, agents, banks, etc.) defining the terms and conditions of use of the system.

> *Publication: Record, Richard; McLinden, Gerard; Siva, Ramesh. 2013. Lao PDR - Preparation of a national single window: a blueprint for implementation (English). Washington DC; World Bank contains a sample SLA between a private sector paperless trade system operator and a public entity (Annex D, Appendix A, referred to as "SLA for LNSW Operational Services") as well as a sample end user agreement (Annex D, Appendix B, referred to as "SLA between LNSW Operator and Traders").*

# III. Cross-border aspects

## III.A. International agreements relevant for cross-border paperless trade facilitation

### III.A.1 Which international agreements relevant to paperless trade facilitation are in force in your country?

Countries may give legal recognition to foreign electronic communications or documents on the basis of reciprocity, which leads to mutual recognition of each other's electronic communications or documents. Alternatively, a country may also unilaterally give legal recognition to electronic communications or documents that originate in another country.

As seen above (sections I.B. to I.E.), domestic laws may contain provisions regarding the validity and effect of foreign electronic communications and signatures, the transfer of data across borders, etc.

This section focuses on international law instruments, i.e. instruments binding under international law that may be called a "convention", a "treaty," etc.

International law instruments may deal directly with the legal status of electronic communications or documents exchanged across borders. The ECC is such an instrument.

International law instruments may also contain provisions specific to cross-border paperless trade facilitation. Such instruments may be of global scope, like the WTO's TFA, regional or bilateral. They may concern broader areas of trade relations (for example, FTA), and take a high-level approach. Article 14.9 of the CPTPP, for instance, sets high-level goals for paperless trading in the member States.

*14.9. Paperless trading*

*Each Party shall endeavour to:*

*a. make trade administration documents available to the public in electronic form; and*
b. *accept trade administration documents submitted electronically as the legal equivalent of the paper version of those documents.*

Alternatively, those international agreements may focus on specific areas and concentrate on selected uses of electronic records, such as customs and electronic payments.

Transport or transit-related conventions that recognize the use of electronic equivalents of paper-based documents are a specific sub-set of international agreements relating to paperless trade facilitation.

One example of such conventions is the Additional Protocol to the Convention on the Contract for the International Carriage of Goods by Road (CMR) concerning the Electronic Consignment Note.

Many other areas of the law are important to cross-border paperless trade facilitation. Some of them are standardization of electronic trade documents, consumer protection and privacy, cybercrime, electronic evidence, government procurement, investment and taxation. As a result, countries may bilaterally, multilaterally or regionally negotiate agreements to address these areas of laws.

For example, Singapore has recently concluded Digital Economy Partnership Agreements with other countries (Australia, Chile and New Zealand) made of different "modules", in the form of MoUs. One of those MoUs deals with the Digital Economy in general; another, on Trade Facilitation aims, to develop compatible paperless trading systems. Further, the MoU on Cooperation for Electronic Invoicing aims to expand electronic invoicing interoperability. The MoU on Cooperation in Personal Data Protection aims to protect personal information and uphold individuals' privacy rights as data flows across borders.

All international agreements that may impact paperless trade facilitation and that are in force in your country are relevant.

If the agreements set out rules or technical standards that foreign electronic communications or signatures must meet in order to be recognized in your country, please mention them. If the agreements require domestic legislation to implement them, please mention that legislation (or its absence).

It may be particularly helpful to identify the types of electronic exchanges and documents that are permitted by these agreements (for example, certificates of origin; electronic invoices), and any differences between legal requirements for domestic and for international electronic exchanges and documents.

### III.A.2 Are there technical or operational international agreements providing for legal recognition of electronic communications or documents?

The implementation of certain trade facilitation treaties may call for the adoption of technical or operational agreements. This is for instance the case with the ASEAN Trade in Goods Agreement (ATIGA) electronic Form D to implement the exchange of electronic certificates of origin in the ASW.

While these agreements engage States and have international legal nature, their conclusion may be delegated to technical bodies as they are meant to operate under the umbrella of a framework agreement.

Some of these agreements apply only to certain types of transactions (such as B2B or B2G) or to specific types of documents or trust services (such as digital signatures). Some of them may be technology neutral while others are technology specific.

These agreements have significant practical relevance as they represent the link between high-level legal statements and their technical implementation.

