

CHAPTER 12

ELECTRONIC COMMERCE

ARTICLE 12.1

Definitions

For purposes of this Chapter:

- (a) "electronic authentication" means the process or act of verifying the identity of a party to an electronic communication or transaction or¹ ensuring the integrity of an electronic communication;
- (b) "personal information" means any information, including data, about an identified or identifiable natural person;
- (c) "commercial electronic message" means an electronic message which is sent for commercial purposes to an electronic address of a person² through telecommunication services, comprising at least electronic mail and to the extent provided for under domestic laws and regulations, other types of messages; and
- (d) "unsolicited commercial electronic message" means a commercial electronic message that is sent without the consent of the recipient or despite the explicit rejection of the recipient.

ARTICLE 12.2

Scope and general principles

¹ It is understood that 'or' includes 'and' and thus encompasses situations where both or either functions are performed.

² For greater certainty, the "electronic address of a person" does not cover IP addresses.

1. This Chapter applies to measures adopted or maintained by a State Party with respect to trade by electronic means.
2. Considering the potential that electronic commerce has as an instrument for social and economic development, the State Parties recognise the importance of:
 - (a) clarity, transparency and predictability of their national policy frameworks to facilitate, to the extent possible, the development of electronic commerce;
 - (b) interoperability, innovation and competition to facilitate electronic commerce; and
 - (c) international and national policies concerning electronic commerce taking into account the interests of all users, including enterprises, consumers, non-governmental organisations and relevant public institutions.
3. For greater certainty, measures adopted or maintained by a State Party with respect to trade by electronic means are subject to the relevant provisions of other Chapters and Annexes of this Agreement, including exceptions, reservations, specific commitments or non-conforming measures that are applicable to those obligations.
4. This Chapter shall not apply to:
 - (a) government procurement;
 - (b) information held or processed by, or on behalf of, a State Party or measures related to that information; or
 - (c) subsidies or grants provided by a State Party or a state enterprise, including government-supported loans, guarantees, and insurance.
5. In the event of an inconsistency between this Chapter and another Chapter, the other Chapter prevails to the extent of the inconsistency.

ARTICLE 12.3

Domestic electronic transactions framework

1. Each State Party shall not deny the legal validity of a transaction, including a contract, solely on the basis that the transaction is in electronic form, except in circumstances provided for under its laws and regulations.
2. For greater certainty, paragraph 1 does not prevent a State Party from requiring that certain categories of contracts be concluded by non-electronic means.
3. Each State Party shall endeavour to:
 - (a) avoid any undue regulatory burden on electronic transactions;
 - (b) facilitate input by interested persons, where appropriate, in the development of its legal framework for electronic transactions; and
 - (c) foster transparency regarding the legal framework for electronic transactions.

ARTICLE 12.4

Electronic authentication

1. Except in circumstances provided for under its laws and regulations, a State Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.
2. A State Party shall not 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 State 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 laws and regulations.
- 4. The State Parties shall encourage the use of interoperable electronic authentication and work towards the mutual recognition of electronic authentication.

ARTICLE 12.5

Online consumer protection

- 1. The State Parties recognise the importance of transparent and effective measures that enhance consumer confidence and trust in electronic commerce. Each State Party shall adopt or maintain measures to proscribe misleading, fraudulent and deceptive commercial activities that cause harm, or potential harm, to consumers engaged³ in electronic commerce.
- 2. Misleading, fraudulent and deceptive commercial activities include:
 - (a) making material misrepresentations⁴, including implied factual misrepresentations, or false claims as to matters such as qualities, price, suitability for purpose, quantity or origin of goods or services;
 - (b) advertising goods or services for supply without intention or reasonable capability to supply;

³ For the purposes of this Article, the term 'engaged' includes the pre-transaction phase of electronic commerce.

⁴ For the purposes of this Article, material misrepresentations refer to misrepresentations that are likely to affect a consumer's conduct or decision to use or purchase a good or service.

