2 Enabling a conducive legal framework

2.1 Legal recognition of electronic transactions and documents

Recognizing legally that electronic transactions and documents can be functionally equivalent to paper versions is essential to replace paper-based with paperless trade systems. Treating electronic transactions and documents as equivalent to their paper versions can facilitate the cross-border legal recognition of transactions and documents (see Table 5).

Key criteria to consider when establishing this equivalence include, *inter alia*, to provide that a document would remain unaltered over time and to establish the identity of the originator of an electronic message.[1] The advantage of this functional equivalence approach is that it obviates the need for a legal system to alter its traditional rules about paper-based documents. It also avoids a "dual regime" approach by creating a special legal regime for electronic communications.

Ideally, once electronic transactions are enabled based on the functional equivalence approach, special rules should not be necessary for trade documents or transactions. This will provide a clear and common legal regime for paperless trade and thus facilitate data exchange.

However, states may pass laws to stipulate how electronic communications are to be applied to different transactions or documents (e.g. electronic contracts, electronically transferable records). Moreover, special requirements may also arise for electronic transactions and documents, for example when public entities such as customs authorities and regulatory agencies are involved.

For commercial documents that are transferable, such as those incorporating the entitlement to a goods delivery (e.g. bills of lading, warehouse receipts) or the payment of money (e.g. checks, promissory notes), additional functional equivalence requirements may be needed for their use in electronic form.

Ideally, all legal regimes should be based on the principle of technology neutrality (i.e. they do not specify the technology needed to achieve legal results). Such neutrality helps paperless trade systems to communicate with each other – since they operate on principles not on technological prescriptions – and thereby facilitate the exchange of electronic documents and information without the need for additional intervention.

Table 5: Trade documents that can be digitized

Type of document	Examples
Trade administration documents	
Product-related documents	Proof of origin documentation Universal certificate of origin Health certificate for live animal products Export/import sanitary and phytosanitary certificate CITES certificate for endangered species Certificate of inspection for organic products Dangerous goods documentation
Movement of products (export, import, transit)	Import/export declaration Export/import licence for controlled/dual-use goods, for agricultural products and any other products subject to a licence regime Safety and security declaration ATA Carnet (transit) TIR (transit) Union Transit Common Transit
Duties and excise documents	Binding tariff information Advance tariff ruling Excise guarantee Administrative documents used in the Excise Movement Control System
Commercial documents	
Finance and payment	Letters of credit Commercial invoices Order forms Insurance policy documents Payment confirmations
Transport and logistics	Weight/packing list Export cargo shipping instruction Standard shipping note CIM consignment note Road consignment (CMR) note Sea cargo manifest Air cargo manifest Airway bills Seaway bills
Documents of title (including the right to delivery of goods or payments of sums of money) which are usually used in finance, payment, transport and logistics	Bills of lading Bills of exchange Promissory notes Ship's delivery order Marine insurance policy Cargo insurance certificate Warehouse receipts

International guidance and good practices

Certain international instruments provide national lawmakers with guidance about cross-border alignment of the legal recognition of trade electronic transactions and documents to give legal validity and effect to electronic trade documents and transactions in different jurisdictions.

Some mechanisms are treaty-based and therefore may be directly legally binding. In other words, the legal status of electronic trade documents and transactions with respect to the states parties to the treaty is established in the treaty itself. Some of these treaties specify the criteria upon which this legal recognition depends. Treaties that do not, often delegate the definition of these criteria to technical bodies that operate under the umbrella of the framework agreement.

Obligation to accept the electronic form of certain documents

Some treaties contain obligations for states to accept certain documents in electronic form. Where it is not possible to reach agreement on establishing such an obligation, the treaty may contain a "best endeavour" clause, requiring states to make efforts towards that goal (e.g. to establish a single window in electronic form).

Treaties dealing with customs formalities

The TFA[2] requires WTO members to provide for advance lodging of documents in electronic format for pre-arrival processing. It also encourages members to accept paper or electronic copies of supporting documents required for import, export or transit formalities.

