14 DIGITAL ECONOMY

ARTICLE 1

Definitions

For the purposes of this Chapter:

(a) "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:

(i) 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

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

(b) "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;

(c) "conformity assessment" means conformity assessment as defined in the *Mutual Recognition Agreement on Conformity Assessment between the Government of Australia and the Government of the Republic of Singapore*;

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

(e) "covered person" means a covered enterprise or a natural person of either Party;

(f) "customs duty" means customs duty as defined in Article 2(e) (General Definitions) of Chapter 1 (Objectives and General Definitions);

(g) "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]

(h) "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;

(i) "electronic invoicing" means the automated creation, exchange and processing of

[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.

a request for payment between a supplier and a buyer using a structured digital format;

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

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

(l) "electronic version" of a document means a document in an electronic format prescribed by a Party, including a document sent by facsimile transmission;

(m) "enterprise" means:

(i) 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

(ii) a branch of an enterprise;

(n) "enterprise of a Party" means an enterprise 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;[3]

(o) "existing" means in effect on the date of entry into force of Chapter 14 (Digital Economy);

(p) "financial market infrastructures" means systems in which financial services suppliers participate with other financial services suppliers, including the operator of the system, used for the purposes of:

(i) clearing, settling or recording of payments, securities or derivatives; or

(ii) other financial transactions;

(q) "financial service" means financial service as defined in Article 1(g) (Definitions) of Chapter 9 (Financial Services);

(r) "FinTech" means the use of technology to improve and automate the delivery and use of financial services;

(s) "measure" includes any law, regulation, procedure, requirement or practice;

(t) "national" means:

[3] For greater certainty, the inclusion of a "branch" in the definitions of "enterprise" and "enterprise 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.

(i) for Australia, a natural person who is an Australian citizen as defined in the *Australian Citizenship Act 2007* (Commonwealth) as amended from time to time, or any successor legislation;

(ii) for Singapore, a person who is a citizen of Singapore within the meaning of its Constitution and its domestic laws; or

(iii) a permanent resident of either Party;

(u) "person" means a natural person or an enterprise;

(v) "person of a Party" means a national or an enterprise of a Party;

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

(x) "RegTech" means the use of information technology to improve and manage compliance with regulatory processes;

(y) "sanitary or phytosanitary measure" means sanitary or phytosanitary measure as defined in the *Agreement on the Application of Sanitary and Phytosanitary Measures*, set out in Annex 1A to the WTO Agreement;

(z) "telecommunications" means telecommunications as defined in Article 1(y) of Chapter 10 (Telecommunications Services);

(aa) "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;

(bb) "TRIPS Agreement" means the *Agreement on Trade-Related Aspects of Intellectual Property Rights*, set out in Annex 1C to the WTO Agreement;[4] and

(cc) "unsolicited commercial electronic messages" mean electronic messages, which are sent to an electronic address of a person for commercial or marketing purposes without the consent of the recipient or despite the explicit rejection of the recipient.

ARTICLE 2

Scope

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

2. This Chapter shall not apply:

[4] For greater certainty, a reference in this Agreement to the TRIPS Agreement includes any waiver in force between the Parties of any provision of the TRIPS Agreement granted by WTO Members in accordance with the WTO Agreement.

(a) to government procurement; or

(b) except for Article 27 (Open Government Data), to information held or processed on behalf of a Party or measures related to such information, including measures related to its collection.

3. Articles 6 (Non-Discriminatory Treatment of Digital Products), 23 (Cross-Border Transfer of Information by Electronic Means), 24 (Location of Computing Facilities) and 25 (Location of Computing Facilities for Financial Services) shall not apply to a measure to the extent that the measure is not subject to an obligation in Chapters 7 (Cross-Border Trade in Services), 8 (Investment) or 9 (Financial Services) by reason of:

(a) Article 7 (Reservations) of Chapter 7 (Cross-Border Trade in Services), Article 11 (Reservations) of Chapter 8 (Investment) or Article 10 (Non-Conforming Measures) of Chapter 9 (Financial Services); or

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

4. For Australia, Articles 23 (Cross-Border Transfer of Information by Electronic Means), 24 (Location of Computing Facilities) and 25 (Location of Computing Facilities for Financial Services) shall not apply to credit information, or related personal information, of a natural person.

