CHAPTER 19

DIGITAL TRADE

Article 19.1: Definitions

For the purposes of this Chapter:

algorithm means a defined sequence of steps, taken to solve a problem or obtain a result;

computing facility means a computer server or storage device for processing or storing information for commercial use;

covered person means:

(a) a covered investment as defined in Article 1.5 (General Definitions);

(b) an investor of a Party as defined in Article 14.1 (Definitions); or

(c) a service supplier of a Party as defined in Article 15.1 (Definitions),

but does not include a covered person as defined in Article 17.1 (Definitions);

digital product means a computer program, text, video, image, sound recording, or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically. For greater certainty, digital product does not include a digitized representation of a financial instrument, including money; [1]

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 signature means data in electronic form that is in, affixed to, or logically associated with, an electronic document or message, and that may be used to identify the signatory in relation to the electronic document or message and indicate the signatory's approval of the information contained in the electronic document or message;

government information means non-proprietary information, including data, held by the central government;

information content provider means a person or entity that creates or develops, in whole or in

[1] This definition should not be understood to reflect a Party's view that digital products are a good or are a service.

part, information provided through the Internet or another interactive computer service;

interactive computer service means a system or service that provides or enables electronic access by multiple users to a computer server;

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

trade administration document means a form 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 communication means an electronic message, which is sent to an electronic address of a person for commercial or marketing purposes without the consent of the recipient or despite the explicit rejection of the recipient.[2]

Article 19.2: Scope and General Provisions

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

2. This Chapter applies to measures adopted or maintained by a Party that affect trade by electronic means.

3. This Chapter does not apply:

(a) to government procurement; or

(b) except for Article 19.18 (Open Government Data), to information held or processed by or on behalf of a Party, or measures related to that information, including measures related to its collection.

4. For greater certainty, a measure that affects the supply of a service delivered or performed electronically is subject to Chapter 14 (Investment), Chapter 15 (Cross-Border Trade in Services), and Chapter 17 (Financial Services), including any exception or non-conforming measure set out in this Agreement that is applicable to the obligations contained in those Chapters.

[2] For the United States, an unsolicited commercial electronic communication does not include an electronic message sent primarily for purposes other than commercial or marketing purposes.

Article 19.3: Customs Duties

1. No Party shall impose customs duties, fees, or other charges on or in connection with the importation or exportation of digital products transmitted electronically, between a person of one 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 a digital product transmitted electronically, provided that those taxes, fees, or charges are imposed in a manner consistent with this Agreement.

Article 19.4: Non-Discriminatory Treatment of Digital Products

1. No Party shall accord less favorable treatment to a digital product created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of another Party, or to a digital product of which the author, performer, producer, developer, or owner is a person of another Party, than it accords to other like digital products.[3]

2. This Article does not apply to a subsidy or grant provided by a Party, including a government-supported loan, guarantee, or insurance.

Article 19.5: Domestic Electronic Transactions Framework

1. Each Party shall maintain a legal framework governing electronic transactions consistent with the principles of the *UNCITRAL Model Law on Electronic Commerce 1996*.

2. Each Party shall endeavor to:

   (a) avoid unnecessary regulatory burden on electronic transactions; and

   (b) facilitate input by interested persons in the development of its legal framework for electronic transactions.

Article 19.6: Electronic Authentication and Electronic Signatures

1. Except in circumstances 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. No Party shall adopt or maintain measures for electronic authentication and electronic

[3] For greater certainty, to the extent that a digital product of a non-Party is a "like digital product," it will qualify as an "other like digital product" for the purposes of Article 19.4.1 (Non-Discriminatory Treatment of Digital Products).

signatures that would:

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

(b) prevent parties to an electronic transaction from having the opportunity to establish before judicial or administrative authorities that their transaction complies with any legal requirements with respect to authentication or electronic signatures.

3. Notwithstanding paragraph 2, a Party may require that, for a particular category of transactions, the electronic signature or method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its law.

