CHAPTER NINE
DIGITAL TRADE

Article 9.1: Definitions

For purposes of this Chapter:

commercial electronic message means an electronic message which is sent for commercial purposes to an electronic address of a person through a telecommunications service, comprising at least electronic mail and, to the extent provided for under a Party's domestic laws and regulations, other types of messages;

computing facilities means computer servers or storage devices for processing or storing information for commercial use;

covered person means a service supplier, as defined in Article 8.1 (Definitions), of the other Party;

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; [1, 2]

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

electronic payments means a payer's transfer of a monetary claim acceptable to a payee made through electronic means;

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

electronic transmission or **transmitted electronically** means a transmission made using any electromagnetic means, including by photonic means;

---

[1] For greater certainty, "digital product" does not include a digitized representation of a financial instrument, including money.

[2] The definition of "digital product" should not be understood to reflect a Party's view on whether trade in digital products through electronic transmission should be categorized as trade in services or trade in goods. 5

FinTech means the use of technology to improve and automate the delivery and use of financial services;

open data means digital data that is made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed. This definition relates only to information held or processed by or on behalf of a Party;

personal data means any information about an identified or identifiable natural person; and

unsolicited commercial electronic message means a commercial electronic message that is sent without the consent of the recipient or despite the explicit rejection of the recipient.

Article 9.2: 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 shall apply to measures adopted or maintained by a Party that affect trade by electronic means.

3. This Chapter shall not apply to:

   (a) government procurement; or

   (b) except for Article 9.16, 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, the Parties affirm that measures affecting the supply of a service delivered or performed electronically are subject to the obligations contained in the relevant provisions of Chapter Eight (Trade in Services) and its Annex 8-A, including any exceptions set out in this Agreement that are applicable to those obligations.

5. Articles 9.4, 9.8, and 9.9 shall not apply to aspects of a Party's measures that do not conform with an obligation in Chapter Eight (Trade in Services) to the extent that such measures are adopted or maintained in accordance with:

   (a) any terms, limitations, qualifications, and conditions specified in a Party's commitments, or are with respect to a sector that is not subject to a Party's commitments, made in accordance with

Article 8.7(Schedules of Specific Commitments); or

(b) any exception that is applicable to the obligations in Chapter Eight (Trade in Services).

Article 9.3: Customs Duties

1. Neither Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of the other Party.

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

Article 9.4: Non-Discriminatory Treatment of Digital Products

1. Neither Party shall accord less favorable treatment to digital products created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of the other Party, or to digital products of which the author, performer, producer, developer, or owner is a person of the other Party, than it accords to other like digital products.[3]

2. Paragraph 1 shall not apply to the extent of any inconsistency with the rights and obligations in Chapter Ten (Intellectual Property).

3. The Parties understand that this Article shall not apply to subsidies or grants provided by a Party, including government-supported loans, guarantees, and insurance.

4. This Article shall not apply to broadcasting.

Article 9.5: Domestic Electronic Transactions Framework

1. To the extent practicable, each Party shall endeavor 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 23 November 2005.

[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 purposes of this paragraph.

2. Each Party shall endeavor to:

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

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

Article 9.6: Electronic Authentication and Electronic Signatures

1. Except in circumstances otherwise provided for under its law, a Party shall not deny the legal validity of an electronic signature solely on the basis that the signature is in electronic form.

2. Neither Party shall adopt or maintain measures for electronic authentication that would:

(a) prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods 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.

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

4. The Parties shall encourage the use of interoperable electronic authentication.

Article 9.7: Electronic Payments

1. To facilitate the rapid growth of electronic payments, in particular those provided by non-bank, non-financial institution and FinTech enterprises, the Parties recognize the importance of developing an efficient, safe, and secure environment for cross-border electronic payments, including by:

(a) fostering the adoption and use of internationally accepted standards for electronic payments;

(b) promoting interoperability and the interlinking of electronic payment infrastructures; and

(c) encouraging innovation and competition in electronic payments services.

