**CHAPTER 12**

**DIGITAL TRADE**

**Article 12.1**
**Definitions**

For purposes of this Chapter:

**administrative ruling of general application** means an administrative ruling or interpretation that applies to all persons and fact situations that fall generally within the ambit of that administrative ruling or interpretation and that establishes a norm of conduct, but does not include:

 (a) a determination or ruling made in an administrative or quasi-judicial proceeding that applies to a particular person, good or service of the other Party in a specific case; or

(b) a ruling that adjudicates with respect to a particular act or practice;

**computing facilities** means computer servers and storage devices for processing or storing information for commercial use but does not include computer servers or storage devices of or used to access financial market infrastructures;

**covered person** means a service supplier of a Party as defined in Article 9.1 (Definitions – Trade in Services);

**customs duty** includes any duty or charge of any kind imposed on or in connection with the importation of a good, and any surtax or surcharge imposed in connection with such importation, but does not include any:

(a) charge equivalent to an internal tax imposed consistently with paragraph 2 of Article III of the GATT 1994;

(b) fee or other charge in connection with the importation commensurate with the cost of services rendered; or

(c) antidumping or countervailing duty;

**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 invoicing** means the automated creation, exchange and processing of a request for payment between a supplier and a buyer using a structured digital format;

**electronic payments** mean 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 document, and that may be used to identify or verify the signatory in relation to the electronic document and indicate the signatory’s approval of the information contained in the electronic document;

**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, including a document sent by facsimile transmission;

**juridical person** means:

(a) any entity constituted or organised under applicable law, whether or not for profit, and whether privately or governmentally owned or controlled, including any corporation, trust, partnership, sole proprietorship, joint venture, association or similar organisation; and

(b) a branch of ajuridical person;

**juridical person of a Party** means a juridical person constituted or organised under the law of a Party, or a branch located in the territory of a Party and carrying out business activities there;[[1]](#footnote-2)

**measure** means any measure by a Party, whether in the form of a law, regulation, rule, procedure, decision, administrative action, or any other form;

**natural person** is defined in accordance with Article 9.1 (Definitions - Trade in Services);

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

**person** means a natural person or a juridical person;

**person of a Party** means a natural person or a juridical person of a Party;

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

**telecommunications** means telecommunications as defined in Article 9B.1 (Definitions – Telecommunications Annex);

**trade administration documents** mean 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 12.2**

**Objectives**

1. The Parties recognise the economic growth and opportunity that digital trade provides, the importance of avoiding barriers to its use and development, and the importance of frameworks that promote consumer confidence in digital trade.
2. The objectives of this Chapter are to:

(a) promote sustainable and stable development of digital trade within the territories of the Parties and between the Parties;

(b) support the growth of economic activity between the Parties;

(c) expand the scope of cooperation between the Parties on matters concerning digital trade;

(d) facilitate greater business-to-business links between the Parties;

(e) foster participation of SMEs in digital trade;

(f) promote consumer confidence in digital trade; and

(g) foster an environment conducive to the further advancement of digital transformation of the Parties’ economies.

# Article 12.3

# Scope and General Provisions

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

2. This Chapter shall not apply to:

 (a) government procurement; or

(b) except for Article 12.18 (Open Government Data), information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection.

3. Articles 12.16 (Cross-Border Transfer of Information by Electronic Means) and 12.19 (Location of Computing Facilities) shall not apply to a measure to the extent that the measure is not subject to an obligation in Chapter 9 (Trade in Services), by reason of:

(a) any term, limitation, qualification, or condition, specified in a Party’s commitments, or with respect to a sector that is not subject to a Party’s commitments, made in accordance with Article 9.5 (Most-Favoured Nation Treatment – Trade in Services) or Article 9.8 (Schedules of Specific Commitments – Trade in Services);

(b) Article 9.9 (Schedules of Non-Conforming Measures and Reservations – Trade in Services); or

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

4. Articles 12.16 (Cross-Border Transfer of Information by Electronic Means) and 12.19 (Location of Computing Facilities) shall not apply to credit information, or related personal data, of a natural person.

# Article 12.4Paperless Trading

Each Party shall endeavour to:

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

(b) accept trade administration documents submitted electronically as the legal equivalent of the paper version of those documents.

