[X]. Chapter Seven (Trade in Services, Establishment and Electronic Commerce) is hereby replaced with the following:

"CHAPTER SEVEN-F

DIGITAL TRADE

ARTICLE 7F.1

Objectives

1. The Parties recognise the economic benefits of, and opportunities provided by, open 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 domestic frameworks to facilitate digital trade;

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

(d) adopting international and domestic frameworks that:

(i) take into account emerging technologies; and

(ii) advance the interests of consumers and businesses engaged in digital trade, while promoting consumer confidence in it.

ARTICLE 7F.2

Scope and General Provisions

1. This Chapter shall apply to a measure of a Party affecting trade enabled by electronic means.

2. This Chapter shall not apply to government procurement.

3. This Chapter shall not apply to information held or processed by or on behalf of a Party, or measures related to that information, including measures related to its collection, except for Article 7F.16.

4. For greater certainty, a measure affecting the supply of a service delivered or performed electronically is subject to the obligations contained in the relevant provisions of

Chapter Seven-A (Cross-Border Trade in Services), Chapter Seven-B (Investment), and Chapter Seven-D (Financial Services), including any exceptions set out in this Agreement that are applicable to those obligations.

ARTICLE 7F.3

Definitions

For the purposes of this Chapter:

central level of government means central level of government, as defined in Article 7A.2 (Definitions);

computing facility means a computer server or storage device for processing or storing information for commercial use;

covered person means:

(a) a covered investment, as defined in Article 7B.2 (Definitions);

(b) an investor of a Party, as defined in Article 7B.2 (Definitions), but does not include an investor in a financial institution[1]; or

(c) a service supplier of a Party, as defined in Article 7A.1 (Definitions),

but does not include a financial service supplier, financial institution, or cross-border financial service supplier of a Party, as defined in Article 7D.2 (Definitions);

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

electronic invoicing or **e-invoicing** means the automated creation, processing, and exchange of an invoice between a seller and a buyer using a structured digital format;

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

electronic transmission means a transmission made using any electromagnetic means and includes the content of the transmission;

[1] For greater certainty, an investor in a financial institution may still be a "covered person" in relation to other investments that are not in a financial institution.

end-user means a person who purchases or subscribes to an Internet access service from an Internet access service supplier;

enterprise means an enterprise, as defined in Article 7A.2 (Definitions);

measure means a measure, as defined in Article 7A.2 (Definitions);

measure of a Party means a measure adopted or maintained by a Party, as defined in Article 7A.2 (Definitions);

person means an individual or an enterprise;

person of a Party means a national or an enterprise of a Party, as defined in Article 7A.2 (Definitions);

personal information means any information, including data, about an identified or identifiable individual;

public telecommunications service means a public telecommunications service, as defined in Article 7E.2 (Definitions);

trade administration document means a form or a document 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 a good; and

unsolicited commercial electronic message means an electronic message[2] that is sent for commercial or marketing purposes directly to an individual or enterprise, via a public telecommunications service, without the consent of the recipient or despite the explicit rejection of the recipient.

ARTICLE 7F.4

Customs Duties

1. A Party shall not impose a customs duty on an electronic transmission between a person of a Party and a person of the other Party.

2. For greater certainty, paragraph 1 does not preclude a Party from imposing internal taxes, fees, or other charges on an electronic transmission, provided that those taxes, fees, or charges are imposed in a manner consistent with this Agreement.

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

ARTICLE 7F.5

Domestic Electronic Transactions Framework

1. Each Party shall maintain a legal framework governing electronic transactions consistent with the principles of the *United Nations Commission on International Trade Law* (hereinafter referred to as "UNCITRAL") *Model Law on Electronic Commerce (1996),* adopted by the United Nations General Assembly on 12 June 1996, or the *United Nations Convention on the Use of Electronic Communications in International Contracts,* done at New York on 23 November 2005.

2. Each Party shall endeavour to:

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

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

3. The Parties recognise the importance of facilitating the use of electronic transferable records. To this end, each Party shall endeavour to adopt or maintain a legal framework governing electronic transferable records consistent with the general principles of the *UNCITRAL Model Law on Electronic Transferable Records (2017),* adopted by UNCITRAL on 13 July 2017.

ARTICLE 7F.6

Conclusion of Contracts by Electronic Means

1. Except in circumstances otherwise provided for in its law, a Party shall not deny the legal effect, legal validity, or enforceability of an electronic contract[3] solely on the basis that the contract has been made by electronic means and shall endeavour to ensure that its legal framework does not create obstacles for the use of electronic contracts solely on the basis that the contract has been made by electronic means.

2. The Parties recognise the importance of transparency for minimising barriers to the use of electronic contracts in digital trade. Further, each Party recognises the benefits of reducing the circumstances referred to in paragraph 1 over time, and to that end shall endeavour to continue to review those circumstances.