ARTICLE 3

General Exceptions

1. For the purposes of this Chapter, Article XX of GATT 1994 and its interpretative notes are incorporated into and made part of this Agreement, *mutatis mutandis.*

2. For the purposes of this Chapter, paragraphs (a), (b) and (c) of Article XIV of GATS are incorporated into and made part of this Agreement, *mutatis mutandis.*

3. The Parties understand that the measures referred to in Article XX(b) of GATT 1994 include environmental measures necessary to protect human, animal or plant life or health, and that Article XX(g) of GATT 1994 applies to measures relating to the conservation of living and non-living exhaustible natural resources.

ARTICLE 4

Disclosure of Information

Nothing in this Chapter shall require a Party to furnish or allow access to confidential information, the disclosure of which would be contrary to its law, impede law enforcement, or otherwise be contrary to the public interest, or which would prejudice legitimate commercial interests of particular enterprises, public or private.

ARTICLE 5

Customs Duties

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

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

ARTICLE 6

Non-Discriminatory Treatment of Digital Products

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

2. Paragraph 1 shall not apply to the extent of any inconsistency with the rights and obligations in the TRIPS Agreement or with Chapter 13 (Intellectual Property).

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 7

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.[5]

3. With respect to a product that uses cryptography and is designed for commercial

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

applications, neither Party shall impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of the product, as a condition of the manufacture, sale, distribution, import or use of the product, to:

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

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

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

other than where the manufacture, sale, distribution, import or use of the product is by or for the government of the Party.

4. Paragraph 3 shall not apply to:

(a) requirements that a Party adopts or maintains relating to access to networks that are owned or controlled by the government of that Party, including 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 8

Domestic Electronic Transactions Framework

1. For the purposes of this Article:

(a) "electronic transferable record" means an electronic record that satisfies the requirements set out in Article 10 of the *UNCITRAL Model Law on Electronic Transferable Records* (2017), and may include an electronic bill of lading; and

(b) "international bodies" means international bodies to which both Parties are participants or members.

2. 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.

3. 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.

4. The Parties recognise the importance of developing mechanisms to facilitate the use of electronic transferrable 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).

ARTICLE 9

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 for electronic authentication that would:

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

(b) prevent parties to an electronic transaction from having the opportunity to establish before judicial or administrative authorities that their transaction complies with any legal requirements with respect to authentication.

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

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

ARTICLE 10

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 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 base its measures relating to electronic invoicing on international frameworks, such as Peppol.

3. The Parties recognise the economic importance of promoting the global adoption of

interoperable electronic invoicing systems. To this end, the Parties shall share best practices and collaborate on promoting the adoption of interoperable systems for electronic invoicing.

4. The Parties shall collaborate on initiatives which promote, encourage, support or facilitate the adoption of electronic invoicing by enterprises. To this end, the Parties shall endeavour to:

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

(b) generate awareness of, and build capacity for, electronic invoicing.

ARTICLE 11

Electronic Payments

1. Recognising the rapid growth of electronic payments, in particular those provided by non-bank, non-financial institution and FinTech enterprises, 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 interlinking of electronic payment infrastructures; and

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

2. To this end, each Party shall:

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

(b) endeavour to finalise decisions on regulatory or licensing approvals 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, for relevant electronic payment systems, international standards for electronic payment messaging, such as the International Organization for Standardization *Standard ISO 20022 Universal Financial Industry Message Scheme*, for electronic data exchange between financial institutions and services suppliers to enable greater interoperability between electronic payment systems;

(e) facilitate the use of open platforms and architectures such as tools and protocols provided for through Application Programming Interfaces (“APIs”) and

encourage payment service providers to safely and securely make APIs for their products and services available to third parties, where possible, to facilitate greater interoperability, innovation and competition in electronic payments; and

(f) facilitate innovation 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

Paperless Trading

1. Each Party shall make publicly available, which may include through a process prescribed by that Party, electronic versions of all of its trade administration documents in English.[6]

2. Each Party shall accept completed electronic versions of its trade administration documents as the legal equivalent of paper documents except where:

(a) there is a domestic or international legal requirement to the contrary; or

(b) doing so would reduce the effectiveness of the trade administration process.

3. Each Party shall endeavour to establish or maintain a single window enabling traders to submit trade administration documents and data requirements for importation, exportation or transit of goods through a single entry point to the participating authorities or agencies.

4. Each Party shall endeavour to establish or maintain a seamless, trusted and secure interface with the other Party's single window to facilitate the exchange of data relating to trade administration documents, which may include:

(a) sanitary and phytosanitary certificates;

(b) customs declaration data; and

(c) any other documents, as jointly determined by the Parties.[7]

5. Each Party recognises the importance of facilitating the exchange of electronic records used in commercial trading activities between enterprises within its territory.

