DIGITAL ECONOMY AGREEMENT

BETWEEN

THE EFTA STATES

AND

THE REPUBLIC OF SINGAPORE

Amending the Agreement between the EFTA States and Singapore

PREAMBLE

Iceland, the Principality of Liechtenstein, the Kingdom of Norway, and the Swiss Confederation (hereinafter referred to as the "EFTA States"),

and

the Republic of Singapore (hereinafter referred to as "Singapore"),

hereinafter collectively referred to as the "Parties",

RECOGNISING their deep and longstanding relationship, underpinned by the Agreement between the EFTA States and Singapore, done at Egilsstadir, Iceland, on 26 June 2002 (hereinafter referred to as the "Free Trade Agreement" or, in Annex I and Annex II, "this Agreement");

REFLECTING their shared vision for greater integration and the digital transformation of their economies and commitment to deepen cooperation in new and emerging areas;

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

ACKNOWLEDGING the importance of the digital economy and that ongoing economic growth depends on their combined ability to harness technological advances to improve existing businesses and create new products and markets;

CONVINCED that the following Digital Economy Agreement will further enhance the competitiveness of their enterprises in global markets and create additional conditions encouraging trade and investment relations between the Parties;

RECOGNISING the role of standards, in particular open standards, in facilitating interoperability between digital systems and enhancing value-added products and services;

RECOGNISING the importance of ensuring that all persons and businesses of all sizes, including small and medium-sized enterprises (hereinafter referred to as "SMEs"), can participate in, contribute to, and benefit from the digital economy;

RECOGNISING their interdependence on matters relating to the digital economy and, as leading online economies, their shared interest in protecting critical infrastructure and ensuring a safe and reliable Internet that supports innovation and economic and social development;

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

REAFFIRMING the right to regulate in the area of digital trade in conformity with the following Digital Economy Agreement to achieve legitimate policy objectives;

REAFFIRMING their commitment to pursue the objective of sustainable development and acknowledging the role of digital trade in harnessing the contribution of international trade to the promotion of sustainable development;

DETERMINED to promote and further strengthen the multilateral trading system, building on their respective rights and obligations under the Marrakesh Agreement Establishing the World Trade Organization and the other agreements negotiated thereunder and on their undertakings in the World Trade Organization, thereby contributing to the harmonious development and expansion of world trade;

Have agreed in pursuit of the above, to conclude the following Digital Economy Agreement:

ARTICLE 1

Amendment of the Free Trade Agreement

In accordance with Article 69 (Amendments) of the Free Trade Agreement, the Parties agree to:

(a) insert a new Chapter III*bis* (Digital Economy) as set out in Annex I to this Digital Economy Agreement, after Chapter III (Services) of the Free Trade Agreement; and

(b) insert a new Article 5*bis* (Location of Computing Facilities for Financial Services) as set out in Annex II to this Digital Economy Agreement, after Article 5 of Annex VIII (Financial Services) to the Free Trade Agreement.

ARTICLE 2

Information Sharing and Stakeholder Engagement

1. Each Party shall establish or maintain its own free, publicly accessible and regularly updated website containing information regarding this Digital Economy Agreement. To the extent possible, the information shall be made available in English and may include:

(a) the text of this Digital Economy Agreement;

(b) a summary of this Digital Economy Agreement;

(c) information designed for SMEs that contains:

(i) a description of the provisions in this Digital Economy Agreement that the Party considers to be relevant to SMEs,

(ii) any additional information that would be useful for SMEs interested in benefitting from the opportunities provided by this Digital Economy Agreement; and

(d) links to equivalent websites on this Digital Economy Agreement.

2. The Parties recognise the importance of stakeholder engagement and of promoting relevant initiatives and platforms within and between Parties, as appropriate.

3. The Parties may engage interested stakeholders, such as businesses, non-government organisations and academic experts for the purposes of implementation efforts and further modernisation of this Digital Economy Agreement, as appropriate.

ARTICLE 3

Entry into Force

1. This Digital Economy Agreement is subject to ratification, acceptance or approval. The instruments of ratification, acceptance or approval shall be deposited with the Depositary of the Free Trade Agreement (hereinafter referred to as the "Depositary").

