DIGITAL ECONOMY AGREEMENT BETWEEN THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND AND THE REPUBLIC OF SINGAPORE

The United Kingdom of Great Britain and Northern Ireland ("the United Kingdom") and the Republic of Singapore ("Singapore") (hereinafter jointly referred to as "the Parties" or individually referred to as "Party"),

Recognising the deep and longstanding relationship, underpinned by the Joint Statement on the Singapore-UK Partnership for the Future and the Free Trade Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore, done at Singapore on 10 December 2020 (the "UK-Singapore Free Trade Agreement");

Recognising the economic opportunities and the wider access to goods and services brought about by the digital economy;

Sharing a vision for greater integration and the digital transformation of the Parties' economies;

Reflecting the forward-looking nature of their partnership and commitment to deepen bilateral cooperation in new and emerging areas;

Further recognising the importance of ensuring all people and businesses of all sizes can participate in, contribute to, and benefit from the digital economy including the fundamental role of small and medium-sized enterprises in maintaining dynamism and enhancing competitiveness;

Resolving to facilitate a trusted and secure digital environment that promotes consumer and business interests;

Desiring to establish a dynamic framework for cooperation in the fast-paced and evolving digital economy;

Complementing the Parties' international leadership roles in the pursuit of ambitious benchmarks, rules and standards for the digital economy; and

Building on the Parties' rights, obligations and undertakings in the World Trade Organization ("WTO"), and other international and bilateral agreements and arrangements concerning digital trade and the digital economy,

Have agreed as follows:

ARTICLE 1

Definitions

For the purposes of this Digital Economy Agreement:

(a) "the Incorporated Agreement" is as defined in paragraph 1(b) of Article 2 (Definitions and interpretation) of the UK-Singapore Free Trade Agreement; and

(b) "this Digital Economy Agreement" means this Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore.

ARTICLE 2

Amendment of the UK-Singapore Free Trade Agreement

The Parties hereby agree to amend the UK-Singapore Free Trade Agreement, in accordance with Article 8 (Amendments) of the UK-Singapore Free Trade Agreement. In particular, the Parties agree to:

(a) replace the provisions of Section F (Electronic Commerce) of Chapter Eight of the Incorporated Agreement with the provisions as set out in Annex A to this Digital Economy Agreement; and

(b) amend the Incorporated Agreement as set out in Annex B to this Digital Economy Agreement.

ARTICLE 3

Cooperation

1. The Parties recognise the fast-paced and evolving nature of the digital economy, and the role of technical cooperation between the Parties in increasing and enhancing the opportunities provided by the digital economy.

2. To this end, the Parties shall endeavour to cooperate on areas of mutual interest concerning the digital economy and shall also encourage businesses, researchers and academics in their respective territories to engage in this cooperation. The Parties may consider relevant input and information arising from cooperation efforts for the purposes of implementation and further modernisation of this Digital Economy Agreement.

3. The Parties may undertake such cooperation under this Digital Economy Agreement, the UK-Singapore Free Trade Agreement or any instrument entered into by the Parties in connection with the conclusion of the Digital Economy Agreement, through efforts such as entering into memoranda of understanding and collaborative projects, or in the context of international fora which the Parties are participants in or members of.

ARTICLE 4

Information Sharing

1. Each Party shall establish or maintain its own free, publicly accessible website containing updated information regarding this Digital Economy Agreement, including:

(a) the text of this Digital Economy Agreement;

(b) a summary of this Digital Economy Agreement; and

(c) any additional information that a Party considers would be useful for SMEs interested in benefitting from this Digital Economy Agreement and in participating in cooperation initiatives agreed by the Parties.

2. Each Party shall make the information published in accordance with paragraph 1 available in English.

ARTICLE 5

Integral Parts

1. This Digital Economy Agreement shall form an integral part of the UK-Singapore Free Trade Agreement.

2. The Annexes and footnotes to this Digital Economy Agreement shall form an integral part thereof.

ARTICLE 6

Final Provisions

1. This Digital Economy Agreement shall enter into force on the first day of the second month following the date of the later of the Parties' written notifications certifying that they have completed their respective applicable legal requirements and procedures for the entry into force of this Digital Economy Agreement. The Parties may agree on another date for entry into force, provided such date occurs after the completion of the exchange of notifications referred to above.

2. Any time after the date of entry of force of this Digital Economy Agreement, this Digital Economy Agreement, or specified provisions of this Digital Economy Agreement, may be brought into force for Gibraltar on the first day of the second month following the United Kingdom's written notification to Singapore certifying the completion of the applicable legal requirements and procedures for the bringing into force of this Digital Economy Agreement, or specified provisions of this Digital Economy Agreement, in respect of Gibraltar. The Parties may agree on another date, provided such date occurs after the United Kingdom's written notification referred to above.