**III.A.3 Are contracts used to provide for mutual recognition of electronic communications and signatures?**

Trading partners may agree on the legal status of electronic communications exchanged across borders, within the limits of mandatory law. A number of tools are available to that end. EDI cross-border agreements are one of them. Others include federated identity schemes that provide a common contractual reference for the use of certain trust services, including electronic signatures.

Some of these contractual arrangements aim to legally enable the cross-border use of trade, logistics and customs electronic documents. This may be done by using PKI-based trust services, especially digital signatures. In that case, such agreements normally describe the standards that the certifying authorities must meet in each country for the recognition of their services as trusted intermediaries (i.e. their "trust services").

> The PAA offers an example of a private consortium that uses mutual recognition contractual agreements under which digital signatures issued in one country in compliance with the requirements of the consortium are accepted by other members of the consortium.

If any such agreement is used in your country, please describe its scope and content.

## III.B. International standards, guidelines and recommendations

**III.B.1 Which standards, regulations or guidelines are in use for the cross-border exchange of trade-related electronic communications?**

A country may have the possibility or the obligation under a trade agreement to use international technical standards for carrying out import, export, or transit formalities and procedures in electronic form. Article 10.3 of the WTO TFA is an example of such agreement. The use of international standards promotes cross-border interoperability and, ultimately, the seamless flow of data.

> *10.3. Use of international standards*
>
> *3. Members are encouraged to use relevant international standards or parts thereof as a basis for their import, export, or transit formalities and procedures, except as otherwise provided for in this Agreement.*

Also, see Article 9 of the Framework Agreement on Facilitation of Cross-Border Paperless Trade in Asia and the Pacific (FA-PT).

> *9. International standards for exchange of trade-related data and documents in electronic form*
>
> *1. The Parties shall endeavour to apply international standards and guidelines in order to ensure interoperability in paperless trade and to develop safe, secure and reliable means of communication for the exchange of data.*
>
> *2. The Parties shall endeavour to become involved in the development of international standards and best practices related to cross-border paperless trade.*

These international standards are produced by international organizations such as the UNECE, the World Customs Organization (WCO), the WTO, the International Telecommunications Union (ITU) and the International Organisation for Standardisation (ISO).

Some standards may be regional, for example, those prepared by the APEC. One example of such standards is the WCO SAFE Framework of Standards to Secure and Facilitate Global Trade. These standards relate often to technical matters and to business processes; they may however also have legal implications.

# IV. Other considerations

## IV.A. Ownership of information in the paperless trade system

Paperless trade facilitation involves the collection and exchange of a large amount of information. Delicate issues arise with respect to data subject rights, confidentiality and other rights on that information. For instance, the paperless trade system operator may acquire the right to use, analyse and redistribute the information submitted to the system. In other cases, the system may be designed to avoid the storage of any information, so as to simplify compliance with privacy and data retention laws.

### IV.A.1 What defines rights regarding information exchanged in the paperless trade system, the law or contractual agreements?

Private sector participants in paperless trade, government agencies, service providers, other intermediaries and other third parties (such as a software developer) may have some type of interest (such as intellectual property) in the information exchanged, filed or stored in the paperless trade system. For instance, government agencies that participate in a trading system may have rights in the information retained in the system. Clear legislative and contractual rules governing the use and redistribution or sharing of information submitted to a paperless trade system are therefore important for its operation.

Laws, regulations and contractual arrangements may spell out the rights to information exchanged in a paperless trade system, including access and control. In particular, laws on the protection of business secrets as well as on enforcement of intellectual property rights, including under Part III of the WTO Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, may affect the rights to information exchanged in the paperless trade system.

For example, the information submitted to a paperless trade system may need to be kept confidential and not be disclosed or otherwise be made available to others without a valid reason (such as a regulatory interest) and consistently with the purpose of the submission.

Section 89 of the *Customs Act 2004 (Cap. 70)* (Singapore) prohibits information collected for a specified and lawful purpose from being shared for another purpose without prior consent of the supplier of the information, unless such sharing is required for a specific purpose authorized by law.

Further, section 28 of the *Electronic Transactions Act 2010 (Cap. 88)* (Singapore) specifies the conditions under which information collected in the performance of duty can be used and disclosed.

