

## CHAPTER 13

### ELECTRONIC COMMERCE

#### Article 13.1: Definitions

For the purposes of this Chapter:

**computing facilities** means computer servers and storage devices for processing or storing information for commercial use;

**covered person** means:

- (i) a service supplier of the other Party within the meaning of Chapter 9 (Trade in Services);
- (ii) an investor of a Party as defined in Chapter 14 (Investment), excluding an investor in a financial institution; or
- (iii) a covered investment as defined in Chapter 1 (Initial Provisions and General Definitions),

but does not include a “financial institution” or a “financial service supplier” as defined in Chapter 10 (Financial Services), or a credit reporting body;

**electronic authentication** means the process of testing an electronic statement or claim in order to establish a level of confidence in the statement’s or claim’s reliability;

**electronic transmission** or **transmitted electronically** means a transmission made using any electromagnetic means, including by photonic means;<sup>1</sup>

**electronic version of a document** means a document in an electronic format prescribed by a Party, including a document sent by facsimile transmission;

**personal information** means any information, including data or opinions, about an identified or identifiable natural person;

**trade administration documents** means forms issued or controlled by a Party which must be completed by or for an importer or exporter in relation to the import or export of goods; and

---

<sup>1</sup> This definition is without prejudice to whether electronic transmissions should be characterised as goods or services.

**unsolicited commercial electronic message** means an electronic message which is sent for commercial or marketing purposes to an electronic address, without the consent of the recipient or despite the explicit rejection of the recipient, through an Internet access service supplier or, to the extent provided for under the laws and regulations of each Party, other telecommunications service.

### **Article 13.2: Scope and General Provisions**

1. The Parties recognise the economic growth and opportunities provided by electronic commerce and the importance of frameworks that promote consumer confidence in electronic commerce and of facilitating its use and development.
2. This Chapter shall apply to measures adopted or maintained by a Party that affect trade by electronic means.
3. This Chapter shall not apply to government procurement.
4. Article 13.11, Article 13.12, and Article 13.13 shall not apply to information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection.
5. For greater certainty, this Chapter may apply to a measure that is also subject to Chapter 9 (Trade in Services), Chapter 14 (Investment) or Chapter 10 (Financial Services).
6. To the extent that such a measure is adopted or maintained in accordance with Article 9.7 (Non-Conforming Measures) of Chapter 9 (Trade in Services) or Article 14.14 (Non-Conforming Measures) of Chapter 14 (Investment) or an exception in Chapter 9 (Trade in Services), Chapter 10 (Financial Services) or Chapter 14 (Investment), it shall not give rise to a violation of Article 13.11, Article 13.12 or Article 13.13.

### **Article 13.3: Cooperation**

1. Recognising the global nature of electronic commerce, each Party shall endeavour to:
  - (a) work together to assist micro, small and medium-sized enterprises<sup>2</sup> to overcome obstacles to its use;
  - (b) exchange information and share experiences on regulations, policies, enforcement and compliance regarding electronic commerce, for example:

---

<sup>2</sup> As defined by each Party.

- (i) personal information protection;
  - (ii) online consumer protection, including means for consumer redress and building consumer confidence;
  - (iii) unsolicited commercial electronic messages;
  - (iv) security in electronic communications;
  - (v) authentication; and
  - (vi) e-government service delivery;
- (c) exchange information and share views on consumer access to products and services offered online;
- (d) participate actively in regional and multilateral fora to promote the development of electronic commerce, including in relation to the development and application of international standards for electronic commerce; and
- (e) 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.
2. In relation to cyber security, each Party recognises the importance of:
- (a) building and maintaining the capabilities of their national entities responsible for computer security incident response, including through exchange of best practices; and
  - (b) using existing collaboration mechanisms to cooperate to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties.

#### **Article 13.4: Paperless Trading**

1. Each Party shall endeavour to make electronic versions of its trade administration documents publicly available.
2. Each Party shall accept electronic versions of its trade administration documents as the legal equivalent of paper documents except where:
- (a) there is a domestic or international legal requirement to the contrary; or

(b) doing so would reduce the effectiveness of the trade administration process.

3. The Parties shall cooperate bilaterally and in international fora to enhance the acceptance of electronic versions of trade administration documents.

