CHAPTER 4

ELECTRONIC COMMERCE

ARTICLE 4.1

Definitions

1. For the purposes of this Chapter, Article 3.3 (Definitions*)* applies.

2. For the purposes of this Chapter:

   (a) "electronic signature" means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

   (b) "electronic seal" means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;

   (c) "electronic transmissions" means transmissions of electronic data through the Internet;

   (d) "electronic trust service" means an electronic service normally provided for remuneration, which consists of any of the following:

      (i) the issuance and validation of certificates for electronic signatures, electronic seals, website authentication or certificates for the provision of other trust services;

      (ii) the creation and validation of electronic signatures, electronic seals and electronic time stamps;

      (iii) the preservation of electronic signatures, electronic seals and related certificates;

      (iv) the management of remote electronic signature creation devices or remote electronic seal creation devices;

      (v) the issuance and validation of electronic attestations of attributes;

      (vi) the provision of electronic registered delivery services and validation of data transmitted through electronic registered delivery services and related evidence;

      (vii) the electronic archiving of electronic data and electronic documents;

      (viii) the recording of electronic data in an electronic ledger.

   (e) "end-user" means a person who purchases or subscribes to an Internet access service from an Internet access service provider;

(f) "surveillance (control)" means activities carried out and measures taken by authorities authorised by domestic law or regulations to ensure that goods and services comply with domestic laws and regulations and do not pose a threat to health and safety or any other aspect of public interest protection;

(g) "surveillance (control) authority" means an authority responsible for carrying out surveillance (control);

(h) "personal data" means any information relating to an identified or identifiable natural person;

(i) "processing" of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, accumulation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, depersonalisation, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data, including by using information (automated) systems;

(j) "trade administration documents" means documents, forms or other information, including in electronic formats, as required by a Party's domestic legislation on commercial trade transactions;

(k) "unsolicited commercial electronic messages" means electronic messages for commercial purposes without the consent of the recipient or against the explicit rejection of the recipient.

ARTICLE 4.2

Scope

1. This Chapter applies to measures of the Parties affecting trade enabled by electronic means.

2. In the event of any inconsistency between this Chapter and Annex IX (Financial Services); Annex IX (Financial Services), shall prevail.

3. This Chapter shall not apply to audio-visual services.

ARTICLE 4.3

General Provisions

The Parties recognise:

(a) the economic growth and opportunities that electronic commerce in goods and services provides, in particular for businesses and consumers as well as the potential for enhancing international trade;

(b) the importance of avoiding barriers to the use and development of electronic commerce in goods and services; and

(c) the need to create an environment of trust and confidence in as well as security for electronic commerce, in particular by:

(i) the protection of privacy of natural persons in relation to the processing of personal data;

(ii) the protection of confidentiality of individual records and accounts, and commercial secrets;

(iii) measures to prevent and proscribe deceptive and fraudulent practices or to deal with the effects of a default on contracts; and

(iv) measures against unsolicited commercial electronic messages.

ARTICLE 4.4

Right to Regulate

The Parties reaffirm the right to regulate in the area of electronic commerce in conformity with this Chapter to achieve legitimate policy objectives.

ARTICLE 4.5

Customs Duties[4]

1. No Party shall impose customs duties on electronic transmissions.

2. For greater certainty, paragraph 1 shall not preclude a Party from imposing internal taxes, fees, or other charges on electronic transmissions, provided that they are imposed in a manner consistent with this Agreement.

ARTICLE 4.6

Electronic Authentication, Trust Services and Contracts by Electronic Means

1. No Party shall deny the legal effect and admissibility as evidence in legal proceedings of an electronic document, electronic signature, electronic seal, electronic time stamp or of data sent and received using an electronic registered delivery service, solely on the ground that it is in electronic form.

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

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

[4] It is understood that "customs duties" means import and export duties.

(b) prevent parties to an electronic transaction from being able to prove to judicial or administrative authorities that the use of electronic authentication or an electronic trust service in that transaction complies with the applicable legal requirements.

3. Notwithstanding paragraph 2, each Party may require that for a particular category of transactions, the method of electronic authentication or trust service is either certified by an authority accredited in accordance with its domestic laws and regulations or that the method meets certain performance standards which shall be objective, transparent and non-discriminatory and shall only relate to the specific characteristics of the category of transactions concerned.

4. Except to the extent provided under a Party's domestic laws and regulations in relation to certain types of contracts, a Party shall not deny that contracts may be concluded by electronic means.

5. Each Party shall ensure that its domestic laws and regulations do not deprive electronic contracts of legal effect and validity solely on the ground that the contracts have been made by electronic means.

ARTICLE 4.7

Paperless Trade Administration

1. Each Party shall make all trade administration documents publicly available in electronic form.

2. Each Party shall accept electronic versions of trade administration documents as legal equivalents of paper documents except if:

(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.

ARTICLE 4.8

Open Internet Access

Subject to applicable domestic laws and regulations, each Party shall adopt or maintain appropriate measures to ensure that end-users in its territory are able to:

(a) access, distribute and use services and applications of their choice available through the Internet, subject to reasonable and non-discriminatory network management;

(b) connect devices of their choice to the Internet, provided that such devices comply with the requirements in the territory where they are used and do not harm the network; and

(c) have access to information on the network management practices of their Internet access service supplier.

