CHAPTER 10

DIGITAL TRADE

ARTICLE 10.1 Definitions

For purposes of this Chapter:

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

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;

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

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}

digital or electronic signature means data in digital or electronic form that is in, affixed to, or logically or cryptographically associated with date in electronic form that is used to identify or verify the signatory in relation to the data in electronic form and used by a signatory to agree on the date in electronic form to which it relates;

electronic invoicing or **e-invoicing** means the automated creation, exchange and processing of request for payments between suppliers and buyers using a structured digital format;

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

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;

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.

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;

open data means non-proprietary information, including data, the central level of government of a Party elects to make freely available to the public;

personal data means any information, including data, about an identified or identifiable natural person; 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 10.2 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, the importance of open standards in enhancing interoperability of digital systems, the importance of the digital economy in promoting inclusive economic growth; the importance of promoting corporate social responsibility, cultural identity and diversity, environmental protection, gender equality, indigenous rights, inclusive trade, sustainable development and traditional knowledge, as well as the importance of preserving the right to regulate in the public interest, and the applicability of the principles of the WTO Agreements to measures affecting digital trade.
- 2. 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 10.3 General Provisions

- 1. This Chapter shall apply to measures adopted or maintained by a Party that affect trade by electronic means.
- 2. This Chapter shall not apply:
 - (a) to government procurement;

- (b) to a service supplied in the exercise of governmental authority;
- (c) except for Article 10.19, to financial services;
- (d) except for Article 10.16, to information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection; and
- (e) to measures adopted or maintained by New Zealand that it deems necessary to protect or promote Māori rights, interests, duties and responsibilities³ in respect of matters covered by this Chapter, including in fulfilment of New Zealand's obligations under te Tiriti o Waitangi / the Treaty of Waitangi. Chapter 20 (Dispute Settlement) does not apply to the interpretation of te Tiriti o Waitangi / the Treaty of Waitangi, including as to the nature of the rights and obligations arising under it.
- 3. For greater certainty, the Parties affirm that measures affecting the supply of a service delivered or performed electronically are subject to the relevant provisions of Chapter 9 (Trade in Services) and its Annexes, including any exceptions or limitations set out in this Agreement that are applicable to such provisions.

ARTICLE 10.4 Customs Duties

- 1. A Party shall not impose customs duties on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of the other Party.
- 2. For greater certainty, paragraph 1 shall not preclude a Party from imposing internal taxes, fees or other charges on content transmitted electronically, provided that such taxes, fees or charges are imposed in a manner consistent with this Agreement.

ARTICLE 10.5 Non-Discriminatory Treatment of Digital Products

1. A Party shall not accord less favourable treatment to digital products created, produced, published, contracted for, commissioned or first made available on commercial terms in the territory of the other Party, or to digital products of which the author, performer, producer, developer or owner is a person of the other Party, than it accords to other like digital products⁴.

³For greater certainty, Māori rights, interests, duties and responsibilities include those relating to mātauranga Māori.

⁴ 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 shall not apply to the extent of any inconsistency with a Party's rights and obligations concerning intellectual property contained in Chapter 13 (Intellectual Property) or another international agreement a Party is party to.
- 3. The Parties understand that this Article does 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 10.6 Information and Communication Technology that Uses Cryptography

- 1. This Article shall apply to information and communication technology (ICT) products that use cryptography.⁵
- 2. With respect to a product that uses cryptography and is designed for commercial applications, no 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.
- 3. Paragraph 2 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.
- 4. For greater certainty, this Section 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, unencrypted communications.

⁵ For greater certainty, for the purposes of this section, a "product" is a good and does not include a financial instrument.

ARTICLE 10.7 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.
- 3. The Parties recognise the importance of facilitating the use of electronic transferable records. When developing measures relating to electronic transferable records, each Party shall take into account the *UNCITRAL Model Law on Electronic Transferable Records* (2017).

ARTICLE 10.8 Authentication

- 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 which are objective, transparent and non-discriminatory or is certified by an authority accredited in accordance with its law.
- 4. The Parties shall encourage the use of interoperable means of authentication.

ARTICLE 10.9 Paperless Trading

- 1. Each Party shall, to the extent practicable, make publicly available, including through a process prescribed by that Party, electronic versions of all existing publicly available trade administration documents.⁶
- 2. Each Party shall provide 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 trade administration.
- 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.
- 5. The Parties shall endeavour to establish or maintain a seamless, trusted, high availability and secure interconnection of their respective single windows to facilitate the exchange of data relating to trade administration documents, which may include:
 - (a) sanitary and phytosanitary certificates;
 - (b) import and export data; or
 - (c) any other documents, as jointly determined by the Parties, and in doing so, the Parties shall provide public access to a list of such documents and make this list of documents available online.
- 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.