The International Convention on the Simplification and Harmonization of Customs Procedures (as amended) (Revised Kyoto Convention)[3] requires contracting parties to permit the lodging by electronic means of goods declarations and supporting documents. It also requires new or revised national legislation to provide for electronic commerce methods as an alternative to paper-based documentary requirements.

The International Convention on the Harmonization of Frontier Controls of Goods[4] encourages contracting parties to reduce reliance on paper documents and to simplify documentation procedures by using electronic systems for the exchange of information contained in railway consignment notes and customs declarations accompanying the goods.

Treaties dealing with transport of goods

The amendments to the Annex to the Convention on Facilitation of International Maritime Traffic, 1965[5] provide that shipping documents produced by electronic and other automatic data processing techniques, in legible and understandable form, shall be accepted.

The Customs Convention on the International Transport of Goods under Cover of TIR Carnets[6] ensures the secure exchange of data on the international transit of goods, vehicles or containers. It counts more than 30,000 authorized operators and is accepted at more than 3,500 customs offices worldwide. The legal framework for the full digitalization of the TIR system (the eTIR) entered into force on 21 May 2021.

The ATA Convention and the Istanbul Convention[7], which provide for the free movement of goods across frontiers and their temporary admission into a customs territory with relief from duties and taxes (ATA System), stipulate that all formalities necessary for implementing the ATA System may be carried out electronically by using data-processing techniques approved by the contracting parties. An eATA carnet project was launched in 2016 by the International Chamber of Commerce (ICC) with the support of the WCO.[8]

Obligation to give legal recognition to the use of electronic communications

Other treaties contain rules on the obligations of the parties to a contract, and, in doing so, give legal recognition to the use of electronic communications in international trade.

Treaties dealing with commercial contracts

The United Nations Convention on the Use of Electronic Communications in International Contracts[9] provides a uniform regime aimed at ensuring that commercial contracts and communications exchanged electronically are as valid and enforceable as their traditional paper-based equivalents. It sets out criteria for establishing the functional equivalence between electronic communications and paper documents, as well as between electronic authentication methods and handwritten signatures among business parties. The Convention requires that the legal validity or enforceability of an electronic contract is not to be denied on the sole ground that it is in the form of an electronic communication. However, it requires neither the use nor acceptance of electronic communications.

The United Nations Convention on Contracts for the International Sale of Goods[10] provides rules for contracts for international sales. Based on the principle of freedom of form, its language is media neutral and its rules can apply to both electronic communications and more traditional media.

Treaties dealing with the transport of goods

The United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (Rotterdam Rules)[11], which is not yet in force, aims to modernize the legal regime governing the international carriage of goods by sea and establishes rules for shippers, carriers and consignees on maritime (and possibly multimodal) shipping. It includes several provisions on the use of electronic transport records and documents (namely on the authenticity of negotiable electronic transport records) and revises the responsibilities and applicable limits of liability for carriers in cases of loss or damage to goods as a result of negligence.

The United Nations Convention on the Carriage of Goods by Sea (Hamburg Rules)[12] establishes a legal regime governing the rights and obligations of shippers, carriers and consignees under a contract of carriage of goods by sea. It allows the signature on the bill of lading in different formats (i.e. handwritten, printed in facsimile, perforated, stamped, in symbols, or by any other mechanical or electronic means).

The Convention on the Contract for the International Carriage of Goods by Road (CMR)[13] and the Additional Protocol concerning the electronic consignment note (eCMR)[14] standardize the conditions governing the contract for the international carriage of goods by road, particularly with respect to the documents used for such international carriage and to the carrier's liability. The additional protocol provides conditions under which electronic consignment notes are considered equivalent to paper-based versions and therefore have the same evidentiary value and produce the same effects.

Uniform models to harmonize the law

Yet another technique relies on the adoption at the national level of uniform models to harmonize the law across jurisdictions. The uniform model laws can be either sector-specific or general. Their adoption may be called for in bilateral or regional agreements and, again, may be in terms of mandatory obligation or best endeavours.