> *28. Obligation of confidentiality*
>
> *1) No person shall disclose any information which has been obtained by him in the performance of his duties or the exercise of his powers under this Act, unless such disclosure is made —*
> - *a) with the permission of the person from whom the information is obtained or, where the information is the confidential information of a third person, with the permission of the third person;*
> - *b) for the purpose of the administration or enforcement of this Act;*
> - *c) for the purpose of assisting any public officer or officer of any other statutory board in the investigation or prosecution of any offence under any written law; or*
> - d) *in compliance with the requirement of any court or the provisions of any written law.*

Terms and conditions for the use and operation of the paperless trade system may also define the rights to information of the system operator and of other participants. Such contractual terms would therefore limit the ability of the system operator to share information. Any agreement between the system operator and the third-party software developer or vendor may also be relevant to the rights in information exchanged in the paperless trade system.

Please describe any condition and limitation as well relating to the rights to information exchanged in the paperless trade system.

## IV.B. Liability issues related to cross-border paperless trade system

Trading parties and other concerned entities may suffer losses from the incorrect transmission of information and may seek compensation for those losses from those liable for them under contracts among the transacting parties or, if this is not possible, under the general law of civil wrongs. This form of liability is separate from any sanction that may apply under criminal and administrative law.

More often, the law may limit or exclude liability of some actors, usually in order to encourage a certain activity or to lower obstacles to market entry. Limits to liability, in particular to the amount that may need to be paid, are also very common in contracts.

This section deals with liability rules that apply to the principal participants in a paperless trading system: the operators of the system itself (such as a single window); other governmental bodies or agencies with a role in trading; communications intermediaries like Internet service providers or the providers of trust services (such as certification authorities); and other participants in the system (such as customs brokers). The potential liability for each group may differ from that of others in its application or its limitation.

### IV.B.1 May the operator of the paperless trade system be held liable for providing its services?

A paperless trade system should enable accurate and timely information exchange. The performance standards for information exchange may be specified in regulations governing the system or in contractual terms and conditions for the use of the system. If the performance standards are not met, the system operator may be held liable.

Another mechanism to address liability of the operator of a paperless trade system is appropriate limited liability or exclusion clauses, which may be prescribed by law or provided by agreement between the system operator and various users of the system. Such clauses in the agreement limit the liabilities of a system operator and may indemnify it against claims for damages.

### IV.B.2 May government agencies participating in the paperless trade system be held liable for their interaction with the system?

Government agencies participate in the paperless trading system by providing and processing trade-related data for a number of purposes such as goods control, taxes etc. The accuracy and speed of their interaction will affect the efficiency of the system and ultimately of trading operations.

The obligations of government agencies with regard to their participation in the paperless trade system may be spelled out in the legislation establishing the system or in the MoU that they may have concluded to become system participants. Agreements among the participants in the paperless trade system may also contain liability rules for not providing or processing trade-related data correctly.

General law, regulation or similar instruments may provide for the liability of government agencies or for their exemption from liability when performing public functions.

### IV.B.3 May service providers, such as internet service providers and trust services providers, be held liable for interacting with the paperless trade system?

Services provided by specialized technical providers are critical in enabling the exchange of electronic communications. In some cases, the law will specify certain aspects of their liability.

Statutes in many places frequently limit the liability of internet service providers for the information they transmit, especially if they do not originate the information.

See section 26 of the *Electronic Transactions Act 2010 (Cap. 88)* (Singapore) that deals with the liability of various network service providers.

> *26. Liability of network service providers*

1. *Subject to subsection (2), a network service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third-party material in the form of electronic records to which he merely provides access if such liability is founded on –*
    a. *the making, publication, dissemination or distribution of such materials or any statement made in such material; or*
    b. *the infringement of any rights subsisting in or in relation to such material.*

In addition, the law may set forth the basic obligations of certification authorities, which are a special type of trust service provider specialized in offering certificates, often PKI-based, supporting electronic signatures and other services such as timestamping, integrity and registered delivery. It may also specify the consequences for non-compliance with those basic obligations, or for otherwise causing a loss to users and third parties. Article 9 of the MLES offers some general principles of conduct for providers of certificates for electronic signatures.

*9. Conduct of the certification service providers*

1. *Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:*
    a. *Act in accordance with representations made by it with respect to its policies and practices;*
    b. *Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;*
    c. *Provide reasonably accessible means that enable a relying party to ascertain from the certificate:*
        i. *The identity of the certification service provider;*
        ii. *That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;*
        iii. *That signature creation data were valid at or before the time when the certificate was issued;*
    d. *Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise:*
        i. *The method used to identify the signatory;*
        ii. *Any limitation on the purpose or value for which the signature creation data or the certificate may be used;*
        iii. *That the signature creation data are valid and have not been compromised;*
        iv. *Any limitation on the scope or extent of liability stipulated by the certification service provider;*
        v. *Whether means exist for the signatory to give notice pursuant to Article 8, paragraph 1 (b), or this Law;*
        vi. *Whether a timely revocation service is offered;*
    e. *Where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to Article 8, paragraph 1 (b), of this Law and, where services under subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service;*
    f. *Utilize trustworthy systems, procedures and human resources in performing its services.*
2. *A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.*

Service providers will also have obligations under SLAs and contractual agreements and may be held liable accordingly. This contractual liability may be limited to the extent permitted by the applicable law.