### **Article 13.5: Electronic Authentication and Electronic Signatures**

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. Each Party shall adopt or maintain measures based on international norms for electronic authentication that:

(a) permit participants in electronic transactions to determine the appropriate authentication technologies and implementation models for their electronic transactions;

(b) do not limit the recognition of authentication technologies and implementation models; and

(c) permit participants in electronic transactions to have the opportunity to prove that their electronic transactions comply with the Party's laws and regulations.

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.

### **Article 13.6: Online Consumer Protection**

1. The Parties recognise the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent and deceptive commercial activities, when they engage in electronic commerce.

2. For the purposes of this Article, fraudulent and deceptive commercial activities refers to those fraudulent and deceptive commercial practices that cause actual harm to consumers, or that pose an imminent threat of such harm if not prevented, for example:

(a) a practice of making misrepresentations of material fact, including implied factual misrepresentations, that cause significant detriment to the economic

interests of misled consumers;

(b) a practice of failing to deliver products or provide services to consumers after the consumers are charged; or

(c) a practice of charging or debiting consumers' financial, telephone or other accounts without authorisation.

3. Each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.

4. The Parties recognise the importance of cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border electronic commerce in order to enhance consumer welfare and affirm that the cooperation under Article 16.5 of Chapter 16 (Competition) includes cooperation with respect to online commercial activities.

#### **Article 13.7: Protection of Personal Information**

1. The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce.

2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the 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.

3. Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction.

4. 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 arrangements to promote compatibility between them.

### **Article 13.8: Unsolicited Commercial Electronic Messages**

1. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that:
  - (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages;
  - (b) require the consent, as specified according to the laws and regulations of each Party, of recipients to receive commercial electronic messages; or
  - (c) otherwise provide for the minimisation of unsolicited commercial electronic messages.
2. Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained in accordance with paragraph 1.
3. The Parties shall endeavour to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

### **Article 13.9: Domestic Regulatory Frameworks**

1. Each Party shall maintain a legal framework governing electronic transactions consistent with the principles of the *UNCITRAL Model Law on Electronic Commerce 1996* or the *United Nations Convention on the Use of Electronic Communications in International Contracts*, done at New York, November 23, 2005.
2. Each Party shall endeavour to:
  - (a) avoid any unnecessary regulatory burden on electronic transactions; and
  - (b) facilitate input by interested persons in the development of its legal framework for electronic transactions.

### **Article 13.10: Transparency**

1. Each Party recognises that transparent regulations and policies are important for trade facilitation, creating a conducive environment for electronic commerce and promoting cross-border electronic commerce.
2. Each Party shall publish information on the rights of, and protections it provides for, users of electronic commerce, including information on:

- (a) how individuals can pursue remedies; and
  - (b) how businesses can comply with legal requirements.
- 3. Each Party shall encourage enterprises to publish, including on the internet, their policies and procedures related to protection of personal information.
- 4. Each Party shall publish the names and addresses of the competent authorities responsible for measures related to electronic commerce.
- 5. Each Party shall ensure that, where information is required to be published in accordance with provisions of this Chapter, such information will be published on the internet.

#### **Article 13.11: Cross-Border Transfer of Information by Electronic Means**

- 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:
  - (a) measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or
  - (b) any measure that it considers necessary for protection of its essential security interests.

#### **Article 13.12: 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. Neither 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, except where such a measure exists at the date of entry into force of this Agreement. A Party may promptly renew a measure in existence at the date of entry into force of this Agreement or amend such a measure to make it less trade restrictive, at any time. Where

a Party amends such a measure to make it less trade restrictive, it shall not subsequently amend that measure to make it more trade restrictive than it was immediately before that amendment.

3. Nothing in this Article shall prevent a Party from adopting or maintaining:
  - (a) measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or
  - (b) any measure that it considers necessary for the protection of its essential security interests.

### **Article 13.13: Source Code**

1. Neither Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.
2. For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure, or software that is specifically made for use by a Party.
3. Nothing in this Article shall preclude:
  - (a) the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts; or
  - (b) a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement.
4. This Article shall not be construed to affect requirements that relate to patent applications or granted patents, including any orders made by a judicial authority in relation to patent disputes, subject to safeguards against unauthorised disclosure under the law or practice of a Party.
5. Nothing in this Article shall prevent a Party from adopting or maintaining any measures that it considers necessary for the protection of its essential security interests.