3. Any time after the date of entry of force of this Digital Economy Agreement, this Digital Economy Agreement, or specified provisions of this Digital Economy Agreement, may be brought into force for:

(a) the Bailiwick of Guernsey;

(b) the Bailiwick of Jersey[1]; or

(c) the Isle of Man,

on the first day of the second month following the United Kingdom's written notification to Singapore certifying the completion of applicable legal requirements and procedures for the bringing into force of this Digital Economy Agreement, or specified provisions of this Digital Economy Agreement, in respect of such territory.[2] The Parties may agree on another date, provided such date occurs after the date of the United Kingdom's written notification referred to above.

4. The United Kingdom shall submit notifications under this Article to the Director, North America and Europe Division, Singapore's Ministry of Trade and Industry or its successor. Singapore shall submit notifications under this Article to the United Kingdom's Foreign, Commonwealth and Development Office or its successor.

5. At any time after the date this Digital Economy Agreement has been brought into force for a territory referred to in paragraphs 2 and 3, the United Kingdom may give written notice to Singapore that this Digital Economy Agreement, or specified provisions of this Digital Economy Agreement, shall no longer apply to such territory. To this end, the procedure as set out in paragraphs 2, 3 and 4 of Article 16.14 (Duration) of the Incorporated Agreement shall apply, *mutatis mutandis*.

---

1 The Bailiwicks of Guernsey and Jersey are jointly known as the Channel Islands.

2 The Parties agree that, prior to this, the UK shall hold consultations with Singapore concerning the application of relevant provisions of the Incorporated Agreement to such territory.

In witness whereof the undersigned, duly authorised thereto by their respective Governments, have signed this Digital Economy Agreement.

DONE in duplicate at Singapore on this 25th day of February 2022 in English.

For the Government of the Republic of Singapore:

For the Government of the United Kingdom of Great Britain and Northern Ireland:

ANNEX A

SECTION F

DIGITAL TRADE AND THE DIGITAL ECONOMY

ARTICLE 8.57

Definitions

For the purposes of this Section:

(a) "algorithm" means a defined sequence of steps, taken to solve a problem or obtain a result;

(b) "ciphertext" means data in a form that cannot be easily understood without subsequent decryption;

(c) "commercial information and communication technology product"[3] ("Commercial Information and Communications Technology (ICT) Product") means a product that is designed for commercial applications and which intended function is information processing and communication by electronic means, including transmission and display, or electronic processing applied to determine or record physical phenomena, or to control physical processes;

(d) "computing facilities" means a computer server or storage device for processing or storing information for commercial use;

(e) "covered person" means:

---

3 For greater certainty, for the purposes of this Section, a commercial ICT product does not include a financial instrument.

(i) an establishment of a Party as defined in subparagraph (d) of Article 8.8 (Definitions);

(ii) an entrepreneur as defined in subparagraph (c) of Article 8.8 (Definitions); or

(iii) a service supplier of a Party as defined in subparagraph (l) of Article 8.2 (Definitions),

but does not include a financial service supplier as defined in subparagraph 2(d) of Article 8.49 (Scope and Definitions);

(f) "cryptographic algorithm" means a defined method of transforming data using cryptography;

(g) "cryptography" means the principles, means or methods for the transformation of data in order to conceal or disguise its content, prevent its undetected modification, or prevent its unauthorised use, and is limited to principles, means or methods where one or more secret parameters, for example, crypto variables, or associated key management is required in order to transform the data or to perform the corresponding reverse transformation;

(h) "electronic authentication" means the electronic process or act of verifying the identity of a party to an electronic communication or transaction, or of ensuring the integrity of an electronic communication;

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

(j) "electronic signature" means data in electronic form that is in, affixed to, or logically associated with an electronic data message that may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message[4];

(k) "electronic transferable record" means a document or instrument in electronic form which under a Party's laws or regulations is both functionally equivalent to a transferable record and satisfies quality requirements such as those referenced in Article 10 of the UNCITRAL Model Law on Electronic Transferable Records of 2017;

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

(m) "emerging technology" means an enabling and innovative technology that has potentially significant application across a wide range of existing and future sectors;

(n) "encryption" means the conversion of data (plaintext) through the use of a cryptographic algorithm into a ciphertext using the appropriate key;

(o) "end-user" means a natural person, or juridical person to the extent provided for in a Party's laws and regulations, using or requesting a public telecommunications service, either as a consumer or for trade, business, or professional purposes;

(p) "government information" means non-proprietary information, including data, held by the central government;

---

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

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

(r) "Lawtech" describes technologies that aim to support, supplement or replace traditional methods for delivering legal services;

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

(t) "public telecommunications service" means a public telecommunications service as defined in subparagraph (i) of Article 8.25 (Definitions);

(u) "trade administration document" means the forms and documents 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

(v) "unsolicited commercial electronic message" means an electronic message[5] that is sent for commercial or marketing purposes directly to an electronic address of an end-user via a public telecommunications service, without the consent of the recipient or despite the explicit rejection of the recipient.