### IV.B.4 May other participants in the paperless trade system (for example, customs brokers) be held liable for their interaction with the system or their role in the passage of information or data passing through their systems?

The transition from a paper-based to a paperless trade system does not affect the obligations of participating parties, in particular traders and their agents, with respect to their acts or omissions during customs clearance or other trade-related operations. For instance, a trader who intentionally submits incorrect or false information may

face criminal, administrative and civil sanctions both in the paper-based and in the paperless environment. The law may specify the duty to comply with general obligations when exchanging electronic information.

Section 96 of the *Customs Act 2004 (Cap. 70)* (Singapore) deals with the obligations of a trader or of its agent when interacting electronically with customs.

> *96. Declaration to give a full and trust account*
>
> 1. *The declarations referred to in sections 37, 59 and 80 shall, unless the Director-General allows under subsection (2), be made and submitted by an electronic notice in accordance with section 86 and such declaration shall give a full and true account of such particulars as required by the Director-General.*
> 2. *The Director-General may, in his direction and subject to such conditions as he may impose, allow any declaration referred to in sections 37, 59 and 80 to be made on a form determined by Director-General.*
> 3. *Such declaration shall –*
>  a. *give a full and true account of the particulars for which provision is made in the form; and*
>  b. *be in duplicate or in such other number of copies as the person to whom the declaration is required to be made may direct.*

As with the other participants in the trade and communications chains, statutes may limit or exclude liability of selected service intermediaries in certain circumstances where the lawmakers want to encourage an activity. Likewise, contracts may allocate liability among parties, or eliminate it entirely, when allowed under applicable law.

## IV.C. Dispute settlement and conflict of laws

The following section is aimed at examining the dispute settlement mechanisms for the operators of a single window or other paperless trade system.

### IV.C.1 Do national laws deal with choice-of-forum and choice-of-law issues relevant to paperless trade facilitation?

Domestic disputes are dealt with in national courts or, within the limits allowed by domestic law, by alternative means discussed below.

However, trade relations almost by definition involve participants from more than one country. If the participants have a dispute, for example, about who is responsible for something going wrong, each party may want its own country's law to apply and for its own country's courts to hear the dispute.

Most if not all countries have legal rules to decide who hears a dispute with cross-border elements and with different possible legal regimes.

This question focuses on the degree to which parties to a trade dispute have the choice of "forum", i.e. of the court or the place where the dispute is heard, or a choice of the law to be applied to resolve it, wherever it is heard.

A country may have a regime of "party autonomy", allowing the parties to agree on their choice of law and choice of forum in their international contracts. Such autonomy implies that individuals and legal entities may choose to have the laws or courts, or both, of a foreign country govern their contractual relationship. In almost every case, that foreign country has some connection with the transaction, normally when another transacting party has its place of business there.

Party autonomy may flow from judge-made law or rules of court or may be in applicable statues such as laws on commercial contracts that are sensitive to international standards.

Often, rules on choice of forum and choice of law in international disputes have a uniform nature. The Hague Conference on Private International Law has prepared a number of texts on choice of forum and mutual legal assistance, and UNCITRAL had done significant work on international commercial arbitration. Those texts, which

may take the form of treaties, model laws or model contractual provisions, are often highly relevant for international trade. Article 5 of the *Hague Convention on Choice of Court Agreements 2005* gives (conditional) effect to party autonomy in choosing the forum for international litigation.

*5. Jurisdiction of the chosen court*

1. *The court or courts of a Contract State designated in an exclusive choice of court agreement shall have jurisdiction to decide a dispute to which the agreement applies, unlles the agreement is null and void under the law of that State.*
2. *A court that has jurisdiction under paragraph 1 shall not decline to exercise jurisdiction on the ground that the dispute should be decided in a court of another State.*
3. *The preceding paragraphs shall not affect rules –*
    a. *On jurisdiction related to subject matter or to the value of the claim;*
    b. *On the internal allocation of jurisdiction among the courts of a Contracting State. However, where the chosen court has discretion as to whether to transfer a case, due consideration should be given to the choice of the parties.*

Furthermore, a country may have conventions on the enforcement of foreign judgments and mutual judicial assistance agreements with their foreign counterparts to facilitate the practical enforcement of foreign court judgements in their countries.