2. This Digital Economy Agreement shall enter into force, in relation to those Parties which have deposited their instruments of ratification, acceptance or approval, on the first day of the third month following the date on which at least one EFTA State and Singapore have deposited their instruments of ratification, acceptance or approval with the Depositary.

3. In relation to an EFTA State depositing its instrument of ratification, acceptance, or approval after the date on which at least one EFTA State and Singapore have deposited their instruments of ratification, acceptance or approval with the Depositary, this Digital Economy Agreement shall enter into force for that EFTA State on the first day of the third month following the deposit of its instrument.

IN WITNESS WHEREOF, the undersigned, being duly authorised thereto by their respective governments, have signed this Digital Economy Agreement.

Done at Bern, this 25th day of September 2025, in one original in English, which shall be deposited with the Depositary. The Depositary shall transmit certified copies to all Parties.

For Iceland

.....

For the Republic of Singapore

.....

For the Principality of Liechtenstein

.....

For the Kingdom of Norway

.....

For the Swiss Confederation

.....

ANNEX I

CHAPTER III*BIS* DIGITAL ECONOMY

ANNEX I

CHAPTER III*BIS* DIGITAL ECONOMY

III*BIS* DIGITAL ECONOMY

ARTICLE 36-A

Definitions

1. For the purposes of this Chapter, Article 22 applies.

2. For the purposes of this Chapter:

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

   (b) "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;

   (c) "cryptographic algorithm" means a defined procedure or formula of transforming data using cryptography;

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

   (e) "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[1];

   (f) "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;

[1] 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.

(g) "electronic transmission" or "transmitted electronically" means a transmission made using any electromagnetic means, including by photonic means, such as through the Internet;

(h) "end-user" means a person who purchases or subscribes to an Internet access service from an Internet access service provider;

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

(j) "metadata" means structural or descriptive information about data, such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher or responsible party, contact information, method of collection and context;

(k) "personal data" means any information relating to an identified or identifiable natural person;

(l) "trade administration documents" 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, export or transit of goods;

(m) "tax convention" means a convention for the avoidance of double taxation or other international taxation agreement or arrangement;

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

ARTICLE 36-B

Scope

1. This Chapter applies to measures of a Party that affect trade enabled by electronic means.

2. In the event of any inconsistency between this Chapter and Annex VIII, Annex VIII shall prevail to the extent of the inconsistency.

3. This Chapter shall not apply to:

(a) audio-visual services[2];

[2] The Parties understand that this includes broadcasting, which means, for the purposes of this Agreement, the transmission of signs or signals via any technology for the reception or display of audio and visual programme signals by all or part of the public.

(b) government procurement, except as provided for in paragraph 1 of Article 36-E, paragraph 3 of Article 36-G, and Article 36-Z; 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 36-I.

ARTICLE 36-C

Objectives

The Parties seek to:

(a) ensure legal certainty and predictability for trade enabled by electronic means;

(b) avoid barriers to the use and development of digital trade in goods and services;

(c) create an environment of trust and confidence in, as well as security for digital trade, including through:

(i) the protection of personal data, and

(ii) the protection of trade secrets;

(d) expand the scope of cooperation between the Parties on matters of mutual interest concerning the digital economy;

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

(f) contribute to the establishment of new, ambitious and transparent benchmarks that will support the growth and effective regulation of the digital economy;

(g) build on the Parties' multilateral and regional engagements on digital trade;

(h) facilitate greater business-to-business and research links between the Parties.

ARTICLE 36-D

Customs Duties[3]

1. No Party shall impose customs duties on electronic transmissions, including content transmitted electronically.

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 they are imposed in a manner consistent with this Agreement.

ARTICLE 36-E

Electronic Authentication

1. 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 it is in electronic form.

2. No Party shall adopt or maintain measures that would:

(a) prohibit parties to an electronic transaction from mutually determining the appropriate electronic authentication methods or electronic signature for their 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 transaction, the method of authentication or the electronic signature meets certain performance standards or is certified by an accredited authority, in accordance with its laws and regulations.

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

5. The Parties shall endeavour to use interoperable electronic authentication.

[3] The Parties understand that "customs duties" means import and export duties.