---

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

ARTICLE 8.58

Objectives and Scope

1. The Parties recognise the economic benefits of, and opportunities provided by, open and connected digital markets.

2. The Parties further recognise the importance of:

(a) avoiding unnecessary barriers to the use and development of digital trading systems;

(b) promoting the interoperability of regulatory frameworks to facilitate seamless end-to-end digital trade;

(c) international cooperation with a view to developing frameworks to govern digital trade that are open and inclusive; and

(d) adopting frameworks that:

(i) take into account emerging technologies;

(ii) facilitate a trusted and secure digital environment;

(iii) promote consumer confidence in digital trade; and

(iv) ensure all people and businesses of all sizes can participate in, contribute to, and benefit from the digital economy.

3. This Section shall apply to measures of the Parties affecting trade enabled by electronic means.

4. This Section shall not apply to:

(a) audio-visual services;

(b) government procurement, except as provided for in paragraph 4 of Article 8.60 (Domestic Electronic Transactions Framework and Electronic Contracts), paragraph 1 of Article 8.61 (Electronic Authentication) and Article 8.61-Q (Small and Medium-sized Enterprises); or

(c) information held or processed by or on behalf of a Party, or measures of a Party related to that information, including measures related to its collection, except as provided for in Article 8.61-H (Open Government Information).

5. For greater certainty, a measure that affects the supply of a service delivered or performed electronically is subject to the obligations contained in relevant provisions of Chapter Eight of this Agreement, including Annex 8-A and Annex 8-B of this Agreement, as well as any exceptions that are applicable to those obligations.

ARTICLE 8.59

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 electronic transmissions, including content transmitted electronically, provided that such taxes, fees, or charges are imposed in a manner consistent with this Agreement.

ARTICLE 8.60

Domestic Electronic Transactions Framework and Electronic Contracts

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, 23 November 2005.

2. Each Party shall endeavour to:

(a) avoid any unnecessary regulatory burden on electronic transactions; and

(b) facilitate input by interested persons in the development of its legal framework for electronic transactions.

3. The Parties recognise the importance of facilitating the use of electronic transferable records. To this end, each Party shall endeavour to establish a legal framework governing electronic transferable records consistent with the UNCITRAL Model Law on Electronic Transferable Records 2017.

4. Except in circumstances otherwise provided for in its domestic law, neither Party shall deny the legal effect, legal validity or enforceability of an electronic contract, solely on the basis that the contract has been concluded by electronic means.

5. Recognising the importance of transparency for minimising barriers to digital trade, each Party shall maintain on a publicly accessible website a list of the circumstances referred to in paragraph 4.

6. With the aim of increasing the use of electronic contracts, each Party shall review its list referred to in paragraph 5 on an ongoing basis.

ARTICLE 8.61

Electronic Authentication

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

2. Neither Party shall adopt or maintain a measure that would:

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

(b) prevent parties to an electronic transaction from being able to prove to judicial and administrative authorities that the use of electronic authentication or an electronic signature in that transaction complies with the applicable legal requirements.

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

4. The Parties shall encourage the use of interoperable electronic authentication and work towards the mutual recognition of electronic authentication and electronic digital signatures.

5. To the extent provided for in its laws and regulations, each Party shall apply paragraphs 1 to 3 to electronic seals, electronic time stamps, or electronic registered delivery services.

6. To the extent provided for in its laws and regulations, each Party shall apply paragraph 1 to the authenticating data resulting from electronic authentication.

ARTICLE 8.61-A

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 take into account international frameworks when developing measures related to electronic invoicing, 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, where appropriate, on promoting the adoption of interoperable systems for electronic invoicing.

4. The Parties recognise the benefits of promoting, encouraging, supporting or facilitating the adoption of electronic invoicing by juridical persons. To this end, the Parties shall endeavour to promote the existence of policies, infrastructure or processes that support electronic invoicing.

ARTICLE 8.61-B

Paperless Trading

1. The Parties recognise the importance of digital connectivity in enabling trade. To this end, the Parties aim to facilitate cross-border supply chain digitalisation with a focus on interoperability.

2. Each Party shall make trade administration documents available to the public in electronic form and in English.

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

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

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

4. The Parties shall, where appropriate, cooperate bilaterally and in international fora on matters related to paperless trading, including by promoting the acceptance of electronic versions of trade administration documents and supporting documents.

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

ARTICLE 8.61-C

Logistics

1. The Parties recognise the importance of efficient cross-border logistics which help lower the cost and improve the speed and reliability of supply chains.

2. The Parties shall endeavour to share best practices and general information regarding the logistics sector, including:

(a) last mile deliveries, including on-demand and dynamic routing solutions;

(b) the use of electric, remote controlled and autonomous vehicles;

(c) facilitating the availability of cross-border options for the delivery of goods, such as parcel lockers; and

(d) new delivery and business models for logistics.

ARTICLE 8.61-D

Standards and Conformity Assessment

1. The Parties recognise the importance and contribution of standards, technical regulations and conformity assessment procedures in fostering a well-functioning digital economy, and further recognise their role in reducing barriers to trade by increasing compatibility, interoperability, and reliability.

2. The Parties shall endeavour to participate and cooperate or, where appropriate, encourage their respective bodies to participate and cooperate, in areas of mutual interest in international fora that both Parties are party to, to promote the development of standards relating to digital trade.