Model laws on the use of electronic transactions

The UNCITRAL Model Law on Electronic Commerce[15] provides national legislators with a set of internationally acceptable rules for the formation and validity of contracts concluded by electronic means. It also provides for the attribution of data messages, for the acknowledgement of receipt and for determining the time and place of dispatch and receipt of data messages, with a view to removing legal obstacles and increasing legal predictability for electronic commerce. It applies to both commercial and non-commercial electronic transactions.

The UNCITRAL Model Law on Electronic Transferable Records[16] aims at facilitating the use of electronic transferable records by providing a common definition of electronic transferable records that can be deemed as valid and enforceable as their paper-based equivalents:

> "Transferable documents or instruments are paper-based documents or instruments that entitle the holder to claim the performance of the obligation indicated therein and that allow the transfer of the

claim to that performance by transferring possession of the document or instrument. Transferable documents or instruments typically include bills of lading, bills of exchange, promissory notes and warehouse receipts."

Guidelines for the transport of goods

The International Maritime Organization Guidelines for the Use of Electronic Certificates[17] introduces common validity criteria to facilitate the use and acceptance of electronic certificates to show compliance with IMO requirements and to describe operating conditions, crewing requirements and ship equipment carriage requirements. Table 6 lists the relevant sections on electronic transactions and documents in the *ESCAP Legal Readiness Assessment Guide* and *Checklist*.

Table 6: Electronic transactions and documents – relevant sections in the *ESCAP Legal Readiness Assessment Guide* and *Checklist*

Questions in the *Guide* and *Checklist*	Section
What is the legal status of electronic transactions?	I.A.1
If an electronic transactions law exists, is it based on uniform models?	I.A.2
What are the conditions, if any, for the legal recognition of electronic transactions?	I.A.3
Does the law establish functional equivalence between paper documents and electronic communications?	I.A.4
What is the legal status of electronic contracts?	I.A.5
Are there special rules for the use of electronic communications in paperless trade?	I.A.6
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?	I.A.7
Are there special rules for the use of electronic transferable records such as bills of lading?	I.A.8

2.2 Trust services

Trust services are electronic services that provide assurance of the quality of data (i.e. their trustworthiness). This assurance is often required in order to provide electronic documents and transactions with legal effects, as a notary's stamp can be necessary to support the legal validity of some types of document.

According to UNCITRAL texts, the requirements for an electronic signature to be functionally equivalent to a handwritten one are to identify[18] a signatory in relation to a data message and to indicate the signatory's intent with respect to the information contained in the data message. Trust service providers may be able to certify these elements of an electronic signature and thus support its validity.

Electronic signatures may themselves be thought of as one type of trust service as they are considered, for instance, under the EU eIDAS Regulation on electronic identification and trust services for electronic transactions[19]. They may serve to guarantee the origin and integrity of data messages, which may include trade documents exchanged by businesses.

It may be noted that proof of origin is perhaps the first and most important function of a signature of any kind. Many of the rules about the validity of electronic signatures affect this function. In this way, they can improve the security of the signed documents against error and malicious attacks. Different technologies can be used to provide trust services, and therefore their level of reliability might differ.

Some types of electronic signature (i.e. digital signature, electronic digital signature) may provide greater assurance of its origins and confirm the integrity of the signed document. These electronic signatures are predicated on a public key infrastructure or on a set of requirements needed to authenticate the signature.

A digital signature based on public key infrastructure relies on the use of a private and a public key, and usually involves a certification authority. Third-party certification service providers (e.g. qualified electronic signature providers) may need to comply with further requirements to associate their services with additional legal effects. Organizations and regions (i.e. the European Union) rely on particular certificate authority to ensure authenticity and prevent forgery. Digital signatures have been legally binding and enforceable through legislation such as the EU Directive on a community framework for electronic signatures[20] and, more recently, the eIDAS Regulation.

The increased use of electronic trust services as substitutes for paper-based processes may result in uncertainty as to their legal effect in the absence of an adequate legal framework. 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 transaction or document.