2. To this end, each Party shall:

(a) make regulations on electronic payments, including in relation to regulatory approval, authorization requirements, procedures and technical standards, publicly available;

(b) endeavor to finalize decisions on regulatory approval or authorization in a timely manner in accordance with its domestic laws and regulations.

(c) not arbitrarily or unjustifiably discriminate between financial institutions and non-financial institutions in relation to access to services and infrastructure necessary for the operation of electronic payment systems;

(d) adopt, for relevant electronic payment systems, international standards for electronic payment messaging, for electronic data exchange between financial institutions and services suppliers to enable greater interoperability between electronic payment systems;

(e) facilitate the use of open platforms and architectures such as tools and protocols provided for through Application Programming Interfaces ("APIs") and encourage payment service providers to safely and securely make APIs for their products and services available to third parties, where possible, to facilitate greater interoperability, innovation and competition in electronic payments; and

(f) facilitate innovation, competition, and introduction of new financial and electronic payment products and services in a

timely manner, such as through adopting regulatory and industry sandboxes.

3. In view of paragraph 1, the Parties recognize the importance of upholding safety, efficiency, trust, and security in electronic payment systems through regulations, and that the adoption and enforcement of regulations and policies should be proportionate to the risks undertaken by the payment service providers.

Article 9.8: Cross-Border Transfer of Information by Electronic Means[4]

1. The Parties recognize that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.

2. Neither Party shall prohibit or restrict the cross-border transfer of information by electronic means, including personal data, when this activity is for the conduct of the business of a covered person.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 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 required to achieve the objective.

Article 9.9: Location of Computing Facilities[5]

1. The Parties recognize that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.

2. Neither 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.

[4] This Article shall not apply to financial services.
[5] This Article shall not apply to financial services.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 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 the use or location of computing facilities greater than are required to achieve the objective.

Article 9.10: Source Code

1. Neither Party shall require the transfer of, or access to, source code of software owned by a person of the other Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory

2. This Article does not preclude a government agency, law enforcement agency, regulatory body or judicial authority ("Relevant Body") of a Party from requiring a person of the other Party to preserve or make available the source code of software, or an algorithm expressed in that source code, to the Relevant Body for an investigation, inspection, examination, enforcement action, or judicial or administrative proceeding, [6] subject to safeguards against unauthorized disclosure under the laws and regulations of the Party.

Article 9.11: Personal Data Protection

1. The Parties recognize the economic and social benefits of protecting the personal data 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 data of the users of digital trade. In the development of its legal framework for the protection of personal data, each Party shall take into account the principles and guidelines of relevant international bodies.[7]

[6] Such 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 the obligation in this paragraph by adopting or maintaining measures such as comprehensive privacy or personal data protection laws, sector-

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

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

(a) individuals can pursue remedies; and

(b) business can comply with any legal requirements pertaining to personal data protection.

Article 9.12: Unsolicited Commercial Electronic Messages

1. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages sent to an electronic address that:

(a) require a supplier of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages;

(b) require the consent, as specified in the laws and regulations of that Party, of recipients to receive commercial electronic messages; or

(c) otherwise provide for the minimization of unsolicited commercial electronic messages.

2. Each Party shall 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 endeavor to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

---

specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.

Article 9.13: Online Consumer Protection

1. The Parties recognize the importance of transparent and effective measures to protect consumers from fraudulent, misleading, or deceptive conduct when they engage in digital trade.

2. For purposes of this Article, "Fraudulent, misleading, or deceptive conduct" includes:

(a) making misrepresentations or false claims as to material qualities, price, suitability for purpose, quantity or origin of goods or services;

(b) advertising goods or services for supply without intention to supply;

(c) failing to deliver products or provide services to consumers after the consumers have been charged; or

(d) charging or debiting consumers' financial, telephone, or other accounts without authorization.

3. The Parties recognize the importance of adoption or maintenance of laws or regulations to proscribe fraudulent, misleading, or deceptive conduct that causes harm or is likely to cause harm to consumers engaged in online commercial activities.