3. The Parties recognise that mechanisms that facilitate the cross-border recognition of conformity assessment results can support the digital economy.

4. To this end, the Parties shall endeavour or, where appropriate, encourage their respective bodies, in areas of mutual interest, to:

(a) exchange best practices relating to the development and application of standards, technical regulations and conformity assessment procedures that are related to the digital economy;

(b) participate actively in international fora that both Parties or their respective bodies are party to in order to develop standards that are related to digital trade and to promote their adoption;

(c) identify, develop, and promote joint initiatives in the field of standards and conformity assessment that are related to digital trade;

(d) actively consider the other Party's and its respective bodies' proposals for cooperation on standards, technical regulations and conformity assessment procedures relating to digital trade; and

(e) cooperate between governmental and non-governmental bodies, including cross-border research or test-bedding projects, to develop a greater understanding, between the Parties and industry, of standards, technical regulations and conformity assessment procedures.

5. The Parties acknowledge the importance of information exchange and transparency with regard to the preparation, adoption and application of standards, technical regulations and conformity assessment procedures for digital trade. Each Party should endeavour to, upon request, or where appropriate, encourage their respective bodies to provide information on standards, technical regulations and conformity assessment procedures relating to digital trade, in print or electronically, within a reasonable period of time agreed by the Parties and, if possible, within 60 days.

ARTICLE 8.61-E

Personal Information Protection

1. The Parties recognise the economic and social benefits of protecting the personal information of natural persons who are involved in digital trade, including electronic transactions, and the contribution that this makes to enhancing consumer confidence in the digital economy and the development of trade.

2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of personal information of natural persons who are involved in digital trade, including 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.[1]

3. The Parties agree that the key principles for its legal framework, which take into account the principles of relevant international bodies, shall 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 natural persons who are involved in digital trade, including electronic transactions, from personal information protection violations occurring within its territory.

5. Each Party shall publish information on the personal information protections it provides to natural persons who are involved in digital trade, including electronic transactions, including how:

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

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

---

[1] 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, or sector-specific laws covering data protection or privacy.

6. Recognising that the Parties may take different legal approaches to protecting personal information, each Party shall encourage the development and adoption of mechanisms to promote compatibility and interoperability between these different regimes. These mechanisms may include mutual arrangements, or broader international frameworks. The Parties recognise that in accordance with their respective laws and regulations, there are existing mechanisms, including contractual provisions, for the transfer of personal information between their respective territories.

7. The Parties shall endeavour to exchange information on how the mechanisms in paragraph 6 are applied in their respective territory and explore ways to extend these or other suitable arrangements to promote compatibility and interoperability between them.

ARTICLE 8.61-F

Cross-Border Transfer of Information by Electronic Means

1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.

2. Neither Party shall prohibit or restrict the cross-border transfer of information by electronic means, including personal information, if this activity is for the conduct of the business of a covered person.

3. Nothing in this Article shall prevent a Party from adopting or maintaining 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 8.61-G

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 8.61-H

Open Government Information

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

2. 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 Application Programming Interfaces ("APIs") and is regularly updated.

3. The Parties shall endeavour to cooperate to identify ways in which each Party can expand access to, and the use of, government information that the Party has made available to the public, with a view to enhancing and generating business and research opportunities, especially for small and medium-sized enterprises ("SMEs").

ARTICLE 8.61-I

Data Innovation

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

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

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

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

(c) sharing policy approaches and industry practices related to data sharing, such as data trusts.

ARTICLE 8.61-J

Commercial Information and Communication Technology Products that Use Cryptography

1. This Article applies to commercial ICT products that use cryptography. This Article does not apply to:

(a) a Party's law enforcement authorities requiring service suppliers using encryption to provide access to encrypted and unencrypted communications pursuant to that Party's legal procedures;

(b) the regulation of financial instruments;

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

(d) measures that a Party adopts or maintains pursuant to supervisory, investigatory or examination authority relating to financial service suppliers or financial markets; or

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

2. Neither Party shall require a manufacturer or supplier of a commercial ICT product that uses cryptography, as a condition of the manufacture, sale, distribution, import or use of the commercial ICT product, to:

(a) transfer or provide access to any proprietary information relating to cryptography, including by disclosing a particular technology or production process or other information, for example, a private key or other secret parameter, algorithm specification or other design detail, to that Party or a person in the territory of that Party;

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

(c) use or integrate a particular cryptographic algorithm.

3. This Article shall not preclude a regulatory body or judicial authority of a Party from requiring a manufacturer or supplier of a commercial ICT product that uses cryptography to:

(a) preserve and make available[1] any information to which paragraph 2(a) applies for an investigation, inspection, examination, enforcement action or a judicial proceeding, subject to safeguards against unauthorised disclosure; or

(b) transfer or provide access to any information to which paragraph 2(a) applies for the purpose of imposing or enforcing a remedy granted in accordance with that Party's competition law following an investigation, inspection, examination, enforcement action or a judicial proceeding.

4. For greater certainty, this Article does not affect the rights and obligations of a Party under Article 8.61-K (Source Code).