Specific legal regimes can be established for a particular sector (e.g. banks) or among particular participants (e.g. public agencies). On a voluntary basis, through co-regulation or parties' agreement, the use of a specific technology may be agreed upon for certain trust services, spelling out how these trust services should be provided and supported (certified) in order to be legally valid.

International guidance and good practices

Paperless trade systems need to rely on mechanisms guaranteeing an international alignment on what constitutes a valid trust service across borders. Various mechanisms exist. Some are treaty-based and therefore may be directly legally binding. Others favour the harmonization of legal systems through the adoption of model laws, while others are based on bilateral or regional agreements.

Moreover, trade agreements may contain provisions requiring states to give legal recognition to electronic signatures in a manner that is technology neutral and favours interoperability (see Box 2).

Conventions and treaties

Conventions and treaties provide substantive law to guarantee legal harmonization in states parties. The provisions they contain are either best endeavours or mandatory requirements. Legal recognition of foreign signatures may be provided by treaty (e.g. United Nations Convention on the Use of Electronic Communications in International Contracts for electronic signatures used in commercial exchanges).

"Paperless trade systems need to rely on mechanisms guaranteeing an international alignment on what constitutes a valid trust service across borders."

Box 2: Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)

The parties to the CPTPP include Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Viet Nam.

In Article 14.6, on electronic authentication and electronic signatures, the CPTPP recognizes electronic signatures in a manner that is technology neutral and favours interoperability:

"1. Except in circumstances otherwise provided for under its law, a Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.

2. No Party shall adopt or maintain measures for electronic authentication that would:

(a) prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction; or

(b) prevent parties to an electronic transaction from having the opportunity to establish before judicial or administrative authorities that their transaction complies with any legal requirements with respect to authentication.

3. Notwithstanding paragraph 2, a Party may require that, for a particular category of transactions, the method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its law.

4. The Parties shall encourage the use of interoperable electronic authentication."

Regional and international mutual recognition schemes

Mutual recognition schemes provide an international or regional accreditation system based on agreed legal principles with regard to the conditions for the recognition of foreign electronic communications and related matters such as electronic signatures. They usually rely upon special entities with the responsibility to issue the certification or accreditation to business entities. For example, the EU eIDAS Regulation provides legal recognition of foreign signatures within the European Union.

Model laws and guidelines

Model laws and guidelines provide lawmakers with uniform laws that support legal harmonization when drafting new laws or amending existing ones. They can be sector-specific or general.

Laws can apply the same standards to validate the use of domestic and foreign electronic signatures. When based on the UNCITRAL Model Law on Electronic Signatures, laws provide for a test of substantial equivalence between the signatures offered in different jurisdictions. UNCITRAL is also working towards the development of a model law on identity management and trust services, which could guide national legislation.

Contractual frameworks

Commercial operators may conclude cross-recognition or cross-certification agreements for the mutual recognition of the legal effects of the electronic communications exchanged and any related service provided. Such agreements may contain a choice of applicable law. However, they also need to respect any mandatory rule of the jurisdictions where they are intended to take effect. The Pan Asian E-Commerce Alliance Mutual Recognition Framework is an example of such a scheme.

Table 7 lists the relevant sections on trust services in the *ESCAP Legal Readiness Assessment Guide* and *Checklist*.

Table 7: Trust services – relevant sections in the *ESCAP Legal Readiness Assessment Guide* and *Checklist*

Questions in the *Guide* and *Checklist*	Section
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?	I.B.1
Does the law adopt a functional equivalence approach for electronic signatures?	I.B.2
Is the law based on international standards?	I.B.3
Does the law recognize foreign electronic signatures?	I.B.4
Are there special rules for the use of electronic signatures in paperless trade?	I.B.5
Does the law deal with trust services?	I.B.6
Does the law establish general requirements for data retention, including a minimum and maximum retention period? Do they apply to electronically stored data?	I.E.1
Does the law require or favour the use of specific trust services or service providers for data retention?	I.E.2
Is electronic evidence admissible in judicial and other proceedings?	I.E.4
Is electronic evidence that is generated, stored or collected abroad admissible? If so, under which conditions?	I.E.5

2.3 Data governance

When documents and information are exchanged between users using electronic systems or between electronic systems, the system must ensure confidentiality (i.e. information is private to only designated parties to the communications) and data integrity (i.e. the accuracy and consistency of data are maintained and assured over their entire life cycle).

