CHAPTER 9
DIGITAL TRADE

Article 9.1: Definitions

For the purposes of this Chapter:

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

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

covered enterprise means an enterprise of a Party that is owned or controlled, directly or indirectly, by a person of either Party;

covered person means a covered enterprise or a natural person of either Party;

digital product means a computer programme, 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 invoicing means the automated creation, exchange and processing of request for payments between suppliers and buyers using a structured digital format;

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

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

electronic version of a document means a document in an electronic format prescribed by a Party;

[1] For greater certainty, "digital product" does not include a digitised 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 categorised as trade in services or trade in goods.

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

open data means non-proprietary information, including data, made freely available to the public by the central level of government;

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

trade administration documents means forms 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 message means an electronic message which is sent for commercial or marketing purposes to an electronic address, without the consent of the recipient or despite the explicit rejection of the recipient, through an Internet access service supplier or, to the extent provided for under the laws and regulations of each Party, other telecommunications service.

Article 9.2: Objectives

1. The Parties recognise the economic growth and opportunity that digital trade provides, the importance of avoiding barriers to its use and development, the importance of frameworks that promote consumer confidence in digital trade, and the applicability of the WTO Agreement to measures affecting digital trade.

2. To that end, the objectives of this Chapter are to:

(a) support the growth of new areas of economic activity between the Parties, including digital cooperation;

(b) expand the scope of cooperation between the Parties on matters concerning the digital economy;

(c) promote emerging technologies to deepen the Parties' economic relationship, and

(d) facilitate greater business-to-business and research links between the Parties.

3. The Parties seek to foster an environment conducive to the further advancement of digital trade, including electronic commerce and the digital transformation of the global economy, by strengthening their bilateral relations on these matters.

Article 9.3: Scope

1. This Chapter shall apply to measures adopted or maintained by a Party that affect trade by electronic means or that, by electronic means, facilitate trade.

2. This Chapter shall not apply to:

(a) government procurement, or

(b) information held or processed by or on behalf of a Party or measures related to such information, including measures related to its collection.

3. Measures affecting the supply of a service delivered or performed electronically are subject to the obligations contained in the relevant provisions of Chapter 8 (Trade in Services).

Article 9.4: Paperless Trading

1. Each Party shall endeavour to make publicly available, which may include through a process prescribed by that Party, electronic versions of all existing publicly available trade administration documents.[3]

2. Each Party shall endeavour to make available electronic versions of trade administration documents referred to in paragraph 1 in English or any of the other official languages of the WTO, and shall endeavour to provide such electronic versions in a machine readable format.

3. Each Party shall accept electronic versions of trade administration documents as the legal equivalent of paper documents, except where:

(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.

4. Noting the obligations in the WTO Agreement on Trade Facilitation, each Party shall establish or maintain a single window, enabling traders to submit documentation or data requirements for importation, exportation, or transit of goods through a single-entry point to the participating authorities or agencies.

[3] For greater certainty, electronic version of trade administration documents includes trade administration documents provided in a machine-readable format.

5. The Parties shall endeavour to establish or maintain a seamless, trusted, high-availability[4] and secure interconnection of each Party's single window to facilitate the exchange of data relating to trade administration documents, which may include:

(a) sanitary and phytosanitary certificates;

(b) import and export data, and

(c) any other documents, as jointly determined by the Parties.[5]

6. The Parties recognise the importance of facilitating, where relevant in each jurisdiction, the exchange of electronic records used in commercial trading activities between the Parties' businesses.

7. The Parties shall endeavour to develop data exchange systems to support the exchange of:

(a) data relating to trade administration documents referred to in paragraph 5 between the competent authorities of each Party,[6] and

(b) electronic records used in commercial trading activities between the Parties' businesses, where relevant in each jurisdiction.

8. The Parties recognise that the data exchange systems referred to in paragraph 7 should be compatible and interoperable with each other. To this end, the Parties recognise the role of internationally recognised and, if available, open standards in the development and governance of the data exchange systems.