---

1 The Parties understand that this making available shall not be construed to negatively affect the status of any proprietary information relating to cryptography as a trade secret.

ARTICLE 8.61-K

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, including an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.

2. For greater certainty, paragraph 1 does not apply to the voluntary transfer of, or granting of access to, source code of software by a person of the other Party, including an algorithm expressed in that source code:

(a) on a commercial basis, such as in the context of a freely negotiated contract; or

(b) under open source licences, such as in the context of open source coding.

3. Nothing in this Article shall preclude a regulatory body or a judicial authority of a Party, or designated conformity assessment body, from requiring a person of the other Party to preserve and make available[1] the source code of software, including an algorithm expressed in that source code, for an investigation, inspection, examination, enforcement action or judicial proceeding, or the monitoring of compliance with codes of conduct and other standards, subject to safeguards against unauthorised disclosure.

4. Paragraph 1 does not apply to transfers of, or the granting of access to, source code of software, including an algorithm expressed in that source code, for the purpose of the imposition, adoption or enforcement of a remedy granted in accordance with that Party's law following an investigation, inspection, examination, enforcement action or judicial proceeding.

---

[1] The Parties understand that this making available shall not be construed to negatively affect the status of the source code of software, including an algorithm expressed in that source code, as a trade secret.

ARTICLE 8.61-L

Cyber Security

1. The Parties have a shared vision to promote secure digital trade to achieve global prosperity and recognise that threats to cyber security undermine confidence in digital trade. Accordingly, the Parties recognise the importance of:

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

(b) establishing or strengthening existing collaboration mechanisms to cooperate to anticipate, identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cyber security incidents;

(c) maintaining a dialogue on matters related to cyber security, including for the sharing of information and experiences for awareness and best practices;

(d) establishing mutual recognition of a baseline security standard for consumer Internet of Things devices to raise overall cyber hygiene levels and better secure cyberspace domestically;

(e) workforce development in the area of cyber security, including through possible initiatives relating to training and development; and

(f) collaborative cyber security research and development as well as innovation projects among academic, research and business entities.

2. Given the evolving nature of cyber security threats, the Parties recognise that risk-based approaches may be more effective than prescriptive, compliance-based approaches in addressing those threats. Accordingly, each Party shall encourage juridical persons within its territory to use risk-based approaches that rely on open and transparent industry standards to:

(a) manage cyber security risks and to detect, respond to, and recover from cyber security events; and

(b) otherwise improve the cyber security resilience of these juridical persons and their customers.

ARTICLE 8.61-M

Online Consumer Protection

1. The Parties recognise the importance of adopting and maintaining transparent and effective measures that contribute to consumer trust in digital trade.

2. To this end, each Party shall adopt or maintain measures that protect consumers engaged in digital trade, including laws and regulations that proscribe misleading, deceptive, fraudulent, and unfair commercial practices that cause harm or potential harm to consumers.

3. The Parties recognise the importance of, and where appropriate, shall promote cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to digital trade in order to enhance consumer welfare.

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

5. The Parties shall endeavour to explore the benefits of mechanisms, including alternative dispute resolution, to facilitate the resolution of disputes concerning digital trade.

ARTICLE 8.61-N

Unsolicited Commercial Electronic Messages

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

(a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or

(b) require the consent, as specified in the laws and regulations of that Party, of recipients to receive commercial electronic messages.

2. Each Party shall ensure that unsolicited commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are made, and to the extent provided for in a Party's laws and regulations, contain the necessary information to enable end-users to request cessation free of charge and at any time.

3. Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained 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 8.61-O

Safety and Security Online

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

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

3. The Parties shall endeavour to cooperate to advance collaborative solutions to global issues affecting online safety and security, including in international fora.

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

ARTICLE 8.61-P

Digital Inclusion

1. The Parties recognise the importance of digital inclusion, that all people and businesses can participate in, contribute to, and benefit from the digital economy. To this end, the Parties recognise the importance of expanding and facilitating opportunities in the digital economy by removing barriers to participation in the digital economy, and that this may require tailored approaches, developed in consultation with juridical persons, individuals and other groups that disproportionately face such barriers. The Parties also recognise the importance of adopting or maintaining labour policies that promote decent conditions of work for workers who are engaged in or support the digital economy, in accordance with each Party's laws and regulations.

2. The Parties shall cooperate on matters relating to digital inclusion, including the participation of women and other groups and individuals that may disproportionately face barriers to digital trade. Such cooperation may include:

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

(b) identifying and addressing barriers in accessing digital trade opportunities;

(c) sharing methods and procedures for developing datasets and conducting analysis in relation to the participation in digital trade by women and other groups that may disproportionately face barriers to participation in the digital economy;

(d) improving digital skills and access to online business tools;

(e) promoting labour protection for workers who are engaged in or support digital trade; and

(f) other areas as jointly agreed by the Parties.

3. Cooperation activities relating to digital inclusion may be carried out through the coordination, as appropriate, of the Parties' respective agencies and stakeholders.