ARTICLE 36-F

Paperless Trading

1. Each Party shall make publicly available electronic versions of all trade administration documents and shall endeavour to make them available in English.[4]

2. Each Party shall accept electronic versions of trade administration documents as legal equivalents of paper documents except if:

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

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

3. The Parties shall endeavour to establish or maintain a single window, enabling traders to submit documentation and data requirements for importation, exportation, or transit of goods through a single entry point to the participating authorities or agencies.

4. The Parties recognise the importance of facilitating, where relevant in each jurisdiction, the exchange of electronic records used in commercial trading activities between the Parties' businesses.

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

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

(b) electronic records used in commercial trading activities between the Parties' respective businesses, where relevant in each jurisdiction.

6. The Parties recognise the benefit of compatible and interoperable data exchange systems. To this end, the Parties shall endeavour to work towards the development and adoption of internationally-recognised standards in the development and governance of data exchange systems.

7. The Parties shall endeavour to cooperate and collaborate on new initiatives which promote, encourage, support and facilitate the use and adoption of the data exchange systems referred to in paragraph 5, such as through:

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

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

[4] For greater certainty, electronic version of trade administration documents refers to trade administration documents provided in a machine-readable format.

8. The Parties shall cooperate under existing international arrangements and agreements to enhance acceptance of electronic versions of trade administration documents.

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

ARTICLE 36-G

Domestic Electronic Transactions Framework

1. The Parties recognise the importance of electronic transactions frameworks. Each Party shall endeavour to adopt or maintain a legal framework consistent with the principles of:

(a) the UNCITRAL Model Law on Electronic Commerce (1996);

(b) the United Nations Convention on the Use of Electronic Communications in International Contracts, done at New York, November 23, 2005; and

(c) the UNCITRAL Model Law on Electronic Transferable Records (2017).

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. Unless otherwise provided for under its laws and regulations, a Party shall not deny the legal effect, legal validity or enforceability of an electronic contract solely on the basis that the contract has been made by electronic means.

ARTICLE 36-H

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

Subject to applicable domestic policies, laws and regulations, the Parties recognise the benefits of ensuring that end-users in their territories are able to:

(a) access, distribute and use services and applications of their choice available through the Internet, subject to reasonable network management;[5]

(b) connect end-user devices of their choice to the Internet, provided that such devices comply with the requirements in the territory where they are used and do not harm the network; and

[5] The Parties recognise that an internet access service supplier that offers its subscribers certain content on an exclusive basis would not be acting contrary to this principle.

(c) have access to information on the network management practices of their Internet access service supplier.

ARTICLE 36-I

Open Government Data

1. This Article applies to measures by a Party with respect to data held by the government, disclosure of which is not restricted under its laws and regulations, and which a Party makes digitally available for public access and use (hereinafter referred to as "government data").

2. The Parties recognise the benefit of making government data digitally available for public access and use in a manner consistent with paragraphs 3 to 5. The Parties shall endeavour to make government data generally available at no or reasonable cost.

3. The Parties recognise that facilitating public access to and use of government data fosters economic and social development, competitiveness and innovation. To this end, the Parties are encouraged to expand the coverage of such data, such as through engagement and consultation with interested stakeholders.

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

(a) made available in a machine-readable and open format;

(b) searchable and retrievable;

(c) updated, as applicable, in a timely manner; and

(d) accompanied by metadata that is based on commonly used formats that allow the user to understand and utilise the data.

5. To the extent that a Party chooses to make government data digitally available for public access and use, with explicit reference to the data source, it shall endeavour to avoid imposing conditions[6] that unduly prevent or restrict users from:

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

(b) regrouping the data; or

(c) using the data 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 in matters that facilitate and expand public access to and use of government data, including exchanging information and experiences on practices and policies, with a view to enhancing and generating business

[6] For greater certainty, nothing in this paragraph prevents a Party from requiring a user of such data to link to original sources.

and research opportunities, especially for small and medium-sized enterprises (hereinafter referred to as "SMEs").

