TITLE III

DIGITAL TRADE

CHAPTER 1

GENERAL PROVISIONS

ARTICLE 196

Objective

The objective of this Title is to facilitate digital trade, to address unjustified barriers to trade enabled by electronic means and to ensure an open, secure and trustworthy online environment for businesses and consumers.

ARTICLE 197

Scope

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

2. This Title does not apply to audio-visual services.

ARTICLE 198

Right to regulate

The Parties reaffirm the right to regulate within their territories to achieve legitimate policy objectives, such as the protection of public health, social services, public education, safety, the environment including climate change, public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity.

ARTICLE 199

Exceptions

For greater certainty, nothing in this Title prevents the Parties from adopting or maintaining measures in accordance with Articles 184, 412 and 415 for the public interest reasons set out therein.

ARTICLE 200

Definitions

1. The definitions in Article 124 apply to this Title.

2. For the purposes of this Title, the following definitions apply:

(a) "consumer" means any natural person using a public telecommunications service for other than professional purposes;

(b) "direct marketing communication" means any form of commercial advertising by which a natural or legal person communicates marketing messages directly to a user via a public telecommunications service and covers at least electronic mail and text and multimedia messages (SMS and MMS);

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

(i) the electronic identification of a natural or legal person, or

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

(d) "electronic registered delivery service" means a service that makes it possible to transmit data between third parties 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;

(e) "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;

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

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

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

(g) "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;

(h) "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;

(i) "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;

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

(k) "user" means any natural or legal person using a public telecommunications service.

CHAPTER 2

DATA FLOWS AND PERSONAL DATA PROTECTION

ARTICLE 201

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

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

(c) prohibiting the 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 Parties' territory or upon localisation requirements in the Parties' territory.

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 to the other Party to review the list of restrictions listed in paragraph 1. Such a request shall be accorded sympathetic consideration.

ARTICLE 202

Protection of personal data and privacy

1. Each Party recognises 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 on 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[1] for the protection of the data transferred.

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

CHAPTER 3

SPECIFIC PROVISIONS

ARTICLE 203

Customs duties on electronic transmissions

1. Electronic transmissions shall be considered as the supply of a service within the meaning of Title II of this Heading.

2. The Parties shall not impose customs duties on electronic transmissions.

[1] 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.

ARTICLE 204

No prior authorisation

1. A Party shall not require prior authorisation of the provision of a service by electronic means solely on the ground that the service is provided online, and shall not adopt or maintain any other requirement having an equivalent effect.

A service is provided online when it is provided by electronic means and without the parties being simultaneously present.

2. Paragraph 1 does not apply to telecommunications services, broadcasting services, gambling services, legal representation services or to the services of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority.

ARTICLE 205

Conclusion of contracts by electronic means

1. Each Party shall ensure that contracts may be concluded by electronic means and that its law neither creates obstacles for the use of electronic contracts nor results in contracts being deprived of legal effect and validity solely on the ground that the contract has been made by electronic means.

2. Paragraph 1 does not apply to the following:

(a) broadcasting services;

(b) gambling services;

(c) legal representation services;

(d) the services of notaries or equivalent professions involving a direct and specific connection with the exercise of public authority;

(e) contracts that require witnessing in person;

(f) contracts that establish or transfer rights in real estate;

(g) contracts requiring by law the involvement of courts, public authorities or professions exercising public authority;

(h) contracts of suretyship granted, collateral securities furnished by persons acting for purposes outside their trade, business or profession; or

(i) contracts governed by family law or by the law of succession.

ARTICLE 206

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 or an 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. 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 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 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 only relate to the specific characteristics of the category of transactions concerned.

ARTICLE 207

Transfer of or access to source code

1. A Party shall not require the transfer of, or access to, the source code of software owned by a natural or legal person of the other Party.

2. For greater certainty:

(a) the general exceptions, security exceptions and prudential carve-out referred to in Article 199 apply to measures of a Party adopted or maintained in the context of a certification procedure; and

(b) paragraph 1 of this Article does not apply to the voluntary transfer of, or granting of access to, source code on a commercial basis by a natural or legal person of the other Party, such as in the context of a public procurement transaction or a freely negotiated contract.