---

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

[7] The Parties shall provide public access to the list of trade administration documents referred to in this paragraph and make this information available online.

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

(a) data relating to the trade administration documents referred to in paragraph 4 between the competent authorities of each Party; and

(b) electronic records used in commercial trading activities between enterprises within each Party's respective territory.

7. The Parties shall cooperate and collaborate on new initiatives which promote, encourage, support and facilitate the use and adoption of the data exchange systems referred to in paragraph 6, including through:

(a) the sharing of information and experiences, including the exchange of best practices, in the area of development and governance of data exchange systems; and

(b) collaboration on pilot projects that relate to the development and governance of data exchange systems.

8. The Parties recognise that the data exchange systems referred to in paragraph 6 should, as far as possible, be compatible and interoperable with each other. To this end, the Parties shall endeavour to work towards the development and adoption of internationally-recognised standards in the development and governance of the data exchange systems.

9. The Parties shall cooperate bilaterally and in international fora, where appropriate, to promote acceptance of electronic versions of trade administration documents and electronic records used in commercial trading activities between enterprises.

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

ARTICLE 13

Express Shipments

1. The Parties recognise that electronic commerce plays an important role in increasing trade. To facilitate air express shipments, each Party shall ensure its customs procedures are applied in a manner that is predictable, consistent and transparent.

2. Each Party shall adopt or maintain expedited customs procedures for air express shipments while maintaining appropriate customs control and selection. Each Party shall ensure its customs procedures:

(a) provide for information necessary to release an express shipment to be submitted and processed before the shipment arrives;

(b) allow a single submission of information covering all goods contained in an

express shipment, such as a manifest, through, if possible, electronic means;[8]

(c) to the extent possible, provide for the release of certain goods with a minimum of documentation;

(d) under normal circumstances, provide for express shipments to be released within six hours of submission of the necessary customs documents, provided the shipment has arrived; and

(e) apply to shipments of any weight or value, recognising that a Party may require formal entry procedures as a condition for release, including a declaration and supporting documentation and payment of customs duties, based on the good's weight or value.

3. If a Party does not provide the treatment in paragraphs 2(a) through (e) to all shipments, that Party shall provide a separate[9] and expedited customs procedure that provides such treatment for express shipments.

4. Each Party shall provide for a *de minimis* shipment value or dutiable amount for which customs duties will not be collected, aside from restricted or controlled goods, such as goods subject to import licensing or similar requirements.[10] Each Party shall review the amount periodically taking into account factors that it may consider relevant, such as rates of inflation, effect on trade facilitation, impact on risk management, administrative cost of collecting duties compared to the amount of duties, cost of cross-border trade transactions, impact on small and medium-sized enterprises ("SMEs") or other factors related to the collection of customs duties.

ARTICLE 14

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

[8] For greater certainty, additional documents may be required as a condition for release.

[9] For greater certainty, "separate" does not mean a specific facility or lane.

[10] Notwithstanding this Article, a Party may assess customs duties, or may require formal entry documents, for restricted or controlled goods such as goods subject to import licensing or similar requirements.

adopt; and

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

5. Where this Chapter requires a Party to publish information, each Party shall ensure that such information is published on the Internet.

ARTICLE 15

Online Consumer Protection

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

2. For the purposes of this Article, misleading and deceptive 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 significant 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, internet or other accounts without authorisation.

3. Each Party shall adopt or maintain consumer protection laws to proscribe misleading and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.

4. The Parties recognise the importance of cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border electronic commerce in order to enhance consumer welfare.

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 16

Cooperation on Competition Policy

1. Recognising that the Parties can benefit by sharing their experiences in enforcing

competition law and in developing and implementing competition policies to address the challenges that arise from the digital economy, the Parties shall consider undertaking agreed technical cooperation activities, subject to available resources, including:

(a) exchanging information and experiences on the development of competition policies for digital markets;

(b) sharing best practices on the enforcement of competition law and the promotion of competition in digital markets;

(c) providing advice or training, including through the exchange of officials, to assist a Party to build necessary capacities to strengthen competition policy development and competition law enforcement in digital markets; or

(d) any other form of technical cooperation agreed by the Parties.

2. Subject to each Party's available resources, the Parties shall endeavour to cooperate, where practicable and in accordance with their respective laws and regulations, on issues of competition law enforcement in digital markets, including through notification, consultation and the exchange of information.