Information submitted to complete border formalities can be confidential and personal. To ensure that traders submit data only once, government entities should be able to share collected or submitted information among themselves. 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.

It is expected that the information and communications technology (ICT) system will be robust enough to safeguard it from being compromised. As the volume of data managed in paperless trade systems increases exponentially, these systems become a more tempting target for hackers. The willingness of users to replace paper-based documents with electronic information depends on their confidence in the security, confidentiality and privacy of personal and business information.

The need for data privacy and confidentiality may inspire conditions on data transfer between parties, and thereby influence the functioning of paperless trade systems. Cross-border exchange of trade-related data should be smooth but not compromise data confidentiality, privacy and security.

Moreover, at the national level, cybersecurity (the protection of the integrity of data against intentional or negligent compromise) requires coordinated action for prevention, preparation, response and incident recovery on the part of government authorities, the private sector and civil society. Protecting computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide, is essential to ensure the adoption of paperless trade systems.

There are international instruments that facilitate cybersecurity cooperation, given that cyberthreats are generally borderless. These cooperation schemes, among other things, enable cross-border information exchange for regulatory oversight or law enforcement purposes.

Technical measures to ensure security and availability of computer systems and networks are discussed in Section 3.6 of the Toolkit. Similarly, data governance involves issues relating to liability, which is discussed in Section 2.4.

International guidance and good practices

General data laws governing collection, access to, use and sharing of data might already apply to operators managing paperless trade systems. For instance, section I.C.7 of the *Legal Readiness Assessment Guide* states that 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, which covers, among others, entities managing paperless trade systems (see Articles 30-33 of the Electronic Trade Facilitation Act 2015 of the Republic of Korea).

The Customs Act (1960) and the Electronic Transactions Act (2010) of Singapore, respectively, prohibit information collected for a specified and lawful purpose from being shared for another purpose without prior consent of the supplier of the information, and specify the conditions under which information collected in the performance of duty can be used and disclosed.[21] The application of criminal laws to incorrect or false declarations to customs in an electronic environment is discussed in Section 2.4.

International instruments can provide national lawmakers with guidance, which may take the form of treaties or model laws, to help foster international alignment on data governance. Examples of these types of instrument are given in Table 8. Trade agreements may also contain dedicated provisions on cross-border information transfer (see Box 3).

Box 3: Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)

In Article 14.11, on cross-border transfer of information by electronic means, the CPTPP states:

"1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.

2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.

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 transfers of information greater than are required to achieve the objective.

Table 8: Example international instruments providing data governance guidance

Data governance area	Example instruments
Privacy	OECD 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (revised in 2013) EU General Data Protection Regulation APEC Privacy Framework Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) of the Council of Europe ASEAN Framework on Personal Data Protection African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS Standards for Personal Data Protection for Ibero-American States Madrid Resolution: International Standards on the Protection of Personal Data and Privacy adopted by the International Conference of Data Protection and Privacy Commissioners Technical standards on privacy protection in ISO/IEC 27701:2019, *Security Techniques: Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management — Requirements and Guidelines*
Cybersecurity	Budapest Convention on Cybercrime of the Council of Europe Directive C/DIR/1/08/11 on Fighting Cyber Crime within ECOWAS African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) ESCWA *Cyber Legislation Directives* OECD recommendations in *Digital Security Risk Management for Economic and Social Prosperity* OECD *Recommendation of the Council on Digital Security of Critical Activities*
Intellectual property rights	Paris Convention for the Protection of Industrial Property WTO Agreement on Trade-Related Aspects of Intellectual Property Rights
Government access to data	Currently under discussion at the OECD Committee on Digital Economy Policy*

* See https://www.oecd.org/sti/ieconomy/trusted-government-access-personal-data-private-sector.htm.

