CHAPTER 14

DIGITAL TRADE

Article 14.1
Definitions

For the purposes of this Chapter:

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

"commercial information and communication technology product" (commercial ICT product) means a product that is designed for commercial applications and whose intended function is information processing and communication by electronic means, including transmission and display, or electronic processing applied to determine or record physical phenomena, or to control physical processes;

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

"covered person" means:

(a) a covered investment as defined in Article 1.4 (General Definitions – Initial Provisions and General Definitions);

(b) an investor of a Party as defined in Article 13.1 (Definitions – Investment); or

(c) a service supplier of a Party as defined in Article 8.1 (Definitions – Cross-Border Trade in Services),

but does not include a financial service supplier as defined in Article 9.1 (Definitions – Financial Services);

"cryptography" means the principles, means or methods for the transformation of data in order to conceal or disguise its 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;

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

(a) the electronic identification of a person; or

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

"electronic invoicing" means the automated creation, exchange, and processing of requests for payments between suppliers and buyers using a structured digital format;

"electronic signature" means data in electronic form that is in, affixed to, or logically associated with, an electronic data message 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;[1]

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

"electronic trust service" means an electronic service which may include:

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

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

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

"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 the appropriate cryptographic key;

"enterprise" means an enterprise as defined in Article 1.4 (General Definitions – Initial Provisions and General Definitions) and a branch of an enterprise;

"key" means a parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that a person with knowledge of the key can reproduce or reverse the operation, but a person without knowledge of the key cannot;

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

[1] For greater certainty, nothing in this provision prevents a Party from according greater legal effect to an electronic signature that satisfies certain requirements, such as indicating that the electronic data message has not been altered or verifying the identity of the signatory.

"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[2] 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, via a public telecommunications service.[3]

Article 14.2
Scope and General Provisions

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

2. This Chapter does not apply to:

   (a) audio-visual services; or

   (b) government procurement, except for Article 14.5 (Conclusion of Contracts by Electronic Means) and 14.6 (Electronic Authentication and Electronic Trust Services).

3. Article 14.10 (Cross-Border Transfer of Information by Electronic Means) and Article 14.11 (Location of Computing Facilities) do not apply to a measure to the extent that the measure is not subject to an obligation in Chapter 8 (Cross-Border Trade in Services) or Chapter 13 (Investment) by reason of:

   (a) Article 8.7 (Non-Conforming Measures – Cross-Border Trade in Services) or Article 13.13 (Non-Conforming Measures – Investment); or

   (b) any exception that is applicable to that obligation.

4. Article 14.10 (Cross-Border Transfer of Information by Electronic Means), Article 14.11 (Location of Computing Facilities), Article 14.18 (Source Code), and Article 14.19 (Commercial Information and Communication Technology Products that Use Cryptography) shall not apply to information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection.

---

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

[3] For Australia, an unsolicited commercial electronic message does not include a commercial electronic message that is a designated commercial electronic message under the *Spam Act 2003* (Cth), as amended from time to time, or any successor legislation.

Article 14.3
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 does not preclude a Party from imposing internal taxes, fees or other charges on electronic transmissions, including content transmitted electronically, provided that those taxes, fees or charges are imposed in a manner consistent with this Agreement.

Article 14.4
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* done at New York on 12 June 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:

   (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.

3. The Parties recognise the importance of developing mechanisms to facilitate the use of electronic transferable records. To this end, in developing such mechanisms, the Parties shall endeavour to take into account, as appropriate, relevant model legislative texts developed and adopted by international bodies, such as the *UNCITRAL Model Law on Electronic Transferable Records 2017* done at New York on 13 July 2017.

Article 14.5
Conclusion of Contracts by Electronic Means

1. Except in circumstances otherwise provided for in its law, each Party shall ensure that:

   (a) its legal framework allows for contracts to be concluded by electronic means; and

(b) its law neither creates obstacles for the use of electronic contracts nor results in electronic contracts being deprived of legal effect, enforceability, or validity, solely on the ground that the contract has been made by electronic means.

2. The Parties recognise the importance of transparency for minimising barriers to the use of electronic contracts in digital trade. To that end, each Party shall:

(a) promptly publish the circumstances referred to in paragraph 1 on a single official website hosted by the central level of government; and

(b) review these circumstances with a view to reducing them over time.

Article 14.6
Electronic Authentication and Electronic Trust Services

1. Except in circumstances otherwise provided for under its law, neither Party shall deny the legal validity or effect, or admissibility as evidence in legal proceedings, of an electronic document or an electronic signature solely on the ground that it is in electronic form.