4. Each Party shall encourage the use of interoperable electronic authentication.

Article 19.7: Online Consumer Protection

1. The Parties recognize the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent or deceptive commercial activities as referred to in Article 21.4.2 (Consumer Protection) when they engage in digital trade.

2. 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.

3. The Parties recognize the importance of, and public interest in, cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border digital trade in order to enhance consumer welfare. To this end, the Parties affirm that cooperation under paragraphs 21.4.3 through 21.4.5 (Consumer Protection) includes cooperation with respect to online commercial activities.

Article 19.8: Personal Information Protection

1. The Parties recognize the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade.

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 digital trade. In the development of this legal framework, each Party should take into account principles and guidelines of relevant international

bodies,[4] such as the *APEC Privacy Framework* and the *OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)*.

3. The Parties recognize that pursuant to paragraph 2, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. The Parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented.

4. Each Party shall endeavor to adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction.

5. Each Party shall publish information on the personal information protections it provides to users of digital trade, including how:

(a) a natural person can pursue a remedy; and

(b) an enterprise can comply with legal requirements.

6. Recognizing 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. The Parties shall endeavor to exchange information on the mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them. The Parties recognize that the *APEC Cross-Border Privacy Rules* system is a valid mechanism to facilitate cross-border information transfers while protecting personal information.

Article 19.9: Paperless Trading

Each Party shall endeavor to accept a trade administration document submitted electronically as the legal equivalent of the paper version of that document.

Article 19.10: Principles on Access to and Use of the Internet for Digital Trade

The Parties recognize that it is beneficial for consumers in their territories to be able to:

(a) access and use services and applications of a consumer's choice available on the

[4] For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as 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.

Internet, subject to reasonable network management;

(b) connect the end-user devices of a consumer's choice to the Internet, provided that such devices do not harm the network; and

(c) access information on the network management practices of a consumer's Internet access service supplier.

Article 19.11: Cross-Border Transfer of Information by Electronic Means

1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.

2. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.[5]

Article 19.12: Location of Computing Facilities

No 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.

Article 19.13: Unsolicited Commercial Electronic Communications

1. Each Party shall adopt or maintain measures providing for the limitation of unsolicited commercial electronic communications.

2. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic communications sent to an electronic mail address that:

[5] A measure does not meet the conditions of this paragraph if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party.

(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 in the laws and regulations of each Party, of recipients to receive commercial electronic messages.

3. Each Party shall endeavor to adopt or maintain measures that enable consumers to reduce or prevent unsolicited commercial electronic communications sent other than to an electronic mail address.

4. Each Party shall provide recourse in its law against suppliers of unsolicited commercial electronic communications that do not comply with a measure adopted or maintained pursuant to paragraph 2 or 3.

5. The Parties shall endeavor to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic communications.

Article 19.14: Cooperation

1. Recognizing the global nature of digital trade, the Parties shall endeavor to:

(a) exchange information and share experiences on regulations, policies, enforcement and compliance relating to digital trade, including:

(i) personal information protection, particularly with a view to strengthening existing international mechanisms for cooperation in enforcing laws protecting privacy,

(ii) security in electronic communications,

(iii) authentication, and

(iv) government use of digital tools and technologies to achieve better government performance;

(b) cooperate and maintain a dialogue on the promotion and development of mechanisms, including the *APEC Cross-Border Privacy Rules*, that further global interoperability of privacy regimes;

(c) actively participate in regional and multilateral fora to promote the development of digital trade;

(d) encourage development by the private sector of methods of self-regulation that

foster digital trade, including codes of conduct, model contracts, guidelines, and enforcement mechanisms;

(e) promote access for persons with disabilities to information and communications technologies; and

(f) promote, through international cross-border cooperation initiatives, the development of mechanisms to assist users in submitting cross-border complaints regarding personal information protection.

2. The Parties shall consider establishing a forum to address any of the issues listed above, or any other matter pertaining to the operation of this Chapter.