**Article 12.5**

# Standards and Conformity Assessment for Digital Trade

1. The Parties recognise the role of international standards and conformity assessment procedures in fostering a well-functioning digital economy, including their potential to decrease compliance costs and increase consistency, interoperability, reliability and efficiency.

2. Each Party shall, where appropriate, actively participate in the work of relevant regional and international bodies relating to the development and adoption of standards that support digital trade.

3. To the extent possible, and if agreed, the Parties shall endeavour to:

(a) share experiences of developing or adopting standards that support digital trade; and

(b) exchange views on potential future areas to develop or adopt standards that support digital trade, including technology standards.

4. The Parties recognise that mechanisms which facilitate the cross-border recognition of conformity assessment results can support digital trade. To this end, the Parties shall endeavour to exchange information to facilitate the acceptance of conformity assessment results with a view to supporting digital trade.

**Article 12.6**

**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* or the *United Nations Convention on the Use of Electronic Communications in International Contracts*, done at New York on November 23, 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, including in relation to trade documentation.

**Article 12.7**

# Electronic Authentication and Electronic Signatures

1. Except in circumstances otherwise 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. Neither Party shall adopt or maintain measures regarding 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 12.8**

# 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 forelectronic invoicing within its territory are interoperable with the systems used in the other Party’s territory.

2. Each Party shall 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, each Party shall endeavour to base its measures relating to electronic invoicing on international frameworks.

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:

 (a) promote, encourage, support or facilitate the adoption of electronic invoicing by juridical persons;

 (b) promote the existence of policies, infrastructure and processes that support electronic invoicing;

 (c) generate awareness of, and build capacity for, electronic invoicing; and

 (d) share best practices and promote the adoption of interoperable international electronic invoicing systems.

**Article 12.9**

# Electronic Payments

1. Recognising the rapid growth of electronic payments, in particular those provided by non-bank, non-financial institutions and financial technology juridical persons, the Parties shall support the development of efficient, safe and secure cross-border electronic payments by:

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

 (b) promoting interoperability and the safe, secure and efficient interlinking of digital electronic payment infrastructures; and

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

2. To this end, each Party shall:

 (a) make publicly available its laws and regulations of general applicability relating to electronic payments, including in relation to regulatory approval, licensing requirements, procedures and technical standards;

 (b) endeavour to finalise decisions on regulatory or licensing approvals relating to electronic payments in a timely manner;

 (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 or utilise international standards for electronic data exchange between financial institutions and services suppliers to enable greater interoperability between electronic payment systems, whichmay include the International Organization for Standardization Standard ISO 20022 Universal Financial Industry Message Scheme;

 (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, if possible, to facilitate greater interoperability, innovation and competition in electronic payments; and

 (f) facilitate innovation and competition and the 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 recognise 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 12.10**

# Online Consumer Protection

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

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

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

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

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

3. Each Party shall adopt or maintain consumer protection laws to proscribe misleading and deceptive commercial activities that may harm 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 digital trade in order to enhance consumer welfare.

5. 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 related to misleading and deceptive commercial activities, including in the enforcement of their consumer protection laws, with respect to online commercial activities.

6. The Parties recognise the benefits of mechanisms, including alternative dispute resolution, to facilitate the resolution of disputes regarding electronic commerce transactions.

**Article 12.11**

# Personal Data Protection

1. The Parties recognise the economic and social benefits of protecting personal data 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 personal data.[[2]](#footnote-3) In the development of any legal framework for the protection of personal data, each Party should endeavour to take into account principles and guidelines of relevant international organisations including collection limitation, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation, and accountability.

3. Each Party shall adopt non-discriminatory practices in protecting natural persons from personal data protection violations occurring within its jurisdiction.

4. Each Party shall publish information on the personal data protections it provides, including how:

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

(b) a juridical person can comply with any legal requirements.

5. Each Party shall encourage juridical persons in its territory to publish, including online, their policies and procedures related to protection of personal data.

6. Recognising that the Parties may take different legal approaches to protecting personal data, 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 12.12**

# 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; or

(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 ensure that commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are made, and contain the necessary information to enable recipients to request cessation free of charge and at any time.