Note: APEC — Asia-Pacific Economic Cooperation; ASEAN — Association of Southeast Asian Nations; ECOWAS — Economic Community of West African States; ESCWA — Economic and Social Commission for West Asia; IEC — International Electrotechnical Commission; ISO — International Organization for Standardization; OECD — Organisation for Economic Co-operation and Development.

With respect to personal information protection, exporting data might be allowed on the condition that the destination jurisdiction provides data protection equal to that in the exporting state. Various international instruments aim at facilitating cross-border data flow by ensuring equal data privacy and protection between two or more territories:

- contractual safeguards defined by companies without approval or review from a public authority (e.g. consent, transmission of privacy notice);
- internal rules defined by a group or company and submitted for approval to a public authority (e.g. binding corporate rules);
- certification schemes and codes of conduct that are submitted for approval to a public authority or third-party agent;
- a public entity's decision recognizing the equivalent level of data protection in a given foreign territory (i.e. public adequacy decisions[22]);
- pre-defined safeguards defined by a public authority (e.g. standard contractual clauses);
- certification schemes and codes of conduct approved by public authority (e.g. Cross-Border Privacy Rules certification system[23]).

Digital economy agreements are a more recent and broader cooperation model than traditional free trade agreements, with a strong focus on digital communications. For example, a memorandum of understanding with regard to the Singapore–Australia Digital Economy Agreement provides additional detailed guidance on cooperation in personal data protection.[24]

"When documents and information are exchanged between users using electronic systems or between electronic systems, the system must ensure confidentiality and data integrity."

Lastly, international cybersecurity cooperation schemes can help to exchange information with a view to mitigating cyberthreats across borders:

- Title III of the Budapest Convention on Cybercrime of the Council of Europe.
- Some bilateral and regional trade agreements, such as the Digital Economy Partnership Agreement and the Regional Comprehensive Economic Partnership,[25] encourage capacity building of national entities responsible for computer security incident response and workforce development through mutual recognition of qualifications, as well as the cross-border exchange of information to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks globally.
- Mutual legal assistance treaties enable authorities to request access to data for law enforcement purposes. However, securing evidence through such processes takes time.

Table 9 lists some of the relevant sections on data governance in the *Legal Readiness Assessment Guide* and *Checklist*.

Table 9: Data governance – relevant sections in the *ESCAP Legal Readiness Assessment Guide* and *Checklist*

Questions in the *Guide* and *Checklist*	Section
Is there a law on privacy and data protection? If so, what are its features? Is it based on international standards?	I.C.1
Are there any special rules on privacy and data protection for paperless trade?	I.C.5
Does the law protect the confidentiality of commercial information in electronic form?	I.C.6
Are there provisions on cybercrimes that are applicable to paperless trade?	I.C.7
Are there agreements or policies for collecting, accessing, using and sharing data among government agencies participating in a paperless trade system?	I.D.1
What defines rights regarding information exchanged in the paperless trade system, the law or contractual agreements?	IV.A.1

2.4 Liability and dispute settlement

Trading parties and other concerned entities may suffer losses from the incorrect transmission or improper reuse of information and may seek compensation for those losses. Guaranteeing access to civil remedies for such losses and dispute settlement opportunities can help to enhance trust in paperless trade systems, and thereby support their adoption.

Most legal systems require people (legal entities) whose fault (i.e. failure to live up to accepted standards of conduct) causes harm to others to repair the harm or to make up their losses. This principle should normally apply to the participants in cross-border paperless trade, in the same way as to offline traders.

However, a number of issues relevant to paperless trade are of an administrative nature (i.e. they affect matters of public policy and not only of the allocation of private rights and remedies). Often public entities such as customs authorities are involved.