ARTICLE 17

Personal Information Protection

1. The Parties recognise the economic and social benefits of protecting the personal information of persons who conduct or engage in electronic transactions and the contribution that this makes to enhancing consumer confidence in electronic commerce.

2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of persons who conduct or engage in electronic transactions. In the development of its legal framework for the protection of personal information, each Party shall take into account the principles and guidelines of relevant international bodies, such as the APEC Cross-Border Privacy Rules ("CBPR") System and the *OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data*.[11]

3. To this end, the key principles each Party shall take into account when developing its legal framework include limitation on collection, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation and accountability.

4. Each Party shall adopt non-discriminatory practices in protecting persons who conduct or engage in electronic transactions from personal information protection violations occurring within its jurisdiction.

[11] 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 publish information on the personal information protections it provides to persons who conduct or engage in electronic transactions, including how:

(a) a natural person can pursue remedies; and

(b) business can comply with any legal requirements.

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

7. 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 and share experiences on any such mechanisms applied in their jurisdictions and explore ways to promote compatibility between them.

8. The Parties recognise that the CBPR System is a valid mechanism to facilitate cross-border information transfers while protecting personal information.[12]

9. The Parties shall endeavour to jointly promote the CBPR System, with the aim to improving awareness of, and participation in, the CBPR System, including by industry.

ARTICLE 18

Creating a Safe Online Environment

1. The Parties shall create and promote a safe online environment where users are protected from harmful content, including terrorist and violent extremist content, and where businesses, innovation and creativity can thrive.

2. The Parties recognise that online safety is a significant challenge but it is a shared responsibility between governments, technology service providers and users. The Parties further recognise that a safe, secure online environment supports the digital economy.

3. The Parties also recognise that industry has a responsibility to adopt or maintain preventative measures to protect natural persons, especially children and vulnerable members of the community, from harmful online experiences.

4. The Parties shall work together and within international fora to create a safe online environment, in accordance with their respective laws and regulations.

5. In working together to create a safe online environment, the Parties shall endeavour to maintain an open, free and secure Internet in accordance with their respective laws and regulations.

[12] The Parties acknowledge that the CBPR System does not displace or change a Party's laws and regulations concerning the protection of personal information.

ARTICLE 19

Unsolicited Commercial Electronic Messages

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

2. Each Party shall endeavour to adopt or maintain measures that enable consumers to reduce or prevent unsolicited commercial electronic messages sent other than to an electronic mail address, or otherwise provide for the minimisation of these messages.

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 or 2.

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

ARTICLE 20

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

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;[13]

(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 21

Internet Interconnection Charge Sharing

Each Party recognises that a supplier seeking international Internet connection should be able to negotiate with suppliers of the other Party on a commercial basis. These negotiations may include negotiations regarding compensation for the establishment, operation and maintenance of facilities of the respective suppliers.

ARTICLE 22

Submarine Telecommunications Cable Systems

1. The Parties recognise the importance of submarine telecommunications cable systems, and the expeditious and efficient installation, maintenance and repair of these systems, to national, regional and global telecommunications connectivity. Each Party shall endeavour to ensure that, to the extent possible, a person of the other Party who operates, owns or controls submarine telecommunications cable systems has flexibility to choose suppliers of installation, maintenance or repair services, including from either Party or a non-Party.

2. Each Party shall ensure that, where it requires a permit for a vessel registered in the territory of the other Party or a non-Party to undertake installation, maintenance or repairs of submarine telecommunications cable systems that are operated, owned or controlled by a person of the other Party:

(a) the activities for which any such permit is required are publicly available;

(b) the requirements and procedures for applying for any such permit, and for renewal of a permit, including any relevant application documents, are publicly available;

[13] 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.

(c) the criteria for assessing an application for any such permit are made available upon reasonable prior request in writing;

(d) the procedures for applying for any such permit and, if granted, the permit and the procedures for renewal of a permit are administered in a reasonable, objective and impartial manner;

(e) within a reasonable period of time after the submission of an application for any such permit and for renewal of a permit that is considered complete under its laws and regulations, it informs the applicant of the decision concerning the application;

(f) any such permit, if granted, is of a sufficient duration to undertake the required installation, maintenance or repairs of submarine telecommunications cable systems; and

(g) any fee charged by any of its relevant bodies to obtain, maintain or renew any such permit is reasonable, transparent, and is limited in amount to the approximate cost of services rendered by that body in respect of any such fee.