4. The Parties also recognise the digital divide between countries, and the role for digital trade in promoting economic development and poverty reduction. To that end, the Parties shall endeavour to undertake and strengthen cooperation, including through existing mechanisms, to promote the participation in digital trade of countries who face barriers to such participation. This may include sharing best practices, collaborating on capacity building initiatives, active engagement in international fora and promoting countries' participation in, and contribution to, the global development of rules on digital trade.

5. The Parties shall also participate actively at the WTO and in other international fora to promote initiatives for advancing digital inclusion in digital trade.

ARTICLE 8.61-Q

Small and Medium-sized Enterprises

1. The Parties recognise the fundamental role played by SMEs in economic growth and job creation, and the need to address the barriers to participation in the digital economy for such entities. To this end, the Parties shall, subject to their available resources, seek opportunities to:

(a) promote close cooperation on digital trade between SMEs of the Parties and cooperate in promoting jobs and growth for SMEs;

(b) encourage SMEs participation in platforms that help link SMEs with international suppliers, buyers and other potential business partners; and

(c) exchange information and share best practices in improving digital skills and leveraging digital tools and technology to improve access to capital and credit, participation in government procurement opportunities, and other areas that could help SMEs adapt to digital trade.

2. The Parties recognise the integral role played by the private sector in the Parties' implementation of this Article.

ARTICLE 8.61-R

Artificial Intelligence and Emerging Technologies

1. The Parties recognise that artificial intelligence ("AI") and emerging technologies, including distributed ledger technologies, digital twins, immersive technologies and the Internet of Things, play important roles in promoting economic competitiveness and facilitating international trade and investment flows, and may require coordinated action across multiple trade policy areas to maximise their economic and social benefits. The Parties also recognise that the use and adoption of AI technologies are becoming increasingly important within a digital economy offering significant social and economic benefits.

2. The Parties shall endeavour, where appropriate, to develop governance and policy frameworks that take into account relevant international principles and guidelines, for the ethical, trusted, safe and responsible development and use of AI and emerging technologies, and that will help realise the benefits of these technologies. To this end, in developing such frameworks, the Parties recognise the importance of:

(a) taking into account the principles and guidelines of relevant international bodies;

(b) utilising risk-based approaches to regulation that are based on industry-led standards and risk management best practices; and

(c) having regard to the principles of technological interoperability and technological neutrality.

3. The Parties shall endeavour, where appropriate, to cooperate on matters related to AI and emerging technologies with respect to digital trade, including their cross-border deployment. Such cooperation may include:

(a) exchanging information and sharing experiences and best practices on research and industry activities, laws, regulations, policies, enforcement and compliance and promoting interoperability between international AI governance frameworks;

(b) cooperating on issues and developments relating to AI and emerging technologies, such as ethical use, human diversity and unintended biases, industry-led technical standards and algorithmic transparency;

(c) promoting collaboration between each Party's governmental and non-governmental entities across research, academia, and industry, in relation to:

(i) research and development opportunities;

(ii) joint deployment and test-bedding opportunities;

(iii) opportunities for investment in and commercialisation of AI and emerging technologies; and

(iv) responsible use and adoption of AI technologies; and

(d) participating actively in international fora, such as the Global Partnership on Artificial Intelligence, on matters concerning the interaction between trade and AI and emerging technologies.

ARTICLE 8.61-S

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 and interoperability between their respective digital identity regimes.

2. To this end, the Parties shall endeavour to facilitate initiatives to promote such compatibility and interoperability, 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) identifying and 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 8.61-T

Lawtech Cooperation

1. The Parties recognise the increasing importance of Lawtech to the Parties' respective legal services markets, and the benefits of expanding the mutual understanding of their respective Lawtech markets. To that end, the Parties shall endeavour to cooperate, as appropriate, including by:

(a) establishing a dialogue on matters related to Lawtech, which may include the sharing of knowledge, research, industry practice, and information relating to relevant legal and regulatory frameworks;

(b) encouraging the sharing of knowledge between their respective regulators, academics, representative bodies and industry bodies; and

(c) encouraging service suppliers supplying Lawtech services to explore new business opportunities in the other Party's territory.

2. The Parties acknowledge the significant role that legal services play in society. In view of this, the Parties recognise the value of encouraging the trusted, safe and responsible use of Lawtech within the principles that underpin their respective legal and regulatory systems.

ARTICLE 8.61-U

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, 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; and

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

2. The Parties shall endeavour to cooperate, where practicable, on issues of competition law enforcement in digital markets between their respective authorities, including through notification, consultation and the exchange of information.

3. Any cooperation under paragraphs 1 and 2 shall be in a manner compatible with each Party's domestic law and important interests, and within their available resources.

ARTICLE 8.61-V

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, and industry. 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 Section and other relevant articles in this Agreement.

ARTICLE 8.61-W

Cooperation

1. The Parties shall, as appropriate, cooperate and participate actively in international fora, including the WTO, to promote the development of international frameworks for digital trade.