3. 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 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 12.13**

# Principles on Access to and Use of the Internet for Digital Trade

Subject to their respective applicable policies, laws and regulations, 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;[[3]](#footnote-4)

(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 12.14**

# Online Safety and Security

1. The Parties recognise that a safe and secure online environment supports the digital economy.

2. The Parties shall create and promote a safer online environment where individuals are protected from harmful content and conduct, including child sexual exploitation material and violence against women and girls, and where innovation and creativity can thrive.

3. The Parties recognise the importance of taking a multi-stakeholder approach to addressing online safety and security issues.

4. The Parties also recognise that industry has a primary responsibility to adopt and maintain measures to protect individuals, especially children, from harmful online experiences.

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

**Article 12.15**

# Customs Duties

1. A Party shall not impose customs duties on electronic transmissions, including content transmitted electronically, between a person of that Party and a person of the otherParty.

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 12.16**

# 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. A Party shall not prohibit or restrict the cross-border transfer of information by electronic means, including personal data, 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 12.17**

# Data Innovation

1. The Parties recognise that digitalisation and the use of data in the digital economy promote economic growth. To support the cross-border transfer of information by electronic means and promote data-driven innovation in the digital economy, 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 industry and regulatory sandboxes where applicable.

2. The Parties shall endeavour to support data innovation, which may include:

(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 portability; and

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

**Article 12.18**

# Open Government Data

1. The Parties recognise that facilitating public access to and use of open governmentdata contributes to stimulating economic and social benefit, competitiveness, productivity improvements and innovation. To the extent that a Party chooses to make available open government data, it shall endeavour to ensure:

(a) that 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 freely by the public; 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 APIs and is regularly updated.

2. The Parties shall endeavour to cooperate to identify ways in which each Party can expand access to and use of opengovernment data, with a view to enhancing and generating business and research opportunities.

**Article 12.19**

**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. A Party shall not 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.

4. This Article shall not apply with respect to a “financial service supplier”, as defined in Article 9A.1 (Definitions - Financial Services Annex).

**Article 12.20**

# Information and Communication Technology Products that Use Cryptography

1. For the purposes of this Article:

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

(b) **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;

 (c) **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

 (d) **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.[[4]](#footnote-5)

3. With respect to a product that uses cryptography and is designed for commercial application, a Party shall not 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 those of 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 authorities from requiring service suppliers using encryption they control to provide, in accordance with that Party’s legal procedures, unencrypted communications.

**Article 12.21**

# Source Code

1. A Party shall not require the transfer of, or access to, source code[[5]](#footnote-6) of software owned by a person of the other Party 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, regulatory body, judicial authority, administrative tribunal of a Party or a designated conformity assessment body operating in the Party’s territory (“Relevant Body”) from requiring a person of the other Party to preserve or make available the source code of software to the Relevant Body for an investigation, inspection, examination, enforcement action, remedy or judicial or administrative proceeding,[[6]](#footnote-7) subject to safeguards against unauthorised disclosure.

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 its laws or regulations which are not inconsistent with this Agreement.

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

**Article 12.22**

# Digital Government

1. The Parties recognise that technology can enable more efficient and agile government operations, improve the quality and reliability of government services, and enable governments to better serve the needs of their citizens and other stakeholders.

2. Recognising that the Parties can benefit by sharing their experiences with digital government initiatives, the Parties shall endeavour to cooperate on activities relating to the digital transformation of government and government services, which may include:

(a) exchanging information and experiences on digital government strategies and policies;

(b) sharing best practices on digital government and the digital delivery of government services; and

(c) providing advice or training, including through exchange of officials, to assist the other Party in building digital government capacity.

**Article 12.23**

# Digital Identities

Recognising that cooperation between the Parties on digital identities for natural persons and juridical persons 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 legal frameworks, 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 and regulations, technical implementation and security standards, and the promotion of the use of digital identities.

**Article 12.24**

# Artificial Intelligence

1. The Parties recognise that the use and adoption of Artificial Intelligence (“AI”) technologies are becoming increasingly important within a digital economy offering significant social and economic benefits to natural persons and juridical persons. The Parties shall cooperate, in accordance with their respective relevant policies, through:

(a) sharing research and industry practices related to AI technologies and their applications and governance;

(b) promoting and sustaining the safe and responsible development, deployment and use of AI technologies by businesses and across the community; and

(c) encouraging commercialisation opportunities and collaboration between researchers, academics and industry.