ARTICLE 36-J

Online Consumer Protection

1. The Parties recognise the importance of transparent and effective measures that enhance consumer confidence and trust in digital trade. Each Party shall adopt or maintain measures to proscribe misleading, fraudulent and deceptive commercial activities that cause harm, or potential harm, to consumers engaged[7] in digital trade.

2. Misleading, fraudulent and deceptive commercial activities include:

(a) making material misrepresentations[8], including implied factual misrepresentations, or false claims as to matters such as qualities, price, suitability for purpose, quantity or origin of goods or services;

(b) advertising goods or services for supply without intention or reasonable capability to supply;

(c) failing to deliver goods or provide services to a consumer after the consumer is charged unless justified on reasonable grounds; or

(d) charging a consumer for services or goods not requested.

3. To protect consumers engaged in digital trade, each Party shall adopt or maintain measures that aim to ensure:

(a) that suppliers of goods and services deal fairly and honestly with consumers;

(b) that suppliers provide complete, accurate, and transparent information on goods and services including any terms and conditions of purchase; and

(c) the safety of goods and, where applicable, services during normal or reasonably foreseeable use.

4. The Parties recognise the importance of affording to consumers who are engaged in digital trade consumer protection at a level not less than that afforded to consumers who are engaged in other forms of commerce.

5. The Parties recognise the importance of cooperation between their respective consumer protection agencies or other relevant bodies, including the exchange of information and experience, as well as cooperation in appropriate cases of mutual concern

---

[7] The term "engaged" shall include the pre-transaction phase of digital trade.

[8] For the purposes of this article, material misrepresentations refer to misrepresentations that are likely to affect a consumer's conduct or decision to use or purchase a good or service.

regarding the violation of consumer rights in relation to digital trade in order to enhance online consumer protection, where mutually agreed.

6. Parties shall promote access to, and awareness of, consumer redress or recourse mechanisms, including for consumers transacting cross-border.

ARTICLE 36-K

Unsolicited Commercial Electronic Messages

1. Each Party shall adopt or maintain measures in order to protect users effectively against unsolicited commercial electronic messages. Such measures shall:

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

(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 endeavour to ensure that unsolicited commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they were made and, to the extent provided for in its laws and regulations, contain the necessary information to enable recipients 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 pursuant to paragraphs 1 and 2.

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

ARTICLE 36-L

Personal Data Protection

1. The Parties recognise that individuals have a right to privacy and the protection of personal data and that high and enforceable standards in this regard contribute to trust in the digital economy and to the development of trade.

2. To this end, each Party shall adopt or maintain a legal framework that provides for the effective protection of the personal data of individuals in digital trade.[9]

3. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures under its legal framework referred to in paragraph 2 that it deems appropriate,

[9] For greater certainty, a Party may comply with the obligation in paragraph 2 by adopting or maintaining measures or a combination of measures such as comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy or other laws that address privacy violations.

including through the adoption and application of rules for the cross-border transfer of personal data, provided that the laws and regulations of that Party provide for instruments enabling transfers under conditions of general application for the protection of the data transferred.

4. In the development of its legal framework for the protection of personal data, each Party should take into account principles and guidelines developed by relevant international bodies or organisations.

5. Each Party shall ensure that its legal framework referred to in paragraph 2 provides non-discriminatory protection of personal data for natural persons.

6. Each Party shall publish information on the personal data protection rights it provides to natural persons in digital trade, including guidance on how:

(a) natural persons can pursue remedies; and,

(b) enterprises can comply with legal requirements.

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

8. Recognising that the Parties may take different legal approaches to protecting personal data, each Party shall encourage the development of mechanisms to promote compatibility between these different regimes. The mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on mechanisms applied in their jurisdictions.

ARTICLE 36-M

Cross-border Data Flows

1. The Parties are committed to ensuring the cross-border transfer of data by electronic means where this activity is for the conduct of business under this Agreement.