2. The Parties shall endeavour to:

(a) exchange information and share experiences and best practices on regulatory matters relating to the digital economy, including:

(i) personal information protection;

(ii) data governance;

(iii) cross-border data flows;

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

(v) unsolicited commercial electronic messages;

(vi) electronic contracts;

(vii) electronic trust and electronic authentication services;

(viii) digital identities;

(ix) digital trade facilitation;

(x) AI and other emerging technology; and

(xi) digital government;

(b) encourage industry, as appropriate, to develop methods of self-regulation that foster the digital economy, including codes of conduct, model contracts, guidelines and enforcement mechanisms; and

(c) exchange information and share best practices on simplified customs procedures applied to expedited shipments.

ARTICLE 8.61-X

Security, Prudential Carve-out and General Exceptions

Further to Article 8.62 (General Exceptions), this Section is subject to the exceptions provided for in Article 2.14 (General Exceptions), and, for greater certainty, the relevant provisions of this Chapter including Article 8.50 (Prudential Carve-out), and Chapter Sixteen (Institutional, General and Final Provisions).

ANNEX B

The Incorporated Agreement shall be amended as follows:

Amendments to Chapter Six (Customs and Trade Facilitation)

1. Article 6.13 (Single Window) shall be replaced by the following:

"ARTICLE 6.13

Single Window

Each Party shall adopt or maintain single window systems enabling traders to submit documentation or information required for the exportation, importation and transit of goods through a single entry point to the participating authorities or agencies."

Amendments to Chapter Eight (Services, Establishment and Electronic Commerce)

2. The title of Chapter Eight (Services, Establishment and Electronic Commerce) shall be substituted with "Services, Establishment and Digital Trade and the Digital Economy", and all such further reference in the Incorporated Agreement shall be read accordingly.

3. In paragraph 1 of Article 8.1 (Objective and Scope), the words "electric commerce" shall be substituted with "digital trade and the digital economy".

4. Article 8.38 (Submarine Cable Landing Stations) shall be replaced by the following:

"ARTICLE 8.38

Submarine Cable Landing Stations and Cable Systems

1. The Parties recognise the importance of submarine cable landing stations and cable systems, and the expeditious and efficient installation, maintenance and repair of these systems, to national, regional and global telecommunications connectivity.

2. Each Party shall ensure access to submarine cable landing stations and cable systems in its territory, where a supplier is authorised to operate a submarine cable system as a public telecommunications service, on reasonable, non-discriminatory and transparent terms and conditions.

3. Each Party may mitigate the risk of damage to submarine cable landing stations and cable systems in its territory that are operated, owned or controlled by a person of the other Party, which may include measures to maintain the functionality of the cable system.

4. The Parties shall endeavour to cooperate on submarine cable landing stations and cable systems to further the mutual interests of the Parties in this area."

5. Article 8.49 (Scope and Definitions) shall be replaced by the following:

"ARTICLE 8.49

Scope and Definitions

1. This Sub-Section sets out the principles of the regulatory framework for all financial services liberalised pursuant to Sections B (Cross-border Supply of Services), C (Establishment) and D (Temporary Presence of Natural Persons for Business Purposes).

2. For the purposes of this Sub-Section:

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

(b) "financial service" means any service of a financial nature, including a service incidental or auxiliary to a service of a financial nature, offered by a financial service supplier of a Party; financial services include the following activities:

(i) insurance and insurance-related services:

(1) direct insurance (including co-insurance):

(aa) life insurance;

(bb) non-life insurance;

(2) reinsurance and retrocession;

(3) insurance inter-mediation, such as brokerage and agency; and

(4) services auxiliary to insurance, such as consultancy, actuarial, risk assessment and claim settlement services;

and

(ii) banking and other financial services (excluding insurance):

(1) the acceptance of deposits and other repayable funds from the public;

(2) lending of all types, including consumer credit, mortgage credit, factoring and financing of commercial transaction;

(3) financial leasing;

(4) all payment and money transmission services, including credit, charge and debit cards, travellers cheques and bankers drafts;

(5) guarantees and commitments;

(6) the trading on own account or for the account of customers, whether on an exchange, in an over-the-counter market or otherwise, of the following:

(aa) money market instruments (including cheques, bills, certificates of deposits);

(bb) foreign exchange;

(cc) derivative products including, but not limited to, futures and options;

(dd) exchange rate and interest rate instruments, including products such as swaps, forward rate agreements;

(ee) transferable securities;

(ff) other negotiable instruments and financial assets, including bullion;

(7) the participation in issues of securities of all kinds, including underwriting and placement as agent, whether publicly or privately, and provision of services related to such issues;

(8) money broking;

(9) asset management, such as cash or portfolio management, any form of collective investment management, pension fund management, custodial, depository and trust services;

(10) settlement and clearing services for financial assets, including securities, derivative products, and other negotiable instruments;

(11) the provision and transfer of financial information, and the provision of financial data processing and related software by suppliers of other financial services; and

(12) advisory, intermediation and other auxiliary financial services on all the activities listed in subparagraphs (1) to (11), including credit reference and analysis, investment and portfolio research and advice, advice on acquisitions and on corporate restructuring and strategy;

(c) "financial service computing facility" means a computer server or storage device for the processing or storage of information relevant for the conduct of the ordinary business of a financial service supplier;