[3] For greater certainty, an electronic contract includes a contract made by interaction with an automated message system.

Article 7F.7

Electronic Authentication and Electronic Signatures[4]

1. The Parties recognise the benefits of electronic authentication and electronic signatures in providing greater certainty, integrity, and efficiency. Accordingly, the Parties recognise the important contribution of electronic authentication and electronic signatures to consumer and business trust in the digital economy.

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

3. A Party shall not adopt or maintain a measure that would:

(a) prohibit parties to an electronic transaction from mutually determining the appropriate electronic authentication method or electronic signature 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 electronic authentication or electronic signature.

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

5. To the extent provided for under its laws and regulations, each Party shall apply paragraphs 2 through 4 to electronic seals, electronic time stamps, and electronic registered delivery services.

6. The Parties:

(a) shall encourage the use of interoperable electronic authentication;

(b) may work towards, on a voluntary basis, the mutual recognition of electronic signatures; and

(c) may endeavour to engage in regulatory cooperation relating to electronic signatures and electronic authentication.

---

[4] For greater certainty, nothing in this Article 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.

ARTICLE 7F.8

Digital Identities

1. While a Party may take different legal and technical approaches to digital identities, the Parties recognise that cooperation on digital identities will increase regional and global connectivity. Accordingly, the Parties shall pursue 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 compatibility and interoperability, which may include:

(a) fostering technical interoperability between each Party's implementation of digital identities;

(b) developing comparable protection of digital identities under each Party's respective law;

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

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

ARTICLE 7F.9

Paperless Trading

1. Each Party shall make trade administration documents available to the public in electronic form.

2. To the extent practicable, each Party shall provide electronic versions of trade administration documents referred to in paragraph 1 in English.

3. Each Party shall accept a trade administration document submitted electronically as the legal equivalent of the paper version of that document, unless:

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

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

4. The Parties shall, if 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.

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

ARTICLE 7F.10

E-Invoicing

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

2. Each Party shall endeavour to ensure that the implementation of any measure 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 any measure related to electronic invoicing.

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

ARTICLE 7F.11

Open Internet Access

Subject to its applicable policies, laws, and regulations, each Party shall endeavour to ensure that an end-user in its territory may:

(a) access and use a service or application of the end-user's choice available on the Internet, subject to reasonable, transparent, and non-discriminatory network management[5];

(b) connect a device of the end-user's choice to the Internet, provided that this device does not harm the network; and

(c) access information on the network management practices of the end-user's Internet access service supplier.

[5] The Parties recognise that an Internet access service supplier that offers its subscribers certain content without counting the associated data toward their data allowances would not be acting contrary to this obligation.

ARTICLE 7F.12

Personal Information Protection

1. The Parties recognise the importance of high standards of personal information protection and that protecting personal information provides economic and social benefits which enhance consumer confidence and trust in digital trade.

2. Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of individuals.

3. In the development of its legal framework for the protection of personal information, each Party shall take into account principles and guidelines of relevant international bodies. The principles underpinning each Party's personal information protection framework shall include:

(a) collection and usage limitation;

(b) data quality;

(c) purpose specification;

(d) security safeguards;

(e) transparency;

(f) individual participation; and

(g) accountability.

4. Each Party shall adopt or maintain non-discriminatory practices in protecting individuals from personal information protection violations occurring within its jurisdiction.

5. Each Party shall publish information on the personal information protections it provides to individuals, including how:

(a) an individual can pursue remedies or recourse; and

(b) a business can comply with any legal requirements.

6. Recognising that the Parties may take different legal approaches to protecting personal information, each Party shall promote compatibility between their respective legal frameworks for protecting personal information and pursue the development of mechanisms to promote interoperability between these frameworks. 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 exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote interoperability and compatibility between them.

ARTICLE 7F.13

Location of Computing Facilities

1. A Party shall not require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

2. Nothing in this Article prevents a Party from adopting or maintaining a measure inconsistent with paragraph 1 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 a restriction on the use or location of computing facilities greater than is required to achieve the objective.

ARTICLE 7F.14

Cross-Border Transfer of Information by Electronic Means

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

2. A Party shall not prohibit or restrict the cross-border transfer of information by electronic means, including personal information, if this activity is for the conduct of the business of a covered person.

3. Nothing in this Article prevents 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 a restriction on transfers of information greater than is required to achieve the objective.

ARTICLE 7F.15

Data Innovation

1. The Parties recognise that data innovation promotes economic and societal benefits through improved data-driven services and technologies. Accordingly, the Parties recognise the importance of creating an environment that enables, supports, and is conducive to,

experimentation and innovation, while also acknowledging the need to protect personal information.