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

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

(b) prevent parties to an electronic transaction from being able to prove to judicial or administrative authorities that the use of electronic authentication 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 is certified by an authority accredited in accordance with its law or meets certain performance standards which shall be objective, transparent, and non-discriminatory and shall only relate to the specific characteristics of the category of transactions concerned.

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

5. To the extent provided for in its law, a Party shall apply paragraphs 1 through 4 to other electronic processes or means of facilitating or enabling electronic transactions, such as electronic seals, electronic time stamps, electronic registered delivery services, or electronic trust services.

Article 14.7
Digital Identities

1. Recognising that cooperation between the Parties on digital identities will increase regional and global connectivity, and recognising that each Party may take different legal and technical approaches to digital identities, the Parties shall pursue the development of mechanisms to promote compatibility between their respective digital identity regimes.

2. To this end, the Parties shall endeavour to facilitate initiatives to promote such compatibility, which may include:

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

   (b) supporting the development of international frameworks on digital identity regimes;

   (c) implementing use cases for the mutual recognition of digital identities; and

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

Article 14.8
Paperless Trading

1. Each Party shall endeavour to:

   (a) make trade administration documents available to the public in electronic form; and

   (b) accept a trade administration document submitted electronically as the legal equivalent of the paper version of that document.

2. The Parties shall cooperate bilaterally and in international fora, where appropriate, to promote acceptance of electronic versions of trade administration documents and on other matters related to paperless trading.

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

Article 14.9
Electronic Invoicing

1. The Parties recognise the importance of electronic invoicing to increase the efficiency, accuracy, and reliability of commercial transactions. Each Party also recognises the benefits of ensuring that the systems used for electronic invoicing within its territory are interoperable with the systems used for electronic invoicing in the other Party's territory.

2. Each Party shall endeavour to ensure that the implementation of measures related to electronic invoicing in its territory supports cross-border interoperability between the Parties' electronic invoicing frameworks. To this end, the Parties shall take into account international frameworks when developing measures related to electronic invoicing.

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

Article 14.10
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.

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 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 14.11
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 14.12
Personal Information Protection

1. The Parties recognise 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 its legal framework for the protection of personal information, each Party shall take into account principles and guidelines of relevant international bodies, including collection limitation, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation, and accountability.[4]

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

4. 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 any legal requirements.

[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 data protection or privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to data protection or privacy.

5. Each Party shall encourage enterprises in its territory to publish, including on the Internet, their policies and procedures related to protection of personal information.

6. Recognising that the Parties may take different legal approaches to protecting personal information, each Party shall 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 14.13
Open Government Data

1. For the purposes of this Article, government information means non-proprietary information, including data, held by the central level of government.

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

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

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

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

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

Article 14.14
Data Innovation

1. The Parties recognise that digitalisation and the use of data in digital trade promote economic growth. To support the cross-border transfer of information by electronic means and promote data-driven innovation in digital trade, the Parties further recognise the need to create an environment that enables and supports, and is conducive to, experimentation and innovation, including through the use of regulatory sandboxes where applicable.

2. The Parties shall endeavour to support data innovation through:

   (a) collaborating on data-sharing projects, including projects involving researchers, academics and industry, using regulatory sandboxes as required to demonstrate the benefits of the cross-border transfer of information by electronic means;

   (b) cooperating on the development of policies and standards for data mobility, including consumer data portability; and

   (c) sharing research and industry practices related to data innovation.

Article 14.15
Open Internet Access

Subject to their applicable policies, laws, and regulations, the Parties recognise the benefits of consumers[5] in their territories having the ability to:

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

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

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

Article 14.16
Online Consumer Protection

1. The Parties recognise the importance of transparent and effective measures that enhance consumer confidence and trust in digital trade.

[5] For the purposes of this Article, "consumer" means any natural or juridical person using the internet for personal, trade, business, or professional purposes.

2. Each Party shall maintain consumer protection laws and regulations that proscribe:

   (a) misleading, deceptive, and fraudulent commercial practices; and

   (b) unconscionable conduct or unfair commercial practices,

   that cause harm, or potential harm, to consumers engaged in digital trade.[6]

3. The Parties recognise the importance of, and where appropriate shall promote, cooperation between their respective national consumer protection agencies or other relevant bodies on activities aimed at online consumer protection.[7]

4. The Parties further recognise the importance of improving awareness of and providing access to consumer redress mechanisms to protect consumers engaged in digital trade, including for consumers of a Party transacting with suppliers of the other Party.

5. The Parties recognise the benefits of dispute resolution mechanisms in facilitating the resolution of disputes regarding electronic commerce transactions, including alternative dispute resolution mechanisms.

Article 14.17
Unsolicited Commercial Electronic Messages

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

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

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

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

2. Each Party shall ensure that commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are made, and

[6] For the purposes of this Article, the term "engaged" includes the pre-transaction phase of online commercial activities.