As a consequence, the law may limit or exclude liability of some actors, usually in order to encourage their activity or to lower obstacles to market entry. Different liability rules may therefore be applicable to the principal participants in a paperless trading system:

- The operators of the system itself (e.g. a single window) should provide accurate and timely information exchange. If the performance standards for information exchange are not met, the system operator may be held liable (subject, as noted, to limitation or exemption because of their public status).

- Other governmental entities provide and process trade-related data for several purposes (e.g. goods control and taxes), where accuracy and speed of interaction will affect the efficiency of the system and ultimately of trading operations. Liability rules for not providing or processing trade-related data correctly may be spelled out in legislation or in contracts. The general law may provide for the liability of government agencies or for their exemption from liability when performing public functions.

- Communications intermediaries such as internet service providers provide transmission or trust services, but they do not originate the information. Their failure can cause harm to trading parties.

- Providers of trust services (e.g. certification authorities) support electronic signatures, timestamping, the integrity of documents, registered delivery and other services guaranteeing the quality of data and electronic messages. Their liability is usually defined in contractual agreements, but a law may establish mandatory liability terms. If they are public agencies, a different liability regime may apply.

- Other participants in the system (e.g. customs brokers) may commit acts or omissions during customs clearance or other trade-related operations that might result in damages. Participants who intentionally submit incorrect or false information may face criminal, administrative and civil sanctions both in the paper-based and in the paperless environment. That said, a law may limit or exclude liability of selected service intermediaries where lawmakers want to encourage their activity.

"Cross-border paperless trade may be subject to special dispute resolution mechanisms that consider the public nature of the parties and interests involved."

Most if not all jurisdictions have legal rules to decide who hears a dispute (choice of forum) and under which legal regime (choice of law). These rules often support the autonomy of parties involved in a transaction (i.e. they may agree themselves on the choice of law and of forum in their international contracts). Sometimes the law specifies criteria for such choices or restricts them to local forums or laws where the national interests are considered to require local treatment, especially when a public entity is involved.

The law may also encourage or require parties to attempt to resolve their disputes through alternative dispute resolution mechanisms such as mediation or arbitration. These processes are increasingly being conducted online, notably by videoconference.

Cross-border paperless trade may be subject to special dispute resolution mechanisms that consider the public nature of the parties and interests involved. Automated online dispute resolution is developing for simple and routine disputes, but so far not for non-standard disputes over matters of high value.

International guidance and good practices

Treaties, model laws and model contractual provisions can help to provide dispute resolution mechanisms in a cross-border context. These instruments are generally designed for civil or commercial matters because of state privileges and immunities and will normally apply to B2B transactions – but not usually to B2G or G2G transactions.

The Hague Conference on Private International Law has adopted a number of texts on the choice of forum and the recognition and enforcement of foreign judgments. For instance, the Convention on Choice of Court Agreements[26] gives conditional effect to party autonomy in choosing the forum for international litigation. If parties do not decide otherwise, the convention provides criteria to establish the competent court.

The Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters[27] also facilitates the effective international application of judgments – and thus the trade creating the adjudicated rights – by setting forth commonly accepted conditions for recognition and enforcement and agreed grounds for refusal.

With respect to international commercial arbitration, the UNCITRAL Model Law on International Commercial Arbitration[28] assists states in reforming their law on arbitral procedures and reflects worldwide consensus on key aspects of international arbitration practice in view of fostering legal harmonization.

The UNCITRAL Arbitration Rules[29] provide paperless trade operators and users with procedural rules for the conduct of arbitral proceedings arising out of their commercial relationship.

A state may also be a party to the Convention on the Recognition and Enforcement of Foreign Arbitral Awards[30] to enforce the results of the arbitration across borders. Commonly known as the New York Convention, it is the worldwide standard on such matters and has reached near-universal acceptance.

Table 10 lists the relevant sections on liability and dispute settlement in the *ESCAP Legal Readiness Assessment Guide* and *Checklist*.