While these laws may be of general nature, they normally apply also to cross-border paperless trade. However, a country may have made special provision for these matters in paperless trade, or in trade in any medium.

However, a number of issues relevant to paperless trade are of public, namely administrative, nature, especially when involving public entities such as customs. National laws may insist that such matters be heard within the national justice system. Agreements on cross-border paperless trade may therefore contain special dispute resolution mechanism that take into account the public nature of the parties and interests involved.

Criminal cases are heard in the prosecuting jurisdiction. Cross-border aspects may be limited to mutual legal assistance such as taking evidence abroad, extradition issues, etc.

### IV.C.2 Does the law contemplate alternative means of resolving disputes in international trade such as arbitration and mediation? Are the results of any such means clearly enforceable across borders?

The law often allows, encourages or even requires parties to attempt to resolve their disputes through alternative dispute resolution mechanisms such as conciliation, mediation and arbitration. Sometimes the law sets dispute resolution mechanisms. Often those mechanisms are contained in contractual agreement.

Section 33 of the *Framework Act on Electronic Documents and Transactions 2016* (Republic of Korea) sets rules regarding the use of mediation to solve disputes, requiring compliance with general principles of accessibility and confidentiality of the proceeding and the impartiality and independence of the mediators.

*33. Mediation of disputes*

1. *Any person who intends to obtain a remedy for any loss or seek mediation of a dispute related to an electronic document or electronic transaction may apply for mediation of the dispute to the committee: Provided, that this shall not apply where the mediation of the dispute has been completed in accordance with other Acts.*

Alternative dispute resolutions mechanisms such as arbitration are particularly relevant in international trade due to their perceived neutrality. It is of interest if a country has an arbitration law that follows international standards such as the *UNCITRAL Model Law on International Commercial Arbitration 1985* (amended in 2006). A country may also be a party to the international convention to enforce the results of the arbitration across borders. The *Convention on the Recognition and Enforcement of Foreign Arbitral Award 1958* is the worldwide standard on such matters.

Alternate dispute resolution laws may also limit the ability to use alternative dispute resolution methods when a public entity is involved. Agreements on cross-border paperless trade may therefore contain special dispute resolution mechanism that take into account the public nature of the parties and interests involved.

#### IV.C.3 Are online dispute resolution mechanisms used in paperless trade facilitation?

Online dispute resolution mechanisms, such as online mediation or arbitration, are conducted wholly or partially by electronic means of communications. They may be more or less automated and allow different degrees of visual or audio input by the parties. Because of their convenience and economy, they are increasingly popular to settle disputes relating to electronic commerce.

Online dispute resolution mechanisms may be applied to a range of disputes including paperless trade transactions. Such an online procedure may be based on an agreement between the transacting parties or may be permitted or required by statute.

## IV.D. Electronic payments and electronic transferable records

Electronic payments are the backbone of the digital economy. To the extent that electronic payments are available, they could be incorporated in the paperless trade system. Usually, this is done by using electronic funds transfers, i.e. by ordering a bank to transfer money (wire transfer) or by using credit or debit cards. In other cases, certain commercial documents may be used to perform payment or give guarantee of payment.

#### IV.D.1 Does the paperless trade system accept or initiate electronic payments?

Electronic payment systems are increasingly common in developing countries as elsewhere. Electronic payments may be accepted by a paperless trade system for various purposes such as the payment of customs duties and fees.

Often, limitations apply to the types of electronic payments accepted, for example, by requiring the exclusive use of a payment service, such as a credit or debit card, or of a bank. Alternatively, payments can be made through electronic funds transfers available to the general public or to businesses in general. Please indicate if electronic payments used in the paperless trade system are restricted to a specific method or provider.

It may also be possible that any sum of money due by the paperless trade system operator, or one of its participants, to a user of that system may be transferred electronically under the rules devised especially for that system.

Finally, the use of electronic payments may be restricted to domestic transactions or may extend to payments originating or bound abroad.