4. The Parties recognize the importance of 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.

5. The Parties shall promote, as appropriate and subject to the respective laws and regulations of each Party, cooperation on matters of mutual interest related to fraudulent, misleading, or deceptive conduct, including in the enforcement of their consumer protection laws, with respect to online commercial activities.

6. The Parties recognize the benefits of mechanisms, including alternative dispute resolution, to facilitate the resolution of claims over electronic commerce transactions.

Article 9.14: Cybersecurity Cooperation

1. The Parties have a shared vision to promote secure digital trade to achieve global prosperity and recognize that cybersecurity underpins the digital economy.

2. The Parties further recognize the importance of facilitating the following activities:

(a) building the capabilities of their national entities responsible for computer security incident response;

(b) using existing collaboration mechanisms to cooperate to identify and mitigate computer security incidents among other malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties;

(c) preemptive sharing of information and actionable intelligence on cyber threats through existing collaboration mechanisms on potential threats affecting the electronic networks of the Parties;

(d) creating or engaging in bilateral or multilateral mechanism, if necessary, to jointly mitigate and investigate computer security incidents affecting the electronic networks of the Parties;

(e) exchanging experience and expertise on the detection and handling of computer security incidents, including the collection, processing, and further analysis of issues related to cyber threat intelligence, in the form of training, workshops, seminars, study visits or other capacity building activities;

(f) committing to cooperate in the exchange of information on the capabilities of relevant cybersecurity agencies; and

(g) expanding cooperation beyond incident response to include sharing knowledge and experience on how to communicate with businesses and raise awareness to improve cyber resilience, and sharing best practices to increase cyber security awareness among members of the digital society.

Article 9.15: Principles on Access to and Use of the Internet for Digital Trade

Subject to their respective applicable policies, laws, and regulations, the Parties recognize the benefits of consumers in their territories having the ability to:

(a) access and use services and applications of a consumer's choice available on the Internet, subject to reasonable network management;[8]

(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 9.16: Open Data

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

2. To the extent that a Party makes government information, including data, available to the public, it shall endeavor to ensure that the information is made available as open data.

3. The Parties shall endeavor to cooperate to identify ways in which the Parties can expand access to and use of open data, with a view to enhancing and generating business opportunities.

[8] The Parties recognize that an Internet access service supplier that offers its subscribers certain content on an exclusive basis would not be acting contrary to this principle.

Article 9.17: Cooperation on Competition

1. Recognizing that the Parties can benefit by sharing their experiences in enforcing competition law and in developing and implementing competition policies to address the additional challenges that arise from the digital economy, the Parties shall endeavor to:

(a) exchange information and share best practices on the competition policies and effective competition law enforcement activities to promote and protect a competitive environment in digital markets; and

(b) facilitate that the Parties' digital markets are open, contestable, and efficient.

2. The Parties shall cooperate, as appropriate, on issues of competition law enforcement in digital markets, including through consultation and exchange of information.

Article 9.18: FinTech Cooperation

The Parties shall promote cooperation between the FinTech industries of the Parties. The Parties recognize that effective cooperation regarding FinTech will require involvement of businesses. To this end, the Parties shall:

(a) promote development of FinTech solutions for business or financial sectors; and

(b) encourage collaboration of entrepreneurship or startup talent in FinTech between the Parties, consistent with the laws and regulations of the respective Parties.

Article 9.19: Cooperation

The Parties shall endeavor to:

(a) exchange information and share experiences on regulations, policies, and enforcement and compliance mechanisms regarding digital trade, including in relation to:

(i) personal data protection;

(ii) online consumer protection;

(iii) unsolicited commercial electronic messages;

(iv) security in electronic communications;

(v) electronic authentication; and

(vi) any other area mutually agreed by the Parties.

(b) exchange information and share views on consumer access to products and services offered online between the Parties;

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

(d) encourage development by industry of methods of self-regulation that foster digital trade, including codes of conduct, model contracts, guidelines, and enforcement mechanisms.