Article 19.15: Cybersecurity

1. The Parties recognize that threats to cybersecurity undermine confidence in digital trade. Accordingly, the Parties shall endeavor to:

(a) build the capabilities of their respective national entities responsible for cybersecurity incident response; and

(b) strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices.

2. Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.

Article 19.16: Source Code

1. No Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.

2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or

an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding,[6] subject to safeguards against unauthorized disclosure.

Article 19.17: Interactive Computer Services

1. The Parties recognize the importance of the promotion of interactive computer services, including for small and medium-sized enterprises, as vital to the growth of digital trade.

2. To that end, other than as provided in paragraph 4, no Party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information.[7]

3. No Party shall impose liability on a supplier or user of an interactive computer service on account of:

(a) any action voluntarily taken in good faith by the supplier or user to restrict access to or availability of material that is accessible or available through its supply or use of the interactive computer services and that the supplier or user considers to be harmful or objectionable; or

(b) any action taken to enable or make available the technical means that enable an information content provider or other persons to restrict access to material that it considers to be harmful or objectionable.

4. Nothing in this Article shall:

(a) apply to any measure of a Party pertaining to intellectual property, including measures addressing liability for intellectual property infringement; or

(b) be construed to enlarge or diminish a Party's ability to protect or enforce an intellectual property right; or

(c) be construed to prevent:

(i) a Party from enforcing any criminal law, or

[6] This disclosure shall not be construed to negatively affect the software source code's status as a trade secret, if such status is claimed by the trade secret owner.

[7] For greater certainty, a Party may comply with this Article through its laws, regulations, or application of existing legal doctrines as applied through judicial decisions.

(ii) a supplier or user of an interactive computer service from complying with a specific, lawful order of a law enforcement authority.[8]

5. This Article is subject to Annex 19-A.

Article 19.18: Open Government Data

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

2. To the extent that a Party chooses to make government information, including data, available to the public, it shall endeavor to ensure that the information is in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed.

3. The Parties shall endeavor to cooperate to identify ways in which each Party can expand access to and use of government information, including data, that the Party has made public, with a view to enhancing and generating business opportunities, especially for SMEs.

[8] The Parties understand that measures referenced in paragraph 4(c)(ii) shall be not inconsistent with paragraph 2 in situations where paragraph 2 is applicable.

ANNEX 19-A

1. Article 19.17 (Interactive Computer Services) shall not apply with respect to Mexico until the date of three years after entry into force of this Agreement.

2. The Parties understand that Articles 145 and 146 of Mexico's *Ley Federal de Telecomunicaciones y Radiodifusión*, as in force on the date of entry into force of this Agreement, are not inconsistent with Article 19.17.3 (Interactive Computer Services). In a dispute with respect to this article, subordinate measures adopted or maintained under the authority of and consistent with Articles 145 and 146 of Mexico's *Ley Federal de Telecomunicaciones y Radiodifusión* shall be presumed to be not inconsistent with Article 19.17.3 (Interactive Computer Services).

3. The Parties understand that Mexico will comply with the obligations in Article 19.17.3 (Interactive Computer Services) in a manner that is both effective and consistent with Mexico's Constitution (*Constitución Política de los Estados Unidos Mexicanos*), specifically Articles 6 and 7.

4. For greater certainty, Article 19.17 (Interactive Computer Services) is subject to Article 32.1 (General Exceptions), which, among other things, provides that, for purposes of Chapter 19, the exception for measures necessary to protect public morals pursuant to paragraph (a) of Article XIV of GATS is incorporated into and made part of this Agreement, *mutatis mutandis*. The Parties agree that measures necessary to protect against online sex trafficking, sexual exploitation of children, and prostitution, such as Public Law 115-164, the "Allow States and Victims to Fight Online Sex Trafficking Act of 2017," which amends the Communications Act of 1934, and any relevant provisions of *Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos delitos,* are measures necessary to protect public morals.