3. If a Party ("the first Party") considers that a measure of the other Party creates a material impediment to the ability of a person of the first Party to expeditiously and efficiently install, maintain, repair or protect submarine telecommunications cable systems, it may request consultations with the other Party with regard to that measure. The Parties shall enter into consultations with a view to exchanging information on the operation of the measure and to considering whether further steps are necessary and appropriate.

4. Each Party shall endeavour to mitigate the risk of damage to submarine telecommunications cable systems that are operated, owned or controlled by a person of the other Party, which may include, as appropriate:

(a) the use of geospatial alert systems;

(b) making information available on the location of submarine telecommunications cable systems to inform mapping and charting;

(c) public demarcation of areas within which submarine telecommunications cable systems are present and where activities are banned within that area to protect submarine telecommunications cable systems; or

(d) activities to promote awareness of submarine telecommunications cable systems.

ARTICLE 23

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 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 24

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.

4. This Article shall not apply with respect to a "financial institution" or a "financial service supplier of a Party", as defined in Article 1(e) and (h) (Definitions) respectively of Chapter 9 (Financial Services).

ARTICLE 25

Location of Computing Facilities for Financial Services

1. For the purposes of this Article, for a Party ("the relevant Party"), a "covered financial person" means:

(a) a "financial institution", as defined in Article 1(e) (Definitions) of Chapter 9 (Financial Services), including a branch, located in the territory of the relevant

Party that is controlled by persons of either Party; or

(b) a "cross-border financial service supplier of a Party", as defined in Article 1(b) (Definitions) of Chapter 9 (Financial Services), that is subject to regulation, supervision, licensing, authorisation, or registration by a financial regulatory authority of the relevant Party.

2. Neither Party shall require a covered financial person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory, provided that the Party's financial regulatory authorities, for regulatory or supervisory purposes, have immediate, direct, complete and ongoing access to information processed or stored on computing facilities that the covered financial person uses or locates outside the Party's territory.

3. Each Party shall, to the extent practicable, provide a covered financial person with a reasonable opportunity to remediate any lack of access to information described in paragraph 2 before the Party requires the covered person to use or locate computing facilities in the Party's territory or the territory of a non-Party.

ARTICLE 26

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 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 portability; and

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

ARTICLE 27

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 contributes to stimulating economic and social benefit, competitiveness, productivity improvements 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 and is in a machine readable and open format that allows it to be searched, retrieved, used, reused and redistributed; and

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

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

ARTICLE 28

Source Code

1. Neither Party shall require the transfer of, or access to, source code of software owned by a person of the other Party, 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 or judicial authority ("Relevant Body") of a Party from requiring a person of the other Party to preserve or make available the source code of software to the Relevant Body for an investigation, inspection, examination, enforcement action, or judicial or administrative proceeding,[14] 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 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.

5. If both Parties undertake obligations[15] under:

(a) an international agreement that enters into force after the date of entry into force of this Agreement; or

(b) an amendment to any existing international agreement,[16]

to not require the transfer of, or access to, an algorithm expressed in source code of software owned by a person of a Party or non-Party as a condition for the import, distribution, sale or use of that software, or of products containing that software, in their respective territories, this Article[17] shall apply, *mutatis mutandis*, to algorithms expressed in source code of software owned by a person of the other Party.

6. If a Party undertakes the obligation referred to in paragraph 5, it shall notify the other

[14] 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.

[15] For greater certainty, a Party will "undertake" an obligation for the purposes of this paragraph regardless of any limitations or exceptions that may apply to those obligations under the relevant international agreement.

[16] For greater certainty, both Parties will "undertake obligations" where each Party has undertaken obligations under separate international agreements or the same international agreement.

[17] For greater certainty, this includes any limitations and exceptions in this Article and is subject to any limitations and exceptions that apply to this Article.

Party within 120 days of the date that the relevant international agreement or amendment enters into force. For greater certainty, paragraph 5 shall apply regardless of whether a Party has provided such notification.

ARTICLE 29

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) 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;

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

(e) 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 30

Standards and Conformity Assessment for Digital Trade

1. The Parties recognise the role of standards in reducing barriers to trade and 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 where agreed, the Parties shall endeavour to:

(a) share experiences of developing or adopting standards that support digital trade, including technology standards;

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

(c) identify, develop and test, with industry participants as appropriate, cross-border projects that demonstrate standards that support digital trade, including technology standards.

4. Where agreed, the Parties shall cooperate on initiatives, including research projects, to develop a greater understanding, between the Parties and industry, of standards that support digital trade and their benefits and applications.[18]

5. The Parties recognise that mechanisms which facilitate the cross-border recognition of conformity assessment results can support digital trade. Such mechanisms include:

(a) voluntary arrangements between relevant conformity assessment bodies; and

(b) the use of regional or international recognition agreements or arrangements that the Parties are party to, or are represented at.