ARTICLE 4.9

Online Consumer Trust

1. Each Party shall adopt or maintain measures to ensure the effective protection of consumers engaging in electronic commerce transactions, including but not limited to measures that:

(a) proscribe fraudulent and deceptive commercial practices;

(b) require suppliers of goods and services to act in good faith and abide by fair commercial practices, including through the prohibition of charging consumers for unsolicited goods and services;

(c) require suppliers of goods and services to provide consumers with clear and thorough information regarding their identity and contact details[5], as well as information regarding the goods and services, the transaction and the applicable consumer rights; and

(d) grant consumers access to redress to claim their rights, including a right to remedies in cases where goods or services are paid and not delivered or provided as agreed.

2. The Parties recognise the importance of entrusting their consumer protection agencies or other relevant bodies with adequate enforcement powers and the importance of cooperation between their agencies in the enforcement of their respective domestic laws and regulations related to consumer protection and online consumer trust.

3. The Parties recognise the importance of promoting effective policy frameworks relating to consumer product safety.

ARTICLE 4.10

Unsolicited Commercial Electronic Messages

1. In order to protect users effectively against unsolicited commercial electronic messages, each Party shall adopt or maintain measures that:

(a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of such messages; and

(b) require the consent, as specified according to its domestic laws and regulations, of recipients to receive commercial electronic messages.

---

[5] In the case of intermediary service suppliers, this also includes the identity and contact details of the actual supplier of the goods and services.

2. Each Party shall provide access to recourse against suppliers of unsolicited commercial electronic messages who do not comply with its measures implemented pursuant to paragraph 1.

ARTICLE 4.11

Cross-border Data Flows

1. The Parties commit to ensuring cross-border data flows to facilitate digital trade. To that end, cross-border data flows shall not be restricted between the Parties by:[6]

(a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the Party´s territory;

(b) requiring the localisation of data in the Party's territory for storage or processing;

(c) prohibiting storage or processing in the territory of the other Party; or

(d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory.

2. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 to achieve a legitimate public policy objective,[7] provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade; and

(b) does not impose restrictions on transfers of information that are greater than necessary to achieve the objective.[8]

3. The Parties shall review the implementation of this Article and assess its functioning in the Joint Committee. The first such review shall take place no later than three years from the entry into force of this Agreement.

---

[6] With respect to financial services, this provision applies as long as the financial supervisory authorities have access to the necessary data for fulfilling their supervisory tasks.

[7] For the purposes of this Article, "legitimate public policy objective" shall be interpreted in an objective manner and shall enable the pursuit of objectives such as the protection of public security, public morals, human, animal or plant life or health, the maintenance of public order or other similar objectives of public interest, taking into account the evolving nature of digital technologies.

[8] For greater certainty, paragraph 2 does neither affect the interpretation of other exceptions in this Agreement and their application to this Article, nor diminish the right of a Party to invoke any of them.

ARTICLE 4.12

Electronic Payments and Invoicing

1. The Parties recognise the pivotal role of electronic payments in enabling electronic commerce and the rapid growth of electronic payments. The Parties agree to support the development of efficient, safe and secure cross-border electronic payments by fostering the adoption and use of internationally accepted standards, promoting interoperability and the interlinking of payment infrastructures, and encouraging useful innovation and competition in the payment's ecosystem.

2. The Parties recognise the importance of e-invoicing, which increases the efficiency, accuracy and reliability of commercial transactions and agree to promote the adoption of interoperable systems for e-invoicing.

3. The Parties shall support and facilitate the adoption of e-invoicing by undertakings. To this end, the Parties shall endeavour to:

(a) promote the existence of underlying infrastructure to support e-invoicing; and

(b) generate awareness of and build capacity for e-invoicing.

ARTICLE 4.13

Protection of Personal Data and Privacy

1. The Parties recognise that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to the development of digital trade and trust therein.

2. Each Party shall adopt or maintain safeguards it deems appropriate to ensure a high level of protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this Agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards.

3. The Parties shall inform each other about any safeguards they adopt or maintain according to paragraph 2.

ARTICLE 4.14

Transfer of or Access to Source Code

1. No Party shall require the transfer of, or access to, the source code of software or parts thereof owned by a natural or juridical person of another Party.

2. The provisions of paragraph 1shall not apply to:

(a) requirements by a court or administrative tribunal;

(b) intellectual property rights and their protection and enforcement;

(c) competition law and its enforcement;

(d) the right of a Party to take measures in accordance with Chapter 7 (Government Procurement);

(e) requirements by surveillance (control) authorities in order to verify the conformity of goods and services with legal requirements; or

(f) the voluntary transfer or granting of access to source code on a commercial basis by a natural or juridical person of a Party.

ARTICLE 4.15

Cooperation on Electronic Commerce

1. The Parties may engage in a dialogue on regulatory issues raised in relation to electronic commerce, which could, *inter alia*, address the following issues:

(a) the liability of intermediary service providers with respect to the transmission and storage of information;

(b) the treatment of unsolicited commercial electronic messages;

(c) the interoperability of infrastructures, such as secure electronic authentication and payments;

(d) consumer protection; and

(e) other issues relevant for the development of electronic commerce.

2. Such a dialogue may include exchange of information on the Parties' respective domestic laws and regulations on these issues as well as on the implementation of such domestic laws and regulations.

ARTICLE 4.16

General Exceptions

For the purposes of this Chapter, Article XX of the GATT 1994 and Article XIV of the GATS apply, and are hereby incorporated into and made part of this Agreement, *mutatis mutandis*.

ARTICLE 4.17

Security Exceptions

For the purposes of this Chapter, Article XXI of the GATT 1994 and Article XIV *bis* of the GATS apply, and are hereby incorporated into and made part of this Agreement, *mutatis mutandis.*