CHAPTER 4

DIGITAL TRADE

ARTICLE 4.1

Objectives

1. The Parties recognise the economic growth and opportunities provided by digital trade and the importance of adopting or maintaining frameworks that promote consumer confidence in digital trade and of avoiding unnecessary barriers to its use and development.

2. The Parties recognise the importance of the principle of technological neutrality in digital trade.

ARTICLE 4.2

Definitions

For the purposes of this Chapter:

(a) "computing facilities" means a computer server or storage device for processing or storing information for commercial use;

(b) "electronic authentication" means an electronic process that enables the confirmation of:

(i) the electronic identification of a person; or

(ii) the origin and integrity of data in electronic form;

(c) "electronic registered delivery service" means a service that makes it possible to transmit data between persons by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;

(d) "electronic seal" means data in electronic form used by a legal person which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;

(e) "electronic signature" means data in electronic form which is attached to or logically associated with other data in electronic form that is:

(i) used by a natural person to agree on the data in electronic form to which it relates; and

(ii) linked to the data in electronic form to which it relates in such a way that any subsequent alteration in the data is detectable;

(f) "electronic time stamp" means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;

(g) "electronic trust service" means an electronic service consisting of:

(i) the creation, verification and validation of electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services and certificates related to those services;

(ii) the creation, verification and validation of certificates for website authentication; or

(iii) the preservation of electronic signatures, seals or certificates related to those services;

(h) "emerging technology" means an enabling and innovative technology that has potentially significant application across a wide range of existing and future sectors, including:

(i) artificial intelligence;

(ii) distributed ledger technologies;

(iii) quantum technologies;

(iv) immersive technologies; and

(v) the Internet of Things;

(i) "end-user" means a natural person, or legal person to the extent provided for in a Party's law, using or requesting a public telecommunications service, either as a consumer or for trade, business or professional purposes;

(j) "government data" means data owned or held by any level of government and by non-governmental bodies in the exercise of powers conferred on them by any level of government;

(k) "legal person" means any legal entity duly constituted or otherwise organised under applicable law, whether for profit or otherwise, and whether privately-owned or governmentally-owned, including any

corporation, trust, partnership, joint venture, sole proprietorship or association;

(l) "measures of a Party" means measures adopted or maintained by:

(i) central, regional or local governments and authorities; and

(ii) non-governmental bodies in the exercise of powers delegated by central, regional or local governments or authorities;

(m) "person" means a natural person or a legal person;

(n) "personal data" means any information about an identified or identifiable natural person;

(o) "public telecommunications service" means any telecommunications service that is offered to the public generally; and

(p) "unsolicited commercial electronic message" means an electronic message[52] which is sent for commercial or marketing purposes, without the consent or despite the explicit rejection of the recipient, directly to an end-user via a public telecommunications service.

ARTICLE 4.3

Scope

1. This Chapter applies to measures of a Party affecting trade enabled by electronic means.

2. This Chapter does not apply to:

(a) audio-visual services;

(b) gambling services;

(c) government procurement, except for Article 4.5 (Electronic Contracts) and Article 4.6 (Electronic Authentication and Electronic Trust Services); and

(d) except for Article 4.14 (Open Government Data), information held or processed by or on behalf of a Party, or measures of a Party related to that information, including measures related to its collection.

[52] For greater certainty, an electronic message includes electronic mail and text (Short Message Service) and multimedia (Multimedia Message Service) messages.

ARTICLE 4.4[53]

Customs Duties

1. A Party shall not impose customs duties on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of another Party.

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

ARTICLE 4.5

Electronic Contracts

Except as otherwise provided for in its law, a Party shall not adopt or maintain measures that:

(a) deprive an electronic contract of legal effect, enforceability or validity, solely on the ground that the contract has been made by electronic means; or

(b) otherwise create obstacles for the use of electronic contracts.

ARTICLE 4.6

Electronic Authentication and Electronic Trust Services

1. A Party shall not deny the legal effect and admissibility as evidence in legal proceedings of an electronic document, an electronic signature, an electronic seal, an electronic time stamp, the authenticating data resulting from electronic authentication, or of data sent and received using an electronic registered delivery service, solely on the ground that it is in electronic form.

2. A Party shall not 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

(b) prevent parties to an electronic transaction from being able to prove to judicial and administrative authorities that the use of electronic

[53] Pursuant to Article 1.4 (Trade and Economic Relations Governed by this Agreement) of Chapter 1 (General Provisions), this Article shall not apply to Liechtenstein.

authentication or an electronic trust service in that transaction complies with the applicable legal requirements.

3. Notwithstanding paragraph 2, a Party may require that for a particular category of transactions, the method of electronic authentication or electronic trust service is certified by an authority accredited in accordance with its law or 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. In accordance with their respective international obligations, the Parties shall encourage the use of interoperable electronic trust services and electronic authentication, and the mutual recognition of electronic trust services and electronic authentication issued by a recognised provider of electronic trust services.

ARTICLE 4.7[54]

Paperless Trading

1. The Parties affirm their commitments under Article 2.53 (Data, Documentation and Automation) of Section 2.4 (Customs and Trade Facilitation).

2. The Parties shall encourage their competent authorities and other relevant bodies to cooperate on matters related to paperless trading, such as the standardisation of trade administration documents.

3. In developing initiatives concerning the use of paperless trading, the Parties shall endeavour to take into account the principles and guidelines of relevant international bodies.

ARTICLE 4.8

Online Consumer Protection

1. Each Party shall adopt or maintain measures that contribute to online consumer trust, including laws and regulations that proscribe unfair, misleading, fraudulent and deceptive commercial practices that cause harm or potential harm to consumers.

2. The Parties recognise the importance of cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to digital trade between the Parties in order to enhance consumer welfare.