6. 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.

[18] For greater certainty, the financial arrangements that may be required for initiatives under this Article will be decided upon by the Parties on a case-by-case basis.

ARTICLE 31

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 enterprises. The Parties shall cooperate, in accordance with their respective relevant policies, through:

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

(b) promoting and sustaining the responsible use and adoption 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 ethical governance frameworks for the trusted, safe and responsible use of AI technologies that will help realise the benefits of AI. In view of the cross-border nature of 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 principles or guidelines when developing such AI Governance Frameworks.

ARTICLE 32

FinTech and RegTech Cooperation

The Parties shall:

(a) encourage collaboration on FinTech and RegTech through their respective policy and trade promotion agencies and regulators;

(b) promote closer and stronger collaboration between their respective FinTech and RegTech enterprises and industry bodies;

(c) encourage their respective FinTech and RegTech enterprises to use facilities and assistance, where available, in the other Party's territory to explore new business opportunities, including through the use of streamlined licencing processes where applicable and access to regulatory sandboxes;

(d) cooperate in relevant regional and international fora to improve opportunities for Australian and Singaporean FinTech and RegTech enterprises; and

(e) cooperate on the development of standards for open banking.

ARTICLE 33

Cooperation

The Parties shall endeavour to:

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

(i) personal information protection;

(ii) online consumer protection, including means for consumer redress and building consumer confidence;

(iii) unsolicited commercial electronic messages;

(iv) security in electronic communications;

(v) electronic authentication; and

(vi) digital government;

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

(c) exchange information on the development, reform, implementation and effectiveness of copyright legal frameworks relevant to the online environment, including on surveys related to online infringement and on enforcement mechanisms;

(d) exchange financial intelligence and share capabilities to support regional efforts to counter terrorism financing, money laundering and other transnational organised crime;

(e) participate actively in regional and multilateral fora to promote the development of the digital economy; and

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

ARTICLE 34

Cybersecurity

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

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

ARTICLE 35

Stakeholder Engagement

1. The Parties shall seek opportunities to convene a Digital Economy Dialogue (the "Dialogue") at times agreeable to the Parties, to promote the benefits of the digital economy. The Parties shall promote relevant collaboration efforts and initiatives between the Parties through the Dialogue.

2. Where appropriate, and as may be agreed by the Parties, the Dialogue may include participation from other interested stakeholders, such as researchers, academics, industry and other stakeholders. The Parties may collaborate with such stakeholders in convening the Dialogue.

3. To encourage inclusive participation by the Parties' stakeholders and increase the impact of outreach, the Parties may consider organising the Dialogue in connection with, or as a part of, existing bilateral initiatives.

4. The Parties may consider relevant technical or scientific input, or other information arising from the Dialogue, for the purposes of implementation efforts and further modernisation of this Chapter.

ARTICLE 36

Small and Medium Enterprises

1. The Parties recognise the fundamental role of SMEs in maintaining dynamism and enhancing competitiveness in the digital economy.

2. With a view towards enhancing trade and investment opportunities for SMEs in the digital economy, the Parties shall endeavour to:

(a) exchange information and best practices in leveraging digital tools and technology to improve:

(i) the capabilities and market reach of SMEs; and

(ii) participation by SMEs in government procurement opportunities;

(b) cooperate in other areas that could help SMEs adapt and thrive in the digital economy;

(c) encourage participation by SMEs in online platforms and other mechanisms that could help SMEs link with international suppliers, buyers and other potential business partners; and

(d) foster close cooperation on the digital economy between SMEs of the Parties.

ARTICLE 37

Capacity Building

The Parties shall endeavour to cooperate on capacity building in the region on issues including:

(a) digital connectivity;

(b) SME digital transformation;

(c) data protection regimes; and

(d) mechanisms to facilitate the cross-border transfer of information.

ARTICLE 38

Review

In any review of this Agreement, conducted in accordance with Article 7 (Review) of Chapter 17 (Final Provisions), the Parties shall consider discussing appropriate amendments to this Chapter, including in light of any treatment that either Party considers a Party is obliged to accord to persons of a non-Party, under an international agreement that enters into force after the date of entry into force of this Chapter 14 (Digital Economy), that is more favourable than the treatment that the Party is obliged to accord to persons of the other Party, in like circumstances, under this Chapter.