3. Nothing in this Article shall affect:

(a) a requirement by a court or administrative tribunal, or a requirement by a competition authority pursuant to a Party's competition law to prevent or remedy a restriction or a distortion of competition;

(b) a requirement by a regulatory body pursuant to a Party's laws or regulations related to the protection of public safety with regard to users online, subject to safeguards against unauthorised disclosure;

(c) the protection and enforcement of intellectual property rights; and

(d) the right of a Party to take measures in accordance with Article III of the GPA as incorporated by Article 277 of this Agreement.

ARTICLE 208

Online consumer trust

1. Recognising the importance of enhancing consumer trust in digital trade, 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 or services to provide consumers with clear and thorough information, including when they act through intermediary service suppliers, regarding their identity and contact details, the transaction concerned, including the main characteristics of the goods or services and the full price inclusive of all applicable charges, and the applicable consumer rights (in the case of intermediary service suppliers, this includes enabling the provision of such information by the supplier of goods or services); and

(d) grant consumers access to redress for breaches of their rights, including a right to remedies if goods or services are paid for and are 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 these agencies in order to protect consumers and enhance online consumer trust.

ARTICLE 209

Unsolicited direct marketing communications

1. Each Party shall ensure that users are effectively protected against unsolicited direct marketing communications.

2. Each Party shall ensure that direct marketing communications are not sent to users who are natural persons unless they have given their consent in accordance with each Party's laws to receiving such communications.

3. Notwithstanding paragraph 2, a Party shall allow natural or legal persons who have collected, in accordance with conditions laid down in the law of that Party, the contact details of a user in the context of the supply of goods or services, to send direct marketing communications to that user for their own similar goods or services.

4. Each Party shall ensure that direct marketing communications are clearly identifiable as such, clearly disclose on whose behalf they are made and contain the necessary information to enable users to request cessation free of charge and at any moment.

5. Each Party shall provide users with access to redress against suppliers of direct marketing communications that do not comply with the measures adopted or maintained pursuant to paragraphs 1 to 4.

ARTICLE 210

Open government data

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

2. To the extent that a Party chooses to make government data accessible to the public, it shall endeavour to ensure, to the extent practicable, that the data:

(a) is in a format that allows it to be easily searched, retrieved, used, reused, and redistributed;

(b) is in a machine-readable and spatially-enabled format;

(c) contains descriptive metadata, which is as standard as possible;

(d) is made available via reliable, user-friendly and freely available Application Programming Interfaces;

(e) is regularly updated;

(f) is not subject to use conditions that are discriminatory or that unnecessarily restrict re-use; and

(g) is made available for re-use in full compliance with the Parties' respective personal data protection rules.

3. The Parties shall endeavour to cooperate to identify ways in which each Party can expand access to, and use of, government data that the Party has made public, with a view to enhancing and generating business opportunities, beyond its use by the public sector.

ARTICLE 211

Cooperation on regulatory issues with regard to digital trade

1. The Parties shall exchange information on regulatory matters in the context of digital trade, which shall address the following:

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

(b) the treatment of direct marketing communications;

(c) the protection of consumers; and

(d) any other matter relevant for the development of digital trade, including emerging technologies.

2. Paragraph 1 shall not apply to a Party's rules and safeguards for the protection of personal data and privacy, including on cross-border transfers of personal data.

ARTICLE 212

Understanding on computer services

1. The Parties agree that, for the purpose of liberalising trade in services and investment in accordance with Title II of this Heading, the following services shall be considered as computer and related services, regardless of whether they are delivered via a network, including the internet:

(a) consulting, adaptation, strategy, analysis, planning, specification, design, development, installation, implementation, integration, testing, debugging, updating, support, technical assistance or management of or for computers or computer systems;

(b) computer programmes defined as the sets of instructions required to make computers work and communicate (in and of themselves), as well as consulting, strategy, analysis, planning, specification, design, development, installation, implementation, integration, testing, debugging, updating, adaptation, maintenance, support, technical assistance, management or use of or for computer programmes;

(c) data processing, data storage, data hosting or database services;

(d) maintenance and repair services for office machinery and equipment, including computers; and

(e) training services for staff of clients, related to computer programmes, computers or computer systems, and not elsewhere classified.

2. For greater certainty, services enabled by computer and related services, other than those listed in paragraph 1, shall not be regarded as computer and related services in themselves.

TITLE IV

CAPITAL MOVEMENTS, PAYMENTS, TRANSFERS AND TEMPORARY SAFEGUARD MEASURES

ARTICLE 213

Objectives

The objective of this Title is to enable the free movement of capital and payments related to transactions liberalised under this Agreement.