9. The Parties shall cooperate and collaborate on new initiatives which promote and advance the use and adoption of the data exchange systems referred to in paragraph 7, including, but not limited to, through:

(a) sharing of information and experiences, including the exchange of best practices, in the area of development and governance of the data exchange systems, and
(b) collaboration on pilot projects in the development and governance of data exchange systems.

[4] High availability refers to the ability of a single window to continuously operate. It does not prescribe a specific standard of availability.
[5] The Parties shall provide public access to the list of documents referred to in subparagraph (c) and make this information available online.
[6] The Parties recognise that the data exchange systems referred to in paragraph 7 may refer to the single window referred to in paragraph 5.

10. The Parties shall cooperate bilaterally and in international forums to enhance acceptance of electronic versions of trade administration documents and electronic records used in commercial trading activities between businesses.

11. In developing other initiatives which provide for the use of paperless trading, each Party shall endeavour to take into account the methods agreed by international organisations.

Article 9.5: Electronic Invoicing

1. The Parties recognise the importance of electronic invoicing, which increases the efficiency, accuracy and reliability of commercial transactions. Each Party also recognises the benefits of ensuring that the systems used for electronic invoicing within their jurisdictions are interoperable with the systems used for electronic invoicing in the other Party's jurisdiction.

2. Each Party shall endeavour to ensure that the implementation of measures related to electronic invoicing in its jurisdiction is designed to support cross-border interoperability. For that purpose, each Party shall endeavour to base its measures relating to electronic invoicing on international standards, guidelines or recommendations, where they exist.

3. The Parties recognise the economic importance of promoting the global adoption of interoperable electronic invoicing systems. To this end, the Parties shall share best practices and collaborate on promoting the adoption of interoperable systems for e-invoicing.

4. The Parties agree to cooperate and collaborate on initiatives which promote, encourage, support or facilitate the adoption of e-invoicing by businesses. 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 9.6: Digital Authentication and Digital Signatures

1. Except in circumstances otherwise provided for under its laws and regulations, a Party shall not deny the legal validity of a signature solely on the basis that the signature is in digital or 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 laws and regulations.

4. The Parties shall encourage the use of interoperable electronic authentication. To this end, the Parties may establish homologation mechanisms and criteria regarding electronic authentication, observing international standards. For this purpose, the Parties may consider the recognition of electronic signature certificates issued by certification service providers operating in their territories in accordance with the procedure determined by their laws and regulations, in order to safeguard security and integrity standards.

Article 9.7: Customs Duties

1. Neither Party shall impose customs duties on digital or 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 digitally or electronically, provided that such taxes, fees or charges are imposed in a manner consistent with this Agreement.

Article 9.8: Non-Discriminatory Treatment of Digital Products

1. Neither Party shall accord less favourable treatment to a digital product created, produced, published, contracted for, commissioned or first made available on commercial terms in the territory of the other Party, or to a digital product of which the author, performer, producer, developer or owner is a person of the other Party, than it accords to other like digital products.[7]

[7] 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 this paragraph.

2. Paragraph 1 is without prejudice to the rights and obligations of the Parties concerning intellectual property under any international agreement to which they are parties or under Chapter 11 (Intellectual Property).

3. 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 9.9: Online Consumer Protection

1. The Parties recognise the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent and deceptive commercial activities, unfair contract terms, and unconscionable conduct, when they engage in electronic commerce.

2. For the purposes of this Article, fraudulent and deceptive commercial activities refer to those commercial practices that can cause actual harm to consumers or pose a potential threat if such harm is not prevented. For example:

(a) making a misrepresentation of material fact, including an implied factual misrepresentation, that may cause significant detriment to the economic interests of a misled consumer;

(b) intentionally failing to deliver products or provide services to a consumer after the consumer is charged, or

(c) charging or debiting a consumer's financial, digital or other accounts without authorisation.

3. 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.

4. The Parties recognise the importance of cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border electronic commerce in order to enhance consumer welfare. To this end, the Parties shall promote, as appropriate and subject to the laws and regulations of each Party, cooperation on matters of mutual interest, including exchanges of best practices regarding vulnerable consumers and mechanisms of enforcement of their consumer protection laws, with respect to online commercial activities.