2. The Parties also recognise the importance of developing governance and regulatory frameworks for the trusted, safe and responsible use of AI technologies to realise the benefits of AI and mitigate risks. In view of the cross-border nature of the digital economy, 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 frameworks that support the trusted, safe, and responsible use of AI technologies (“AI Governance Frameworks”), through relevant regional and international fora; and

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

**Article 12.25**

**Digital Inclusion**

1. The Parties recognise the importance of digital inclusion and that all people and businesses, including SMEs, can participate in, contribute to, and benefit from electronic commerce and digital trade. To this end, the Parties recognise the importance of expanding and facilitating electronic commerce and digital trade opportunities by addressing barriers to, and encouraging participation in, electronic commerce and digital trade. The Parties also recognise that this may require tailored approaches, developed in consultation with any individuals and groups that disproportionately face such barriers, as well as other relevant stakeholders.

2. To this end, the Parties shall cooperate on matters relating to digital inclusion, including the participation of women, rural populations, low socio-economic groups, First Nations peoples and people with disabilities in the digital economy. Such cooperation may include:

(a) sharing of experience and best practices, including exchange of experts, with respect to digital inclusion;

(b) promoting inclusive and sustainable economic growth, to help ensure that the benefits of the digital economy are more widely shared;

(c) addressing barriers in accessing digital economy opportunities;

(d) developing programs to promote participation of all groups in the digital economy;

(e) supporting universal acceptance of domain names regardless of language script (internationalised domain names) or domain length, including email address internationalisation;

(f) sharing methods and procedures for the collection of disaggregated data, the use of indicators, and the analysis of statistics related to participation in the digital economy; and

(g) other areas jointly decided by the Parties.

3. Cooperation activities relating to digital inclusion may be carried out through the coordination, as appropriate, of the agencies of the Parties, companies, labour unions, civil society, academic institutions, and non-governmental organisations, among others.

**Article 12.26**

# Cooperation

Recognising the importance of digital trade to their collective economies, the Parties shall endeavour to maintain a dialogue on regulatory matters relating to digital trade with a view to sharing information and experiences, as appropriate, including on related laws and regulations, and their implementation, and best practices with respect to digital trade, including in relation to:

(a) online consumer protection;

(b) personal data protection;

(c) anti-money laundering and sanctions compliance for digital trade;

(d) unsolicited commercial electronic messages;

(e) authentication; and

(f) challenges for SMEs in digital trade.

**Article 12.27**

# Cybersecurity

The Parties have a shared vision to promote secure digital trade and recognise that threats to cybersecurity undermine confidence in digital trade. Accordingly, the Parties recognise the importance of:

(a) building the capabilities of their government agencies responsible for cybersecurity 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, diversity and equality.

**Article 12.28**

# Transparency

1. The Parties recognise that transparent measures are important for building trust in the digital economy, creating a conducive environment for digital trade and facilitating trade.

2. Each Party shall promptly publish, or otherwise promptly make publicly available where publication is not practicable, its laws, regulations, procedures and administrative rulings of general application with respect to any matter covered by this Chapter.

3. Each Party shall respond promptly to any request by the other Party for specific information on any of its actual or proposed laws or regulations referred to in paragraph 2.

4. To the extent possible, each Party shall:

(a) publish in advance any measure referred to in paragraph 2 that it proposes to adopt; and

(b) provide interested persons and the other Party with a reasonable opportunity to comment on such proposed measures.

5. To the extent possible, where this Chapter requires a Party to publish information, each Party shall ensure that such information is published online.

1. For greater certainty, the inclusion of a “branch” in the definitions of “juridical person” and “juridical person of a Party” is without prejudice to a Party’s ability to treat a branch under its laws as an entity that has no independent legal existence and is not separately organised. [↑](#footnote-ref-2)
2. For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a 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 juridical persons relating to privacy. [↑](#footnote-ref-3)
3. 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. [↑](#footnote-ref-4)
4. For greater certainty, for the purposes of this Article, a “product” is a good and does not include a financial instrument. [↑](#footnote-ref-5)
5. 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 prose. [↑](#footnote-ref-6)
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. [↑](#footnote-ref-7)