---

[54] Pursuant to Article 1.4 (Trade and Economic Relations Governed by this Agreement) of Chapter 1 (General Provisions), this Article shall not apply to Liechtenstein.

ARTICLE 4.9

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; or

   (b) require the consent, as specified according to its law, of recipients to receive commercial electronic messages.

2. Each Party shall require suppliers of unsolicited commercial electronic messages to ensure that these messages are clearly identifiable as such, clearly disclose on whose behalf they are made and contain the necessary information to enable end-users to request cessation free of charge and at any time.

3. Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained pursuant to paragraphs 1 and 2.

ARTICLE 4.10

Source Code

1. A Party shall not 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 that software, or of a product containing that software, in that Party.

2. Paragraph 1 does not apply to the voluntary transfer of, or grant of access to, source code of software by a person of another Party:

   (a) under open source licences, such as in the context of open source coding; or

   (b) on a commercial basis, such as in the context of a freely negotiated contract.

3. Nothing in this Article shall preclude a regulatory body or judicial authority of a Party, or a Party with respect to a conformity assessment body, from requiring a person of another Party:

(a) to preserve and make available[55] source code of software for an investigation, inspection, examination, enforcement action or a judicial proceeding, or the monitoring of compliance with codes of conduct and other standards, subject to safeguards against unauthorised disclosure; and

(b) to transfer or provide access to source code of software for the purpose of the imposition and enforcement of a remedy granted in accordance with that Party's law following an investigation, inspection, examination, enforcement action or a judicial proceeding.

ARTICLE 4.11

Cross-Border Data Flows

1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by a Party:

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

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

   (c) prohibiting the storage or processing of data in another Party; or

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

2. The Parties shall keep the implementation of this provision under review and assess its functioning within three years of the date of entry into force of this Agreement. A Party may at any time propose that the Parties review the list of restrictions listed in paragraph 1. Such a request shall be accorded sympathetic consideration.

[55] The Parties understand that this making available shall not be construed to negatively affect the status of the source code of software as a trade secret.

ARTICLE 4.12

Protection of Personal Data and Privacy

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

2. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures for the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application[56] for the protection of the data transferred.

3. Each Party shall inform the other Parties about any measure referred to in paragraph 2 that it adopts or maintains.

ARTICLE 4.13

Open Internet Access

Subject to their applicable policies, laws and regulations, each Party should adopt or maintain appropriate measures to ensure that end-users in that Party may:

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

(b) connect devices of their choice to the Internet, provided that these devices do not harm the network; and

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

ARTICLE 4.14

Open Government Data

1. The Parties recognise that facilitating public access to and use of government data fosters economic and social development, competitiveness and innovation.

2. To the extent that a Party chooses to make government data available to the public, it shall endeavour to ensure that the data is in a machine-readable

[56] For greater certainty, "conditions of general application" refer to conditions formulated in objective terms that apply horizontally to an unidentified number of economic operators and thus cover a range of situations and cases.

and open format and can be searched, retrieved, used, reused and redistributed.

3. The Parties shall endeavour to cooperate to identify ways in which each Party can expand access to and the use of government data that the Party has made available to the public, with a view to enhancing and generating business opportunities, especially for small and medium-sized enterprises.

ARTICLE 4.15

Cybersecurity

1. The Parties recognise that threats to cybersecurity undermine confidence in digital trade.

   Accordingly, the Parties shall endeavour to:

   (a) build the capabilities of their respective national entities responsible for cybersecurity incident response, taking into account the evolving nature of cybersecurity threats;

   (b) establish, or strengthen existing, collaboration mechanisms for cooperating to anticipate, identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents; and

   (c) maintain a dialogue on matters related to cybersecurity, including for the sharing of information and experiences for awareness and best practices in respect of risk-based approaches to addressing cybersecurity threats.

2. Given the evolving nature of cybersecurity threats, the Parties recognise that risk-based approaches may be more effective than prescriptive approaches in addressing those threats. Accordingly, each Party shall endeavour to encourage legal persons within its jurisdiction to use risk-based approaches to protect against cybersecurity risks.

ARTICLE 4.16

Cooperation on Regulatory Issues with Regard to Digital Trade

1. The Parties shall, where appropriate, cooperate and participate actively in multilateral fora, including the WTO, to promote the development of international frameworks for digital trade.

2. The Parties shall endeavour to cooperate on regulatory matters of mutual interest in the context of digital trade, including:

(a) the recognition and facilitation of interoperable electronic authentication and electronic trust services;

(b) the treatment of unsolicited commercial electronic messages;

(c) the conclusion and use of electronic contracts; and

(d) the protection of consumers.

ARTICLE 4.17

Emerging Technology Dialogue

1. The Parties recognise the importance of:

(a) emerging technology as a contributor to economic growth and quality of life;

(b) developing standards relating to emerging technology;

(c) promoting public trust in the development and use of emerging technology;

(d) facilitating and promoting investment in emerging technology research and development;

(e) training workforces to use emerging technology; and

(f) collaboration between government and non-governmental entities in relation to the development, use and regulation of emerging technology.

2. The Parties shall establish a strategic dialogue on emerging technology (Dialogue), which shall meet as decided by the Parties. The Parties shall, through the Dialogue, endeavour to:

(a) cooperate on issues and developments relating to emerging technology, such as ethical use, human diversity and unintended biases, technical standards and algorithmic transparency;

(b) exchange information, and share experiences and best practices on laws, regulations, policies, enforcement and compliance relating to emerging technology;

(c) promote collaboration between government and non-governmental entities of the Parties in relation to investment, research and development opportunities in emerging technology;

(d) promote the involvement of non-governmental persons or groups in the Dialogue; and

(e) discuss any other matter related to this Article they consider appropriate.