2. To that end, a Party shall not adopt or maintain measures which prohibit or restrict the cross-border transfer of data set out in paragraph 1 by:

(a) requiring the use of computing facilities or network elements in the Party's territory for processing of data, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Party;

(b) requiring the localisation of data in the Party’s territory for storage or processing;

(c) prohibiting storage or processing of data in the territory of another Party;

(d) making the cross-border transfer of data contingent upon the use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory; or

(e) prohibiting the transfer of data into the territory of the Party.[10]

3. The Parties shall keep the implementation of this provision under review and assess its functioning within three years of the entry into force of the Digital Economy Agreement between the EFTA States and Singapore done at Bern, Switzerland, on 25 September 2025. A Party may at any time propose to the other Parties to review the list of restrictions listed in paragraph 2, including if it or another Party has agreed not to adopt or maintain other types of measures in addition to those listed in paragraph 2 in a future bilateral or multilateral agreement. Such request shall be accorded sympathetic consideration.

4. 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[11], 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 necessary to achieve the objective.[12]

5. This Article shall not apply with respect to a "financial service supplier", as defined in paragraph II of Article 1 of Annex VIII.

ARTICLE 36-N

Electronic Payments

1. The Parties recognise the pivotal role of electronic payments in enabling digital trade and the rapid growth of electronic payments, including those provided by non-banks, non-financial institutions, and financial technology ("FinTech") enterprises. The Parties agree to support the development of efficient, safe and secure cross-border electronic payments by fostering the adoption and use of internationally accepted standards, promoting interoperability and the interlinking of payment infrastructures, and encouraging useful innovation and competition in the payments ecosystem.

2. Each Party shall endeavour to:

---

[10] For greater certainty, requirements listed in sub-paragraphs (a) to (d) of do not prevent a Party from requiring storage of accounting and bookkeeping information in its territory, as long as cross-border data flows are permitted.

[11] For the purposes of this Article, "legitimate public policy objective" shall be interpreted in an objective manner and shall enable the pursuit of objectives such as the protection of public security, public morals, human, animal or plant life or health, the maintenance of public order or other objectives of public interest, taking into account the evolving nature of digital technologies and related challenges.

[12] For greater certainty, this provision does not affect the interpretation of other exceptions in this Agreement and their application to this Article, or the right of a Party to invoke any of them.

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

(b) encourage the adoption of international standards for electronic payment messaging to enable greater interoperability between electronic payment systems;

(c) facilitate innovation and competition on a level playing field and the introduction of new financial and electronic payment products and services in a timely manner such as through the adoption of regulatory and industry sandboxes; and

(d) promote or facilitate the adoption of payment instruments or systems based on distributed ledger technology for commercial and financial transactions, including the use of smart contracts to increase efficiency.

3. The Parties recognise the importance of upholding safety, efficiency, trust and security in electronic payment systems through their respective laws and regulations.

ARTICLE 36-O

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 another Party's territory.

2. Each Party shall endeavour to 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, the Parties shall take into account international frameworks.

3. The Parties recognise the economic importance of promoting the global adoption of interoperable electronic invoicing systems. To this end, the Parties shall endeavour to share best practices pertaining to electronic invoicing, as appropriate.

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

(a) share information and experiences, including the exchange of best practices, in the area of electronic invoicing;

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

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

ARTICLE 36-P

Source Code[13]

1. No Party shall require the transfer of, or access to, the source code of software or parts thereof owned by a natural or juridical person of another Party as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.

2. Paragraph 1 shall not apply to:

(a) requirements by a court, regulatory body or other competent authority for an investigation, inspection, examination, enforcement or judicial proceeding, or the monitoring of compliance with codes of conduct and other standards, subject to safeguards against unauthorised disclosure;

(b) the imposition, adoption or enforcement of a remedy granted in accordance with a Party's laws and regulations following an investigation, inspection, examination, enforcement action or judicial proceeding;

(c) requirements by competent authorities to verify the conformity of goods and services with legal requirements in the context of market surveillance; or

(d) the voluntary transfer or granting of access to source code on a commercial basis by a natural or juridical person of a Party or under open source licences.

ARTICLE 36-Q

Information and Communication Technology Products that Use Cryptography

1. For the purposes of this Article, "Information and Communication Technology product (ICT product)" means any hardware or software whose intended function is information processing or communication by electronic means, including storage, transmission and display, or electronic processing applied to determine or record physical phenomena, or to control physical processes, but does not include any instrument for supplying a financial service or any financial asset, including money.