- (c) failing to deliver goods or provide services to a consumer after the consumer is charged unless justified on reasonable grounds; or
 - (d) charging a consumer for services or goods not requested.
3. To protect consumers engaged in electronic commerce, each State Party shall endeavour to adopt or maintain measures that aim to ensure:
- (a) that suppliers of goods and services deal fairly and honestly with consumers;
 - (b) that suppliers provide complete, accurate, and transparent information on goods and services including any terms and conditions of purchase; and
 - (c) the safety of goods and, where applicable, services during normal or reasonably foreseeable use.
4. The State Parties recognise the importance of affording to consumers who are engaged in electronic commerce consumer protection at a level not less than that afforded to consumers who are engaged in other forms of commerce.
5. The State Parties recognise the importance of cooperation between their respective consumer protection agencies or other relevant bodies including the exchange of information and experience, as well as cooperation in appropriate cases of mutual concern regarding the violation of consumer rights in relation to electronic commerce in order to enhance online consumer protection, where mutually agreed.
6. The State Parties shall endeavour to promote access to, and awareness of, consumer redress or recourse mechanisms, including for consumers transacting cross-border.

ARTICLE 12.6

Unsolicited commercial electronic communication

1. State Parties recognise the importance of promoting confidence and trust in electronic commerce, including through transparent and effective measures that limit unsolicited commercial electronic messages.
2. Each State Party shall adopt or maintain measures that:
 - (a) require suppliers of commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages;
 - (b) require the consent, as specified in the laws or regulations of each State Party, of recipients to receive commercial electronic messages; or
 - (c) otherwise provide for the minimisation of unsolicited commercial electronic messages.
3. Each State Party shall endeavour to ensure that commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are sent, and contain the necessary information to enable recipients to request cessation free of charge and at any time.
4. Each State Party shall endeavour to provide access to either redress or recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained pursuant to paragraph 2.
5. The State Parties shall endeavour to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

ARTICLE 12.7

Paperless trading

1. Each State Party shall endeavour to make any form issued or controlled by its customs authority and other government agencies for export, import and transit available to the public in electronic format.

2. Each State Party shall endeavour to accept any form issued or controlled by its customs authority and other government agencies for export, import and transit submitted electronically as the legal equivalent of the paper version of those documents.
3. A State Party shall not be required to apply paragraphs 1 and 2 where:
 - (a) there is an international legal requirement to the contrary; or
 - (b) doing so would reduce the effectiveness of the trade administrative process.
4. Each State Party shall endeavour to develop data exchange systems to support the exchange of electronic records used in commercial cross-border trading activities of enterprises within each State Party's respective territory.

ARTICLE 12.8

Electronic invoicing

1. The State Parties recognise the importance of electronic invoicing to increase the efficiency, accuracy and reliability of commercial transactions.
2. The State Parties also recognise the benefits of interoperable electronic invoicing systems in the context of international trade and the importance of exchanging information on the adoption of best practices related to interoperable systems for electronic invoicing.

ARTICLE 12.9

Cooperation

Recognising the global nature of electronic commerce, the State Parties shall endeavour to:

- (a) work together to facilitate the use of electronic commerce by small and medium sized

enterprises;

- (b) share information and experiences on laws, regulations, and programs in the sphere of electronic commerce, including those related to the protection of personal information, consumer confidence and protection, security in electronic communication, e-government, the recognition of electronic signatures, including digital signatures, and facilitation of interoperable cross border electronic authentication;
- (c) work together to promote cross-border information flows to support a dynamic environment for electronic commerce;
- (d) encourage development by the private sector of methods of self-regulation that foster electronic commerce, including codes of conduct, model contracts, guidelines and enforcement mechanisms;
- (e) participate actively in regional and multilateral forums to promote the development of electronic commerce, including in relation to the development and application of international standards for electronic commerce; and
- (f) promote information and communications technologies accessibility for people with specific needs, including persons with disabilities, and under-represented groups, including indigenous peoples, people living in rural and remote areas, women and girls, and youth and children.

ARTICLE 12.10

Cooperation on cybersecurity matters

The State Parties recognise the importance of:

- (a) building the capabilities of their national entities responsible for cyber security, including computer security incident response; and
- (b) using existing collaboration mechanisms to cooperate on matters related to cyber security,

including to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the State Parties.