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

Article 9.10: 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 each Party, of recipients to receive commercial electronic messages, or

(c) otherwise provide for the minimisation 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 endeavour to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

Article 9.11: Information and Communication Technology Products that Use Cryptography

1. For the purposes of this Article:

cryptographic algorithm or **cipher** means a mathematical procedure or formula for combining a key with plaintext to create a ciphertext;

cryptography means the principles, means or methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorised use; and is limited to the transformation of information using one or more secret parameters, for example, crypto variables, or associated key management;

encryption means the conversion of data (plaintext) into a form that cannot be easily understood without subsequent re-conversion (ciphertext) through the use of a cryptographic algorithm, and

key means a parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot.

2. This Article shall apply to information and communication technology products that use cryptography.[8]

3. With respect to a product that uses cryptography and is designed for commercial applications, neither Party shall impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of the product, as a condition of the manufacture, sale, distribution, import or use of the product, to:

(a) transfer or provide access to a particular technology, production process or other information, for example, a private key or other secret parameter, algorithm specification or other design detail, that is proprietary to the manufacturer or supplier and relates to the cryptography in the product, to the Party or a person in the Party's territory;

(b) partner with a person in its territory, or

(c) use or integrate a particular cryptographic algorithm or cipher, other than where the manufacture, sale, distribution, import or use of the product is by or for the government of the Party.

4. Paragraph 3 shall not apply to:

(a) requirements that a Party adopts or maintains relating to access to networks that are owned or controlled by the government of that Party, including critical infrastructure and central banks, or

(b) measures taken by a Party pursuant to supervisory, investigatory or examination authority relating to financial institutions or markets.

5. For greater certainty, this Article shall not be construed to prevent a Party's law enforcement and regulatory authorities from requiring service suppliers using encryption they control to provide, in accordance with that Party's legal procedures, unencrypted communications.

[8] For greater certainty, for the purposes of this Article, a "product" is a good, digital product or a service and does not include a financial instrument.

Article 9.12: Principles on Access to and Use of the Internet for Electronic Commerce

Subject to their laws and regulations, and policies, the Parties recognise 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;[9]

(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 9.13: Personal Data Protection

1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.

2. Each Party shall adopt or maintain a legal framework that provides for the protection of the personal data of the users of electronic commerce. In the development of its legal framework for the protection of personal data, each Party should take into account principles and guidelines of relevant international bodies.[10]

3. The Parties recognise that the principles underpinning a robust personal data protection framework should include:

(a) collection limitation;

(b) data quality;

(c) purpose specification;

(d) use limitation;

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

[10] For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.

(e) security safeguards;

(f) transparency;

(g) individual participation, and

(h) accountability.

4. Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal data protection violations occurring within its jurisdiction.

5. Each Party shall endeavour to publish information on the personal data protections it provides to users of electronic commerce, including how:

(a) individuals can pursue remedies, and

(b) business can comply with any legal requirements.

6. Recognising that the Parties may take different legal approaches to protecting personal data, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them.

Article 9.14: Cross-Border Transfer of Information by Electronic Means

1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means, provided the requirements are not arbitrary or a disguised restriction on trade, and are proportionate.

2. Neither Party shall prohibit or restrict the cross-border transfer of information by electronic means, including personal information, if this activity is for the conduct of 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 9.15: Location of Computing Facilities

1. The Parties recognise 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.

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 9.16: Open Government Data

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

2. To the extent that a Party chooses to make government information available to the public, it shall endeavour to ensure that:

(a) the information is appropriately anonymised, contains descriptive metadata, and is in a machine readable and open format that allows it to be searched, retrieved, used, reused, and redistributed, and

(b) to the extent practicable, the information is made available in a spatially enabled format with reliable, easy to use, and freely available APIs and is regularly updated.

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

Article 9.17: Source Code

1. Neither Party shall 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 such software, or of products containing such software, in its territory.

2. For the purposes of this Article, software subject to paragraph 1 does not include software used for critical infrastructure.

3. Nothing in this Article shall preclude:

(a) the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts, or

(b) a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement.

4. This Article shall not be construed to affect requirements that relate to patent applications or granted patents, including any orders made by a judicial authority in relation to patent disputes, subject to safeguards against unauthorised disclosure under the law or practice of a Party.

