

## **CHAPTER 9 DIGITAL TRADE**

### **Article 9.1: Definitions**

For the purposes of this Chapter:

**Electronic authentication** means the process or act of verifying the identity of a party to an electronic communication or transaction and ensuring the integrity of an electronic communication;

**Electronic transmission** means a transmission made using any electromagnetic means, including by photonic means;

**Open government data** means information, including data, made available to the public by the central level of government;

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

**Trade administration documents** means forms issued or controlled by a Party that must be completed by or for an importer or exporter in connection with the import or export of goods; and

**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 9.2: Objectives**

1. The Parties recognise the economic growth and opportunity that electronic commerce provides, the importance of frameworks that promote consumer confidence in electronic commerce, and the importance of facilitating the development and use of electronic commerce.
2. The objectives of this Chapter are to:
  - (a) promote digital trade between the Parties and the wider use of electronic commerce globally;
  - (b) contribute to creating an environment of trust and confidence in the use of electronic commerce; and

- (c) enhance cooperation between the Parties regarding development of electronic commerce.

### **Article 9.3: General Provisions**

1. This Chapter shall apply to measures adopted or maintained by a Party that affect trade by electronic means.
2. This Chapter shall not apply to:
  - (a) government procurement;
  - (b) information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection, except for Article 9.13 (Open Government Data); or
  - (c) financial services and financial service suppliers as defined in the Annex of Financial Services of the GATS.
3. For greater certainty, the Parties affirm that measures affecting the supply of a service delivered or performed electronically are subject to the relevant provisions of Chapter 8 (Trade in Services) and its Annexes and Chapter 10 (Investment Facilitation), including any exception or limitation set out in this Agreement that is applicable to such provisions.

### **Article 9.4: Customs Duties**

1. Each Party shall maintain its current practice of not imposing customs duties on electronic transmissions between the Parties.
2. The practice referred to in paragraph 1 is in accordance with the WTO Ministerial Decision of 2 March 2024 in relation to the Work Programme on Electronic Commerce (WT/MIN(24)/38).
3. Each Party may adjust its practice referred to in paragraph 1 with respect to any further outcomes in the WTO Ministerial Decisions on customs duties on electronic transmissions within the framework of the Work Programme on Electronic Commerce.
4. The Parties shall review this Article in light of any further WTO Ministerial Decisions in relation to the Work Programme on Electronic Commerce.
5. For greater certainty, paragraph 1 shall not preclude a Party from imposing taxes, fees, or other charges on electronic transmissions, provided that such taxes, fees, or charges are imposed in a manner consistent with this Agreement.

### **Article 9.5: Domestic Electronic Transactions Framework**

1. Each Party shall endeavour to 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 on November 23, 2005*.
2. Each Party shall endeavour to avoid any unnecessary regulatory burden on electronic transactions.

### **Article 9.6: Electronic Authentication and Electronic Signature**

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. Taking into account international norms for electronic authentication, each Party shall endeavour to:
  - (a) permit participants in electronic transactions to determine appropriate electronic authentication technologies and implementation models for their electronic transactions;
  - (b) not limit the recognition of electronic authentication technologies and implementation models for electronic transactions; and
  - (c) permit participants in electronic transactions to have the opportunity to prove that their electronic transactions comply with its laws and regulations with respect to electronic authentication.
3. Notwithstanding paragraph 2, a Party may require that, for a particular category of electronic 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 Parties shall encourage the use of interoperable electronic authentication.

### **Article 9.7: Paperless Trading**

1. 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.
2. The Parties shall cooperate in international fora to enhance acceptance of electronic versions of trade administration documents.

### **Article 9.8: Online Consumer Protection**

1. The Parties recognise the importance of adopting and maintaining transparent and effective consumer protection measures for electronic commerce as well as other measures conducive to the development of consumer confidence.
2. Each Party shall endeavour to adopt or maintain consumer protection laws or regulations to proscribe misleading, deceptive, and fraudulent commercial activities that cause harm or potential harm to consumers engaged in electronic commerce.

### **Article 9.9: Online Personal Information Protection**

1. The Parties recognise the economic and social benefits of protecting the personal information of persons who conduct or engage in electronic transactions and the contribution that this makes to enhancing consumer confidence in electronic commerce.
2. To this end, each Party shall endeavour to adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce.<sup>1</sup> In the development of any legal framework for the protection of online personal information, each Party shall endeavour to take into account principles and guidelines of relevant international organisations.
3. The Parties shall cooperate, to the extent possible, for the protection of personal information transferred by any electronic means from a Party.