Table 10: Liability and dispute settlement – relevant sections in the *ESCAP Legal Readiness Assessment Guide* and *Checklist*

Questions in the *Guide* and *Checklist*	Section
Do data custodians, such as data centres, assume liability for loss or damage to electronically stored information? Is such liability contractual, statutory or both?	I.E.3
May the operator of the paperless trade system be held liable for providing its services?	IV.B.1
May government agencies participating in the paperless trade system be held liable for their interaction with the system?	IV.B.2
May service providers, such as internet service providers and trust services providers, be held liable for interacting with the paperless trade system?	IV.B.3
May other participants in the paperless trade system (e.g. 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?	IV.B.4
Do national laws deal with choice-of-forum and choice-of-law issues relevant to paperless trade facilitation?	IV.C.1
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?	IV.C.2
Are online dispute resolution mechanisms used in paperless trade facilitation?	IV.C.3

Endnotes

1 UNCITRAL Model Law on Electronic Commerce.

2 See https://www.wto.org/english/tratop_e/tradfa_e/tradfa_e.htm.

3 See http://www.wcoomd.org/zh-cn/topics/facilitation/instrument-and-tools/conventions/pf_revised_kyoto_conv.aspx.

4 See https://unece.org/transport/documents/2021/03/working-documents/international-convention-harmonization-frontier.

5 See https://www.imo.org/en/OurWork/Facilitation/Pages/FALConvention-Default.aspx.

6 See https://unece.org/transport/tir.

7 See http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/conventions/pf_ata_system_conven.aspx.

8 See https://iccwbo.org/resources-for-business/ata-carnet/e-ata-carnet-project.

9 See https://uncitral.un.org/en/texts/ecommerce.

10 See https://uncitral.un.org/en/texts/salegoods/conventions/sale_of_goods/cisg.

11 See https://uncitral.un.org/en/texts/transportgoods.

12 *Ibid.*

13 See https://treaties.un.org/doc/Treaties/1961/07/19610702%2001-56%20AM/Ch_XI_B_11.pdf.

14 See https://treaties.un.org/doc/Treaties/2008/03/20080303%2006-53%20PM/CTC-xi-B-11b.pdf.

15 See https://uncitral.un.org/en/texts/ecommerce.

16 See https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records.

17 See https://wwwcdn.imo.org/localresources/en/OurWork/IIIS/Documents/FAL.5-Circ.39-Rev.2%20-%20Guidelines%20For%20The%20Use%20Of%20Electronic%20Certificates.pdf.

18 This identification function can also be complemented by digital identity systems (see Section 3.1).

19 See *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*, 28 August 2014.

20 See *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures,*19 January 2000.

21 For case studies of national cybersecurity policies in Thailand and the United States, see https://thainetizen.org/wp-content/uploads/2019/11/thailand-cybersecrutiy-act-2019-en.pdf and https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. For an example of national laws aiming at ensuring privacy and confidentiality in electronic communications, see https://www.cr-online.de/17-06-29_vzbv-amendments_eprivacy-regulation.pdf.

22 Examples of adequacy decisions include the European Union with Andorra, Argentina, Canada (commercial organizations), the Faroe Islands, Guernsey, the Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay (see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).

23 See https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system.

24 See https://www.mti.gov.sg/-/media/MTI/Microsites/DEAs/Singapore-Australia-Digital-Economy-Agreement/MOUs/MOU-on-Cooperation-in-Personal-Data-Protection.pdf.

25 Singapore has entered multiple free trade agreements and economic partnership agreements over e-commerce and cybersecurity to build up their cyber capabilities in responding to computer security incidents. These agreements also encourage bilateral or multilateral cooperation in identifying and mitigating malicious intrusions or dissemination of malicious code that may affect the networks of involved parties.

26 See https://www.hcch.net/en/instruments/conventions/full-text/?cid=98.

27 See https://www.hcch.net/en/instruments/conventions/full-text/?cid=137.

28 See https://uncitral.un.org/en/texts/arbitration/modellaw/commercial_arbitration.

29 See https://uncitral.un.org/en/texts/arbitration/contractualtexts/arbitration.

30 See https://www.newyorkconvention.org.