2. This Article shall apply to ICT products that use cryptography.

3. With respect to a product that uses cryptography and is designed for commercial applications, no Party shall impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of the product, as a condition of the manufacture, sale, distribution, import or use of the product, to:

(a) transfer or provide access to a particular technology, production process or other information, for example, a private key or other secret parameter,

[13] For greater certainty, the Parties understand that this Article shall not prevent a Party from requiring the disclosure of source code in patent applications and patent grant procedures.

algorithm specification or other design detail, that is proprietary to the manufacturer or supplier and relates to the cryptography in the product, to the Party or a person in the Party's territory;

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

(c) use or integrate a particular cryptographic algorithm,

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

4. Paragraph 2 shall not apply to:

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

(b) measures taken by a Party pursuant to supervisory, investigatory or examination authority relating to financial institutions or markets; or

(c) requirements by a regulatory body or judicial authority of a Party in respect of any information to which paragraph 2 applies for an investigation, inspection, examination, enforcement action or a judicial proceeding, subject to safeguards against unauthorised disclosure.

5. For greater certainty, this Article shall not be construed to prevent a Party's law enforcement authorities from requiring service suppliers using encryption they control to provide, in accordance with that Party's legal procedures, encrypted and unencrypted communications.

6. For greater certainty, this Article does not affect the rights and obligations of a Party under Article 36-P.

ARTICLE 36-R

Cybersecurity

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

(a) building the capabilities of their respective national entities responsible for cybersecurity incident response, taking into account the evolving nature of cybersecurity 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 to use those mechanisms to swiftly address cybersecurity incidents;

(c) maintaining a dialogue on matters related to cybersecurity, 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; and

(e) workforce development in the area of cybersecurity, including through possible initiatives relating to training and development.

2. Given the evolving nature of cybersecurity threats, the Parties recognise that risk-based approaches may be more effective than compliance-based approaches in addressing those threats. The Parties therefore underscore the benefit of incorporating security into the design phase and shall endeavour to employ, and to encourage enterprises within their jurisdictions to use, risk-based approaches that rely on technical, objective, and interoperable standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to and recover from cybersecurity events.

ARTICLE 36-S

Cooperation and Review

1. The Parties may, in addition to the topic-specific cooperation provisions set out in this Chapter, cooperate on any additional matter of mutual interest in relation to digital trade, which could, inter alia, address the following issues:

(a) the liability of intermediary service providers with respect to the transmission and storage of information;

(b) interoperability of infrastructures, such as secure electronic authentication and payments; and

(c) personal data protection.

2. The Parties shall periodically review this Chapter in the Joint Committee regarding new developments in the field of digital trade.

ARTICLE 36-T

Cooperation on Competition Policy

1. Recognising that the Parties can benefit by sharing their experience 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 technical cooperation activities, subject to available resources, including:

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

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

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

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

ARTICLE 36-U

Digital Identities

The Parties recognise that cooperation on digital identities may increase regional and global connectivity, and that each Party may take different legal and technical approaches to digital identities. In order to promote compatibility, the Parties may pursue initiatives of mutual interest 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 framework, or the recognition of their legal effects, whether accorded autonomously or by agreement;

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

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

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

ARTICLE 36-V

Financial Technology Cooperation

The Parties recognise the importance of cooperation between their FinTech industries and that effective cooperation regarding FinTech will require the involvement of businesses. To this end, the Parties shall encourage:

(a) cooperation between businesses in the FinTech sector;

(b) the development of FinTech solutions for business or financial sectors; and

(c) collaboration of entrepreneurship or start-up talent in FinTech, consistent with the laws and regulations of the Parties.

ARTICLE 36-W

Artificial Intelligence

1. The Parties recognise that the use and adoption of Artificial Intelligence ("AI") technologies is becoming increasingly important within a digital economy, and that it offers significant social and economic benefits to persons and businesses. At the same time, the Parties recognise that technologies related to AI present challenges and pose risks that need to be adequately addressed. The Parties may cooperate, in accordance with their respective relevant policies, through:

(a) sharing AI-related initiatives as well as research and industry practices related to AI technologies and their governance;

(b) promoting and sustaining the responsible use and adoption of AI technologies by businesses and across the community;

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

(d) exploring opportunities for joint AI projects and deployment or test-bedding initiatives between the Parties.