[7] To this end, the Parties affirm that cooperation under Article 17.6 (Cooperation on Competition Policy and Consumer Protection – Competition Policy and Consumer Protection) includes cooperation with respect to online commercial activities.

contain the necessary information to enable recipients to request cessation free of charge and at any time.

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

4. The Parties shall endeavour to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

Article 14.18
Source Code

1. Neither Party shall require the transfer of, or access to, source code[8] of software owned by a person of the other Party, as a condition for the import, distribution, sale, or use of that software, or of a product containing that software, in its territory.

2. This Article does not preclude a government agency, regulatory body, administrative tribunal, or judicial authority of a Party, or a designated conformity assessment body operating in the Party's territory, from requiring a person of the other Party to preserve and make available[9] the source code of software for an investigation, inspection, examination, enforcement action, or judicial or administrative proceeding, subject to safeguards against unauthorised disclosure.

3. Paragraph 1 does not apply to a remedy imposed, enforced, or adopted in accordance with a Party's law following an investigation, inspection, examination, enforcement action, or judicial or administrative proceeding.

4. Paragraph 1 does not apply to the voluntary transfer of, or granting of access to, source code by a person of the other Party on a commercial basis, such as in the context of a freely negotiated contract.

5. For greater certainty, nothing in paragraph 1 shall prevent a person of a Party from licensing its software on a free and open-source basis.

[8] For greater certainty, for the purposes of this Article, a reference to "source code" includes an algorithm embedded in the source code, but does not include the expression of the algorithm in any other form, including in prose.

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

Article 14.19
Commercial Information and Communication Technology Products that Use Cryptography

1. Neither Party shall impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of a commercial information and communication technology (ICT) product that uses cryptography,[10] as a condition of the manufacture, sale, distribution, import, or use of the ICT product,[11] 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;[12]

   (b) partner or otherwise cooperate with a person in the Party's territory in the development, manufacture, sale, distribution, import, or use of the ICT product; or

   (c) use or integrate a particular cipher or cryptographic algorithm.

2. This Article does not apply to:

   (a) a requirement that a Party adopts or maintains relating to access to networks, including user devices, that are owned or controlled by that Party, including those of central banks;

   (b) measures by a Party adopted or maintained pursuant to supervisory, investigatory, or examination authority relating to financial service suppliers or financial markets; or

   (c) the manufacture, sale, distribution, import, or use of the commercial ICT product by or for a Party.

3. For greater certainty, this Article shall not be construed to prevent a Party's law enforcement authorities from requiring service suppliers using encryption they control to provide, pursuant to that Party's legal procedures, access to encrypted and unencrypted communications.

---

[10] For the purposes of this Article, a "commercial ICT product" is a good and, for greater certainty, does not include a financial instrument.

[11] For greater certainty, for the purposes of this Article, measures of a Party affecting trade enabled or facilitated by electronic means includes measures relating to the development, manufacture, sale, distribution, import, or use of ICT products.

[12] For greater certainty, this Article does not affect the rights and obligations of a Party under Article 14.18 (Source Code).

Article 14. 20
Cybersecurity

1. The Parties recognise that threats to cybersecurity undermine confidence in digital trade. The Parties further recognise the importance of:

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

   (b) enhancing the cybersecurity capability of businesses, including SMEs, and enabling greater cybersecurity resilience within industry.

2. The Parties shall endeavour to:

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

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

   (c) maintain a dialogue on matters related to cybersecurity, including for the sharing of information and experiences for awareness and best practices.

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

Article 14.21
Cooperation

1. Recognising the global nature of digital trade, the Parties shall endeavour to:

   (a) work together to address challenges for SMEs in the use of digital trade;

(b) exchange information and share experiences and best practices on laws, regulations, policies, enforcement, and compliance regarding digital trade, including:

(i) personal information protection;

(ii) online consumer protection;

(iii) unsolicited commercial electronic messages;

(iv) cybersecurity;

(v) electronic authentication and electronic trust services;

(vi) digital government; and

(vii) electronic contracts;

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

(d) participate actively in multilateral fora, including the WTO, to promote the development of international frameworks for digital trade, including in relation to the development and adoption of relevant international standards;

(e) work together in areas of mutual interest relating to the development and application of standards and conformity assessment procedures with a view to facilitating digital trade;

(f) encourage development by the private sector of methods of self-regulation that foster digital trade, including codes of conduct, model contracts, guidelines, and compliance mechanisms;

(g) collaborate to improve opportunities for each Party's RegTech enterprises, including through their respective trade promotion agencies and regulators, and in relevant international fora; and

(h) facilitate participation by women in digital trade, acknowledging the objectives in Chapter 24 (Trade and Gender Equality).