(d) "financial service supplier" means any natural or juridical person of a Party that is engaged or is seeking to engage in the business of supplying financial services within the territory of that Party but does not include a public entity;

(e) "new financial service" means a service of a financial nature, including services related to existing and new products or the manner in which a product is delivered, that is not supplied by any financial service supplier in the territory of a Party but which is supplied in the territory of the other Party;

(f) "public entity" means:

(i) a government, central bank or monetary authority of a Party, or an entity owned or controlled by a Party, that is principally engaged in carrying out governmental functions or activities for governmental purposes, other than an entity principally engaged in supplying financial services on commercial terms; or

(ii) a private entity, performing functions normally performed by a central bank or monetary authority, when exercising those functions; and

(g) "self-regulatory organisation" means any non-governmental body, including any securities or futures exchange or market, clearing agency, or other organisation or association, that exercises regulatory or supervisory authority over financial service suppliers by statute or delegation from central, regional or local governments or authorities."

6. Article 8.53 (New Financial Services) shall be replaced by the following:

"ARTICLE 8.53

New Financial Services[1]

1. Each Party shall permit a financial service supplier of the other Party to supply any new financial service that the first Party would permit its own like financial service suppliers to supply without additional legislative action required by the first Party. Each Party may determine the institutional and juridical form through which the new financial service may be supplied and may require authorisation for the supply of the service. Where a Party requires such authorisation, a decision shall be made within a reasonable time and the authorisation may only be refused for prudential reasons under Article 8.50 (Prudential Carve-out).

2. To support innovation in financial services, the Parties shall endeavour to collaborate, share knowledge, experiences and developments in financial services, in areas such as, but not limited to: FinTech and RegTech,[2] advancing financial integrity, consumer protection, financial inclusion, financial stability, operational resilience, sustainability and facilitating cross-border development of new financial services."

---

1 Nothing in this Article shall be construed as preventing a financial service supplier of a Party from applying to the other Party to request that it authorises the supply of a financial service that is not supplied in the territory of either Party. That application shall be subject to the domestic law of the Party to which the application is made and, for greater certainty, shall not be subject to this Article.

2 For the purposes of this Article, the Parties shall treat "FinTech and RegTech" as referring to activities which involve the improved use of technology across financial services.

7. Article 8.54 (Data Processing) shall be replaced by the following:

"ARTICLE 8.54

Financial Information

1. Neither Party shall, subject to appropriate safeguards on privacy and confidentiality, prohibit or restrict a financial service supplier of the other Party from transferring information in electronic or other form, into and out of its territory, where such transfer is required in the ordinary course of business of such financial service supplier.

2. Subject to paragraph 3 and to appropriate safeguards on privacy and confidentiality, it is prohibited for either Party to require, as a condition for conducting business in the Party's territory, a financial service supplier of the other Party to use or locate financial service computing facilities, in the former Party's territory.[1]

3. Each Party shall have the right to require a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory, where it is not able to ensure appropriate[2] access to information required for the purposes of financial regulation and supervision, provided that the following conditions are met:

(a) to the extent practicable, the Party provides a financial service supplier of the other Party with a reasonable opportunity to remediate any lack of access to information; and

---

1 For greater certainty, this prohibition also applies to circumstances in which a financial service supplier of the other Party uses the services of an external business for such use, storage or processing of information.

2 For greater certainty, "appropriate" access may include sufficient and timely access that is provided without undue delay.

(b) the Party or its regulatory authorities consult the other Party or its regulatory authorities before imposing any requirements on a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory.

4. Each Party shall adopt or maintain appropriate safeguards to protect privacy and personal data, including individual records and accounts, as long as these safeguards are not used to circumvent the provisions of this Agreement."

8. After Article 8.54 (Data Processing), insert the following:

"ARTICLE 8.54-A

Electronic Payments

1. Noting the rapid growth of electronic payments, in particular those provided by non-banks and FinTech enterprises, the Parties recognise, subject to maintaining resilience, the importance of developing an efficient, safe and secure environment for cross-border electronic payments, including by:

(a) encouraging 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 endeavour, subject to maintaining resilience, to:

(a) make regulations on electronic payments, including in relation to regulatory approval, licensing requirements, procedures and technical standards, publicly available, where to do so does not prejudice the security or integrity of a financial service supplier;

(b) for the electronic payment systems solely operated by either Party, publicly disclose objective and risk-based criteria for participation which promote fair and open access;

(c) adopt, for relevant electronic payment systems, international standards for electronic payment messaging, payment service providers and services suppliers to enable greater interoperability between electronic payment systems;

(d) encourage payment service providers to safely and securely make available new technologies and standards for their financial products and services available to third parties, and where possible, to facilitate greater interoperability, innovation and competition in electronic payments; and

(e) 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 and cooperation at international fora.

3. In view of paragraph 1, the Parties recognise the importance of upholding safety, efficiency, trust and security in electronic payment systems through laws and regulations, and that the adoption and enforcement of laws, regulations and policies should be proportionate to the risks undertaken by the payment service providers."