⁶ For greater certainty, electronic versions of trade administration documents include trade administration documents provided in a machine-readable format.

⁷ For greater certainty, "high availability" refers to the ability of a single window to continuously operate. It does not prescribe a specific standard of availability.

- 7. The Parties shall endeavour to develop 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;⁸ 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, experiences and 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.
- 10. The Parties shall cooperate bilaterally and in international fora 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 relevant international organisations.

ARTICLE 10.10 Online Consumer Protection

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

10-7

⁸ The Parties recognise that the data exchange systems referred to in this paragraph may refer to interconnection of the single windows referred to in paragraph 5.

2. Each Party shall adopt or maintain consumer protection laws to proscribe misleading, deceptive, and fraudulent commercial activities that cause harm or potential harm to consumers engaged in digital trade.⁹

ARTICLE 10.11 Personal Data Protection

- 1. The Parties recognise the economic and social benefits of protecting the personal data of persons who conduct or engage in electronic transactions and the contribution that this makes to enhancing consumer confidence in digital trade.
- 2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal data of the users of electronic commerce and digital trade. ¹⁰ In the development of any legal framework for the protection of personal data, each Party shall take into account principles and guidelines of relevant international organisations.
- 3. The Parties recognise that the principles underpinning a robust legal framework for the protection of personal data should include:
 - (a) collection limitation;
 - (b) data quality;
 - (c) purpose specification;
 - (d) use limitation;
 - (e) security safeguards;
 - (f) transparency;
 - (g) individual participation; and
 - (h) accountability.
- 4. Each Party shall adopt non-discriminatory practices in protecting users of electronic commerce from personal data protection violations occurring within its jurisdiction.

⁹ For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as generally-applicable consumer protection laws or regulations or sector or medium-specific laws or regulations regarding consumer protection.

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 information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.

- 5. Each Party shall publish information on the personal data protections it provides to users of electronic commerce, including how:
 - (a) individuals can pursue remedies; and
 - (b) businesses can comply with any legal requirements.
- 6. Recognising that the Parties may take different legal approaches to protecting personal information, each Party shall pursue the development of mechanisms to promote compatibility and interoperability between their different regimes for protecting personal data. These mechanisms may include:
 - (a) the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement;
 - (b) broader international frameworks;
 - (c) where practicable, appropriate recognition of comparable protection afforded by their respective legal frameworks' national trustmark or certification frameworks; or
 - (d) other avenues of transfer of personal information between the Parties.
- 7. The Parties shall endeavour to exchange information on how the mechanisms in paragraph 6 are applied in their respective jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility and interoperability between them.
- 8. The Parties shall encourage adoption of data protection trustmarks by businesses that would help verify conformance to personal data protection standards and best practices.
- 9. The Parties shall endeavour to exchange information on and share experiences on the use of data protection trustmarks.
- 10. The Parties shall endeavour to mutually recognise the other Party's data protection trustmarks as a valid mechanism.

ARTICLE 10.12 Principles on Access to and Use of the Internet for Digital Trade

Subject to applicable policies, laws and regulations, each Party recognizes that consumers in its territory should be able to:

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

- (b) connect their choice of devices 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 provider.

ARTICLE 10.13 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 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 cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

ARTICLE 10.14 Cross-Border Flow of Information

- 1 The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.
- 2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.
- 3. Nothing in this Article shall prevent a Party from adopting or maintaining a measure 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 10.15 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 a measure 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 10.16 Open Data

- 1. The Parties recognise that facilitating public access to and use of open data may foster economic and social benefit, competitiveness, productivity improvements and innovation. To the extent that a Party chooses to make open data available, it shall endeavour to ensure:
 - (a) that the information is appropriately anonymised, is accompanied by appropriate 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 regularly updated.
- 2. The Parties shall endeavour to cooperate to identify ways in which each Party can expand access to and use of open data, with a view to enhancing and generating business and research opportunities.