Article 9.18: Artificial Intelligence

1. The Parties recognise that the use and adoption of Artificial Intelligence ("AI") technologies are becoming increasingly important to digital trade, offering significant social and economic benefits to natural persons and enterprises.

2. The Parties also recognise the importance of developing ethical governance frameworks for the trusted, safe, and responsible use of AI technologies that will help realise the benefits of AI. In view of the cross-border nature of digital trade, the Parties further acknowledge the benefits of ensuring that such frameworks are internationally aligned as far as possible.

3. To this end, the Parties shall endeavour to:

(a) collaborate on and promote the development and adoption of ethical governance frameworks that support the trusted, safe, and responsible use of AI technologies ("AI Governance Frameworks"), through relevant regional and international fora;

(b) take into consideration internationally recognised principles or guidelines when developing such AI Governance Frameworks, and

(c) cooperate through promoting dialogue and sharing experiences on regulations, policies and initiatives relating to the use and adoption of AI technologies.

Article 9.19: Cybersecurity Cooperation

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

3. The Parties further recognise the importance of:

(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 malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties, and

(c) workforce development in the area of cybersecurity, including possible initiatives relating to mutual recognition of qualifications, diversity, and equality.

3. The Parties shall endeavour to cooperate to advance collaborative solutions to global issues affecting online safety and security.

Article 9.20: Domestic Electronic Transactions Framework

1. Each Party shall endeavour 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.

2. Each Party shall endeavour to avoid any unnecessary regulatory burden on electronic transactions, and facilitate input by interested persons in the development of its legal framework for electronic transactions, including in relation to trade documentation.

Article 9.21 Electronic Payments

1. Recognising the rapid growth of digital and electronic payments, the Parties shall endeavour to support the development of efficient, safe, and secure cross-border electronic payments by:

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

(b) promoting interoperability and the interlinking of payment infrastructures, and

(c) encouraging useful innovation and competition in the payment ecosystem/industry.

2. To this end, and in accordance with their respective laws and regulations, each Party recognises the following principles:

(a) the Parties shall endeavour to make their respective regulations on electronic payments, including those pertaining to regulatory approval, licensing requirements, procedures and technical standards, publicly available in a timely manner;

(b) the Parties shall endeavour to take into account, for relevant payment systems, internationally accepted payment standards to enable greater interoperability between payment systems;

(c) the Parties shall endeavour to enable cross-border authentication and electronic know-your-customer of individuals and businesses using digital identities, and

(d) the Parties recognise the importance of upholding safety, efficiency, trust, and security in electronic payment systems through regulation. The implementation of regulation should, where appropriate, be proportionate to and commensurate with the risks posed by the provision of electronic payment systems.

Article 9.22: Digital Identities

Recognising that cooperation between the Parties on digital identities for natural persons and enterprises will promote connectivity and further growth of digital trade and recognising that each Party may take different legal and technical approaches to digital identities, the Parties shall endeavour to pursue mechanisms to promote compatibility between their respective digital identity regimes. This may include:

(a) developing appropriate frameworks and common standards to foster technical interoperability between each Party's implementation of digital identities;

(b) developing comparable protection of digital identities under each Party's respective laws and regulations, or the recognition of their legal effects, whether accorded autonomously or by agreement;

(c) supporting the development of international frameworks on digital identity regimes, and

(d) exchanging knowledge and expertise on best practices relating to digital identity policies, laws and regulations, technical implementation and security standards, and the promotion of the use of digital identities.

Article 9.23: Cooperation

1. Recognising the importance of digital trade to their collective economies, the Parties shall endeavour to maintain a framework that addresses threats to cybersecurity that undermine confidence in digital trade. Accordingly, the Parties recognise the importance of:

(a) building the capabilities of their government agencies responsible for computer security incident response;

(b) using existing collaboration mechanisms to cooperate to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties, and

(c) promoting the development of a strong public and private workforce in the area of cybersecurity, including possible initiatives relating to mutual recognition of qualifications.

2. The areas of cooperation can include, among others:

(a) competition in digital economy;

(b) data innovation, and

(c) small and medium enterprises and startups.