Electronic payments may be accepted by public entities on the basis of a law of general application or of a specific provision for paperless trade systems. Section 25 of the *Electronic Transactions Act 2010 (Cap. 88)* (Singapore) contains general provisions for the use and acceptance of electronic payments by public agencies.

> *25. Acceptance of electronic filing and issue of documents*
>
> > *(1) Any public agency that, pursuant to any written law –*
> >
> > > *(e) requires payment of any fee, charge or other amount by any method and manner of payment,*
> >
> > *may, notwithstanding anything to the contrary in such written law, carry out that function by means of electronic record or in electronic form.*
> >
> > *(2) In any case where a public agency decides to perform any of the functions in subsection (1) by means of electronic records or in electronic form, the public agency may specify —*
> >
> > > *(d) such control processes and procedures as may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments*

*(e)any other required attributes for electronic records or payments that are currently specified for corresponding paper documents.*

**IV.D.2 Does the paperless trade system accept electronic transferable records?**

Certain commercial documents incorporate the right to the payment of money or to delivery of goods. These documents are called transferable documents or instruments, or documents of title, and are essential for logistics and trade financing and, more generally, for supply chain management. These documents include bills of lading, bills of exchange, cheques, promissory notes and warehouse receipts, as well as, in certain countries, letters of credit.

In certain countries, the law may allow the use of some of these documents in electronic form. For instance, Article 862 of the *Commercial Act 2016* of the Republic of Korea has been amended to allow the use of bills of lading in electronic form compliant with the "Regulation on Implementation of the Provisions of the Commercial Act regarding Electronic Bills of Lading" and other implementing regulations. This was done to facilitate the full dematerialisation of all commercial documents that may be exchanged in a paperless trade system.

UNCITRAL has prepared the MLETR to legally enable the use of electronic transferable records in comprehensive manner and based on the principles of technology neutrality and functional equivalence.

The inclusion of electronic transferable records in a paperless trade system may indicate that the system performs the broader function of a national trade platform facilitating all types of trade-related electronic exchanges.

## IV.E. Competition laws

The following section is aimed at examining the competition law issues involved in a single window or other paperless trade system.

**IV.E.1 Does a competition law exist? If so, is it applicable to single window operators or other paperless trade services providers?**

The term "competition law" may refer to measures intended to ensure equal opportunity to enter and compete in markets and to prevent some market participants from taking advantage of their size or market position to unduly affect their competitors. These measures may be referred to as anti-trust legislation.

Competition law may also include rules to ensure fair competition in business practices at a microeconomic or transactional level by banning activities such as price discrimination, predatory pricing and misrepresentation.

There is no global multilateral agreement on trade and competition policy. Some regional bodies, such as the European Union, have such rules. However, a State may have an obligation under WTO agreements or other international treaties related to competition laws (mentioned in the checklist) to review its laws when establishing a single window or other paperless trade system.

Competition law may affect single window operators or other paperless trade services providers through their general application or through specific provisions that address such services. Their impact may be to control their participation in the domestic markets, to prevent abuse of their size or strategic position in serving these markets, or to ensure their survival in the face of foreign competition.

Alternatively, a country may choose to exempt providers of paperless trade services, including single window operators, from competition law. This may be done in light of the nature of the services offered and the public interest and may be associated with a licensing mechanism for eligible providers. Such an exemption would normally apply only to the rules about market entry, and not to transactional rules.

**IV.E.2 Does the law give authorized economic operators preferential access to the paperless trade system?**

Certain commercial operators may obtain "advanced economic operator" or "authorized economic operator" (AEO) status, which gives certain rights to expedited service or filing with government agencies, or even access

to the single window itself. AEO are selected on the basis of the frequency and volume of their interaction with customs and are considered reliable customs partners.

Since all users should be able to access the paperless trade system on an equal basis, AEOs' preferential access to paperless trade services may require an exemption from the application of competition law.

### IV.E.3 Are paperless trade service providers selected on a competitive basis? Are foreign providers admitted?

The end goal of paperless trade facilitation may be the establishment of a single national trade platform for all trade-related exchanges involving both public and private operators. However, historically the evolution of paperless trade systems has been based on the development of pilot projects and their aggregation in one or a limited number of larger systems, such as single windows. The operators of those systems may be chosen by competitive bid or may be subject to licensing. The selection process and its criteria may have implications for competition law. For instance, considerations relating to the security of sensitive data and of its transmission may also be relevant to justify the choice of a certain operator or of its features (for example, by limiting the selection to national service providers).