ARTICLE 10.17 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. To this end, the Parties shall endeavour to develop and implement strategies to digitally transform their respective government operations and services, which may include:
 - (a) adopting open and inclusive government processes focusing on accessibility, transparency, and accountability in a manner that overcomes digital divides;
 - (b) promoting cross-sectoral and cross-governmental coordination and collaboration on digital agenda issues;
 - (c) shaping government processes, services, and policies with digital inclusivity in mind;
 - (d) providing a unified customer services experience and common digital enablers for government service delivery;
 - (e) leveraging emerging technologies to build capabilities in anticipation of disasters and crises and facilitating proactive responses;
 - (f) generating public value from government data by applying it in the planning, delivering, and monitoring of public policies, and adopting rules and ethical principles for the trustworthy and safe use of data;
 - (g) making government data and policy-making processes (including algorithms) available for the public to engage with; and
 - (h) promoting initiatives to raise the level of digital capabilities and skills of both the populace and the government workforce.
- 3. 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 10.18 Digital and Electronic Invoicing

- 1. The Parties recognise the importance of digital and electronic invoicing which increases the efficiency, accuracy and reliability of commercial transactions. The Parties also recognise the benefits of ensuring that the systems used for digital and electronic invoicing within their respective 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 digital and electronic invoicing in its jurisdiction supports cross-border interoperability. To this end, each Party shall base its measures relating to digital and electronic invoicing on international frameworks, where they exist.
- 3. The Parties recognise the economic importance of promoting the global adoption of digital and electronic invoicing systems, including those based on interoperable international frameworks. To this end, the Parties shall endeavour to:
 - (a) promote, encourage, support, or facilitate the adoption of digital and electronic invoicing by enterprises;
 - (b) promote the existence of policies, infrastructure, and processes that support digital and electronic invoicing;
 - (c) generate awareness of, and build capacity for, digital and electronic invoicing; and
 - (d) share best practices and promote the adoption of interoperable international digital and electronic invoicing systems.

ARTICLE 10.19 Electronic Payments

- 1. Noting the rapid growth of electronic payments, in particular, those provided by new payment service providers, Parties agree to support the development of efficient, safe and secure cross border electronic payments by fostering the adoption and use of internationally accepted standards, promoting interoperability and the interlinking of payment infrastructures, and encouraging useful innovation and competition in the payments ecosystem.
- 2. To this end, and in accordance with their respective laws and regulations, the Parties recognise 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.
- (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.
- (e) The Parties agree that policies should promote innovation and competition in a level playing field and recognise the importance of enabling the introduction of new financial and electronic payment products and services by incumbents and new entrants in a timely manner such as through adopting regulatory and industry sandboxes.

ARTICLE 10.20 Digital Identities

- 1. Recognising that cooperation between the Parties on digital identities, for natural persons and enterprises, will promote connectivity and growth of digital trade, and recognising that each Party may take different legal and technical approaches to digital identities, the Parties shall endeavour 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.
- 2. For greater certainty, nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 to achieve a legitimate public policy objective.

ARTICLE 10.21

Cooperation

- 1. 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. Such dialogue will be conducted with a view to sharing information and experiences, as appropriate, including on related laws, regulations, and their implementation, and best practices with respect to digital trade. Such dialogue may include discussions on:
 - (a) online consumer protection;
 - (b) personal data protection;
 - (c) unsolicited commercial electronic messages;
 - (d) authentication;
 - (e) intellectual property concerns with respect to digital trade;
 - (f) challenges for small and medium-sized enterprises in digital trade; and
 - (g) digital government.
- 2. 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 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.
- 3. For greater certainty, all cooperation activities under this Chapter are:
 - (a) subject to the availability of resources;
 - (b) pursuant to a request from a Party; and
 - (c) to be conducted on the terms and conditions mutually decided upon between the Parties.

ARTICLE 10.22 Digital Inclusion

- 1. The Parties acknowledge the importance of digital inclusion to ensure that all people and businesses have what they need to participate in, contribute to, and benefit from the digital economy.
- 2. The Parties recognise the importance of expanding and facilitating digital economy opportunities by removing barriers. This may include enhancing cultural and people-to-people links, including between Indigenous Peoples, and improving access for women, rural populations and low socio-economic groups.
- 3. To this end, the Parties shall cooperate on matters relating to digital inclusion, including the participation of women, rural populations, low socio-economic groups and Indigenous Peoples in the digital economy. Cooperation may include:
 - (a) sharing of experiences 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 programmes to promote participation of all groups in the digital economy;
 - (e) 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
 - (f) other areas as mutually agreed by the Parties.
- 4. Cooperation activities relating to digital inclusion may be carried out through the coordination, as appropriate, of the Parties' respective agencies, enterprises, labour unions, civil society, academic institutions and non-governmental organisations, among others.