2. To this end, the Parties shall endeavour to support data innovation, including through:

(a) collaborating on data-sharing projects, including projects involving researchers, academia or industry, using regulatory sandboxes as required;

(b) cooperating on the development of policies and standards for data portability; and

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

ARTICLE 7F.16

Open Government Information

1. For the purposes of this Article, **government information** means information held by the central level of government, if disclosure of that information is not restricted under domestic law.[6]

2. The Parties recognise that facilitating public access to and use of government information fosters economic and social development, competitiveness, and innovation. To this end, each Party is encouraged to expand the coverage of government information digitally available for public access and use, through engagement and consultation with interested stakeholders.

3. Each Party shall endeavour to provide interested persons of a Party with a mechanism to request the disclosure of specific government information.

4. To the extent that a Party chooses to make government information digitally available for public access and use, it shall endeavour to ensure that the information is:

(a) in a machine-readable and open format, and can be searched, retrieved, used, reused, and redistributed;

(b) accompanied by metadata that is, to the extent possible, based on commonly used formats that allow the user to understand and utilise the data; and

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

[6] For greater certainty, this Article is without prejudice to a Party's laws pertaining to intellectual property and personal information protection.

5. To the extent that a Party chooses to make government information digitally available to the public, it shall endeavour to avoid imposing a condition[7] that unduly prevents or restricts a user of that information from:

(a) reproducing, redistributing, or republishing the information;

(b) regrouping the information; or

(c) using the information for commercial and non-commercial purposes, including in the process of production of a new product or service.

6. 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 research and business opportunities, especially for small and medium-sized enterprises ("SMEs").

ARTICLE 7F.17

Online Consumer Protection

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

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

3. While recognising that the form of protection may be different as between online and other forms of commerce, each Party shall provide a consumer engaged in online commercial activities with a level of protection that is, in its effect, not less than that provided under its law to a consumer engaged in other forms of commerce.[8]

4. The Parties recognise the importance of online consumer protection and, as appropriate, shall promote cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to online consumer protection.

5. The Parties further recognise the importance of improving awareness of, and access to, policies and procedures related to consumer protection, including consumer redress mechanisms, including for consumers from one Party transacting with suppliers from the other Party.

[7] For greater certainty, nothing in this paragraph prevents a Party from requiring a user of that information to link to original sources.

[8] For greater certainty, this paragraph shall not be construed to require a Party to compensate for any inherent competitive disadvantages which result from the online character of online commercial activities.

6. The Parties shall endeavour to explore the benefits of mechanisms, including alternative dispute resolution, to facilitate the resolution of claims concerning online commercial activities.

ARTICLE 7F.18

Unsolicited Commercial Electronic Messages

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

(a) require a supplier of unsolicited commercial electronic messages to facilitate the ability of a recipient[9] to prevent ongoing reception of those messages; or

(b) require the consent, as specified according to its laws and regulations, of a recipient to receive a commercial electronic message.

2. Each Party shall require that a supplier of unsolicited commercial electronic messages ensures that an unsolicited commercial electronic message is clearly identifiable as such, clearly discloses on whose behalf it is made, and contains the necessary information to enable a recipient to request cessation free of charge and at any time.

3. Each Party shall provide access to redress or recourse against a supplier of an unsolicited commercial electronic message that does not comply with a measure adopted or maintained pursuant to 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 7F.19

Source Code

1. A Party shall not 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. Nothing in paragraph 1 shall be construed to:

(a) preclude a regulatory authority, law enforcement body, or judicial body of a Party, or a conformity assessment body of a Party or designated by a Party, from requiring a person of the other Party to preserve and make available the source code of software in furtherance of an investigation, inspection,

[9] For the purpose of this Article, measures adopted or maintained by the UK in relation to recipients apply to individuals, and to enterprises to the extent provided for in the UK's laws and regulations. Measures adopted or maintained by Korea in relation to recipients apply to individuals and enterprises.

examination, enforcement action, administrative or judicial proceeding subject to safeguards against unauthorised disclosure; or

(b) apply to a remedy imposed, enforced, or adopted by a regulatory body or a judicial authority of a Party, in accordance with a Party's competition law, following an investigation, inspection, examination, enforcement action, or administrative or judicial proceeding.

3. 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 on a commercial basis, such as in the context of a freely negotiated contract.

ARTICLE 7F.20

Cyber Security

1. The Parties recognise that threats to cyber security undermine confidence in digital trade. The Parties also recognise the importance of:

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

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

2. The Parties shall endeavour to:

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

(b) maintain cooperation to anticipate, identify, and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks in the Parties' respective territories, and to swiftly address cyber security incidents; and

(c) cooperate by sharing information and best practices on matters related to cyber security.