### **Article 9.10: Principles on Access to and Use of the Internet for Electronic Commerce**

To support the sustainable development and growth of electronic commerce, each Party recognises that consumers in its territory should be able to:

- (a) access and use services and applications of their choice, unless prohibited by the Party's laws and regulations;
- (b) run services and applications of their choice, subject to the Party's laws and regulations, including the needs of legal and regulatory enforcement activities; and
- (c) connect their choice of devices to the Internet, provided that such devices do not harm the network and are not otherwise prohibited by the Party's laws and regulations.

---

<sup>1</sup> For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.

### **Article 9.11: Unsolicited Commercial Electronic Messages**

1. Each Party shall endeavour to adopt or maintain measures regarding unsolicited commercial electronic messages that:
  - (a) require a supplier of unsolicited commercial electronic messages to facilitate the ability of a recipient to prevent ongoing reception of those messages;
  - (b) require the consent, as specified in 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 endeavour to provide recourse against a supplier of unsolicited commercial electronic messages that does not comply with a measure 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 9.12: Cross-Border Transfer of Information by Electronic Means**

Recognising the importance of the cross-border transfer of information by electronic means in facilitating trade, and the importance of protecting personal data/information and sensitive data/information and information of entities in its territory, the Parties shall endeavour to refrain from imposing or maintaining unnecessary barriers to cross-border transfer of information by electronic means when this activity is for the conduct of business objectives in accordance with laws and regulations of each Party.

### **Article 9.13: Open Government Data**

1. The Parties recognise that facilitating public access to and use of open government data may foster economic and social development, competitiveness, and innovation.
2. To the extent that a Party makes government data available to the public, it is encouraged, to the extent practicable, to ensure that the information is made available in an open or machine readable format that allows it to be searched, retrieved, used, reused, and redistributed freely by the public.
3. The Parties shall endeavour to cooperate in matters that facilitate and expand public access to, and use of, open government data with a view to encouraging the development of electronic commerce and creating business opportunities.
4. For greater certainty, this Article is without prejudice to a Party's laws and regulations, including, but not limited to, intellectual property and personal information/data protection.

#### **Article 9.14: Digital Government**

1. The Parties recognise that electronic and digital technology can enable more efficient government operations, improve the quality and reliability of government services, and enable governments to better serve the needs of their citizens and other stakeholders.
2. To this end, the Parties shall endeavour to develop and implement strategies to digitally transform their respective government operations and services.
3. Recognising that the Parties can benefit by sharing their experiences with electronic or digital government initiatives, the Parties shall endeavour to cooperate on activities relating to the digital transformation of government and government services, which may include:
  - (a) exchanging information and experiences on digital government strategies and policies;
  - (b) sharing best practices on digital government and the digital delivery of government services; and
  - (c) providing advice or training, including through exchange of officials, and technical assistance projects, to assist the other Party in building digital government capacity.

#### **Article 9.15: Electronic Invoicing**

1. The Parties recognise the importance of electronic invoicing, which increases the efficiency, accuracy, and reliability of transactions.
2. The Parties recognise the benefits of interoperable electronic invoicing systems. When developing measures related to electronic invoicing, a Party shall endeavour to take into account international standards, where applicable, and in accordance with its readiness in terms of capacity, regulations, and infrastructure.
3. The Parties agree to cooperate and collaborate on initiatives which promote, encourage, support, or facilitate the adoption of e-invoicing.

#### **Article 9.16: Digital Identities**

Recognising that cooperation between the Parties on digital identities for natural persons and enterprises will promote connectivity and further growth of digital trade, and recognising that each Party may take different legal and technical approaches to digital identities, the Parties shall endeavour to pursue mechanisms to promote compatibility between their respective digital identity regimes. This may include:

- (a) promoting technical interoperability between Parties' implementation of digital identities;

- (b) developing comparable protection of digital identities under each Party's respective legal frameworks, or the recognition of their legal effects, whether accorded autonomously or by agreement;
- (c) supporting the development of international frameworks on digital identity regimes; and
- (d) exchanging knowledge and expertise on best practices relating to digital identity policies and regulations, technical implementation and security standards, and the promotion of the use of digital identities.

#### **Article 9.17: Cooperation**

1. Recognising the importance of digital trade to their collective economies, the Parties shall endeavour to maintain a mechanism of cooperation on regulatory matters relating to digital trade with a view to sharing information and experiences.
2. The Parties have a shared vision to promote secure digital trade and recognise that threats to cybersecurity undermine confidence in digital trade. Accordingly, the Parties recognise the importance of cooperation in:
  - (a) building the capabilities of their government agencies responsible for computer security incident response;
  - (b) using existing collaboration mechanisms to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties; and
  - (c) promoting the development of a strong public and private workforce in the area of cybersecurity.