2. The Parties recognise that governance and policy frameworks and corresponding standards that promote interoperability and take into account relevant international principles, guidelines and standards, are needed for the ethical, trusted, safe, and responsible development and use of AI, and that such frameworks and standards will help realise the benefits of these technologies. To this end, the Parties recognise the importance of:

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

(b) utilising risk-based approaches to frameworks and 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.

ARTICLE 36-X

Standards, Technical Regulations and Conformity Assessment Procedures

1. The Parties shall, where appropriate, encourage the adoption of international or internationally recognised standards relating to the digital economy. In emerging areas of mutual interest in the digital economy, the Parties shall also, where appropriate:

(a) participate and cooperate in fora that all the Parties are party to, to promote the development of standards; and

(b) in areas where no such standards exist, jointly explore cooperation towards recognising the standards developed by the other Parties.

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

3. The Parties shall, in areas of mutual interest in the digital economy:

(a) identify and cooperate on joint initiatives in the field of standards and conformity assessment;

(b) utilise established international accreditation mutual recognition arrangements, where appropriate;

(c) give positive consideration to proposals of another Party for co-operation on standards, technical regulations and conformity assessment procedures; and

(d) encourage cooperation between the public and private sector, 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.

4. 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 relating to the digital economy. Each Party shall endeavour to, upon request by another Party, provide information on standards, technical regulations and conformity assessment procedures relating to the digital economy within a reasonable period of time agreed by the requesting and requested Parties and, if possible, within 60 days of the request.

ARTICLE 36-Y

Innovation

The Parties recognise the importance of digitalisation and the use of new technologies in the digital economy, including distributed ledger technology and its use cases in asset tokenisation, which support economic growth and development. The Parties further recognise the need for an environment conducive for experimentation and innovation in order to support trade by electronic means and promote the digital economy, including by:

(a) identifying relevant approaches and technology to enable cross-border data flows;

(b) cooperating to develop policy frameworks and reference use cases; and

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

ARTICLE 36-Z

Small and Medium-Sized Enterprises

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

2. The Parties shall foster cooperation on the digital economy between their SMEs.

3. With a view to a more robust cooperation between the Parties to enhance trade and investment opportunities for SMEs in the digital economy, the Parties may:

(a) continue cooperation with the other Parties to exchange information and best practices in leveraging digital tools and technology to improve SMEs' participation in the digital economy; and

(b) encourage participation by the Parties' SMEs in platforms that could help link SMEs up with international suppliers, buyers and other potential business partners.

ARTICLE 36-AA

Digital Inclusion

1. The Parties acknowledge the importance of digital inclusion to ensure that all persons and businesses have what they need to participate in, contribute to and benefit from the digital economy.

2. The Parties recognise the importance of expanding and facilitating digital economy opportunities by removing barriers. This may, as appropriate, include enhancing cultural and people-to-people links, including between indigenous peoples, and improving access for women, rural populations, the young, elderly, persons with disabilities, and low socio-economic groups.

3. The Parties may cooperate on:

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

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

(c) addressing barriers in accessing digital economy opportunities;

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

(e) opportunities for "new forms" of work, such as teleworking and co-working;

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

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

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

ARTICLE 36-AB

General Exceptions

1. For the purposes of this Chapter, Article XX of the GATT 1994 and its interpretive notes and Article XIV (a)-(c) of the GATS apply and are hereby incorporated into and made part of this Agreement, *mutatis mutandis*.

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

ARTICLE 36-AC

Security Exceptions

Articles 20 and 34 shall apply, *mutatis mutandis*, to this Chapter.

ARTICLE 36-AD

Protection of Critical Public Infrastructure

1. Nothing in this Chapter shall be construed to prevent a Party from taking any action which it considers necessary to protect its essential security interests with regard to the protection of critical public infrastructure, such as communications, power, water and transportation infrastructure providing essential goods or services, from deliberate attempts to disable or degrade it.