3. Given the evolving nature of cyber security threats, the Parties recognise the importance of risk-based approaches in addressing those threats. Accordingly, to identify and protect against cyber security risks, to detect cyber security events, to respond to and recover from cyber security incidents, and to improve their cyber resilience, each Party shall endeavour to use, and shall encourage enterprises within its jurisdiction to use, risk-based approaches that rely on risk management best practices and on standards developed in a consensus-based, transparent, and open manner.

ARTICLE 7F.21

Artificial Intelligence

1. The Parties recognise that artificial intelligence (hereinafter referred to as "AI") plays an important role in promoting economic growth, particularly by bolstering international trade and investment flows.

2. The Parties recognise the economic and social importance of developing governance and policy frameworks for the trusted, safe, secure and human-centric use of AI technologies. In view of the cross-border nature of the digital economy, the Parties further acknowledge the benefits of developing mutual understanding and ultimately ensuring that such frameworks are interoperable as far as appropriate, in order to facilitate the adoption and use of AI technologies across the Parties' respective jurisdictions.

3. To this end, the Parties shall endeavour to promote governance and policy frameworks that support the trusted, safe, secure, and human-centric use of AI technologies. In promoting those frameworks, the Parties recognise the importance of regulation that is based on technical standards and best practices, and of having regard to the principle of technological interoperability.

4. In adopting AI governance and policy frameworks, the Parties shall endeavour to take into consideration internationally recognised principles or guidelines, including explainability, transparency, safety, security, accountability, fairness and human-centred values.

5. In view of the cross-border nature of the digital economy and the benefits of developing mutual understanding, minimising barriers to trade, and ultimately ensuring that governance and policy frameworks are compatible and interoperable as far as appropriate, the Parties may take action to improve such compatibility and interoperability, which may include cooperation.

6. The Parties shall endeavour to cooperate on matters related to AI with respect to digital trade. That cooperation may include:

(a) exchanging information and sharing experiences and best practices on laws, regulations, policies, enforcement, and compliance;

(b) cooperating on issues or developments relating to unintended biases and technical standards;

(c) promoting collaboration between each Party's governmental and non-governmental entities in relation to AI research and development and investment opportunities; and

(d) playing an active role in international fora in:

(i) supporting the development of international technical standards, regulations, and conformity assessment procedures that support the growth of AI; and

(ii) matters concerning the interaction between trade and AI.

7. In view of the cross-border nature of the digital economy and the benefits of facilitating the adoption and use of AI technologies across the Parties' respective jurisdictions, the Trade Committee may, pursuant to Articles 15.1.4(c) and 15.1.4(e), consider or recommend amendments to this Article, with a view to, among other things, improving compatibility and interoperability of the Parties' respective AI governance frameworks.

ARTICLE 7F.22

Digital Inclusion

1. The Parties recognise the importance of digital inclusion, so that all people and businesses can participate in, contribute to, and benefit from digital trade. To this end, the Parties recognise the importance of expanding and facilitating digital trade opportunities by removing barriers to participation in digital trade.

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

(a) identifying and addressing barriers in accessing digital trade opportunities including challenges associated with connectivity;

(b) sharing methods and procedures for developing datasets, and conducting gender-focused analysis in relation to digital trade policies, including by developing methods for monitoring women's participation in digital trade;

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

(d) other cooperation activities as the Parties may decide.

3. The Parties recognise the role played by SMEs, including women-led enterprises, in economic growth and job creation, and the need to address the barriers to participation in digital trade for those entities. To this end, the Parties shall endeavour to:

(a) exchange information and share best practice in leveraging digital tools and technologies to improve access to capital and credit and the capabilities and market reach of SMEs;

(b) 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

(c) promote cooperation on digital trade between SMEs of the Parties.

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

ARTICLE 7F.23

Environmental Sustainability

1. The Parties recognise the existing and the potential future links between digital trade and environmental sustainability, and the importance of policies to maximise the positive impacts of digital trade while addressing negative impacts.

2. To this end, the Parties shall endeavour to cooperate on environmental aspects of digital trade. That cooperation may include evaluating the mutual impacts between digital trade and the environment, and identifying ways to enhance, prevent, or mitigate those impacts.

3. The Parties shall also actively participate in international fora to promote initiatives related to addressing the links between environmental sustainability and digital trade.

ARTICLE 7F.24

Cooperation

1. The Parties recognise the fast-paced and evolving nature of digital trade, and the role of cooperation between the Parties in increasing and enhancing opportunities for businesses, consumers, and society.

2. In addition to areas of cooperation between the Parties identified in other parts of this Chapter, the Parties shall exchange information on, and share experiences and best practices on, laws, regulations, policies, enforcement, and compliance relating to digital trade.

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

4. The Parties shall encourage the development, by the private sector, of methods of self-regulation that foster digital trade, including codes of conduct, model contracts, guidelines, and compliance mechanisms."