2. For greater certainty, this Article does not affect the interpretation of other exceptions in this Agreement or the right of a Party to invoke any of them.

ARTICLE 36-AE

Prudential Measures

1. Nothing in this Chapter shall be construed to prevent a Party from adopting or maintaining reasonable measures for prudential reasons, such as:

(a) the protection of investors, depositors, policy-holders, policy-claimants, persons to whom a fiduciary duty is owed by a financial service supplier, or similar financial market participants;

(b) the maintenance of the safety, soundness, integrity or financial responsibility of financial service suppliers; and

(c) ensuring the integrity and stability of a Party's financial system.

2. These measures shall not be more burdensome than necessary to achieve their aim, and shall not constitute a means of arbitrary or unjustifiable discrimination against financial service suppliers of another Party in comparison to its own like financial service suppliers, or a disguised restriction on trade in services.

3. Nothing in this Chapter shall be construed to require a Party to disclose information relating to the affairs and accounts of individual consumers or any confidential or proprietary information in the possession of public entities.

4. Each Party shall make its best endeavours to ensure that the Basel Committee's "Core Principles for Effective Banking Supervision", the standards and principles of the International Association of Insurance Supervisors and the International Organisation of Securities Commissions' "Objectives and Principles of Securities Regulation" are implemented and applied in its territory.

ARTICLE 36-AF

Specific Exceptions

1. Nothing in this Chapter shall be construed to prevent a Party, including its public entities, from exclusively conducting activities or supplying services in its territory forming part of a public retirement plan or statutory system of social security.

2. Nothing in this Chapter shall be construed to prevent a Party, including its public entities, from exclusively conducting activities or supplying services in its territory for the account or with the guarantee or using the financial resources of the Party, or its public entities.

3. If a Party allows any of the activities or services referred in paragraphs 1 or 2 to be conducted or supplied by its financial service suppliers in competition with a public entity or a financial service supplier, "services" shall include such activities.

4. Nothing in this Chapter shall apply to activities conducted or services supplied by a central bank or monetary authority or by any other public entity, in pursuit of monetary or exchange rate policies.

ARTICLE 36-AG

Taxation

1. Nothing in this Chapter shall apply to taxes or taxation measures.[14]

2. Nothing in this Chapter shall affect the rights and obligations of any Party under any tax convention. In the event of any inconsistency between this Chapter and any such tax convention, that convention shall prevail to the extent of the inconsistency. The competent authorities under that convention shall have sole responsibility for determining whether any inconsistency exists between this Chapter and that convention.

---

[14] Taxes and taxation measures include excise duties but do not include customs duties as defined in paragraph 2 of Article 8 of this Agreement.

ANNEX II

ARTICLE 5*BIS*

ANNEX II

ARTICLE 5*BIS*

ARTICLE 5*BIS*

Location of Computing Facilities for Financial Services

1. For the purposes of this Article, "computing facilities" means computer servers and storage devices for processing or storing information for commercial use but does not include computer servers or storage devices of or used to access financial market infrastructures.

2. 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.

3. No Party shall require a financial service supplier to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory provided that the Party's financial regulatory or supervisory authorities have timely access to the necessary data for fulfilling their supervisory tasks. To that end, a Party shall not adopt or maintain measures which prohibit or restrict the cross-border transfer of data by:

(a) requiring the use of computing facilities or network elements in the Party's territory for processing of data, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Party;

(b) requiring the localisation of data in the Party's territory for storage or processing;

(c) prohibiting storage or processing of data in the territory of another Party;

(d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory; or

(e) prohibiting the transfer of data into the territory of the Party.

4. For greater certainty, Article 4 of this Agreement applies to paragraph 3 of this Article.

5. The Parties shall keep the implementation of this provision under review and assess its functioning within three years of the entry into force of the Digital Economy Agreement between the EFTA States and Singapore done at Bern, Switzerland, on 25 September 2025. A Party may at any time propose to the other Parties to review the list of restrictions listed in paragraph 3, including if it or another Party has agreed not to adopt or maintain other types of measures in addition to those listed in paragraph 3 in a future

bilateral or multilateral agreement. Such request shall be accorded sympathetic consideration.