CHAPTER 9

DIGITAL TRADE

SECTION A

GENERAL PROVISIONS

ARTICLE 9.1

Objective

The objective of this Title is to facilitate digital trade, to address unjustified barriers to trade enabled by electronic means and to ensure an open, secure and trustworthy online environment for businesses and consumers.

ARTICLE 9.2

Scope

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

2. This Chapter does not apply to:

(a) Audio-visual services;

(b) Government procurement; and

(c) Information or data held or processed by or on behalf of a Party, or measures related to such information or data, including measures related to its collection except Open Government Data (Article 9.12).

3. 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 8 (Trade in Services), Annex 8-C (Financial Services), and Annex 8-D (Telecommunications Services) including the Party's schedules of specific commitments, non-conforming measures or exceptions set out in this Agreement that are applicable to those obligations.

ARTICLE 9.3

Right to regulate

Consistent with the provisions of this Chapter, the Parties retain their right to regulate within their respective territories to achieve their legitimate policy objectives.

ARTICLE 9.4

Definitions

1. The definitions in Article 8.2 [Trade in Services] apply to this Chapter unless otherwise defined in this chapter.

2. For the purposes of this Chapter, the following definitions apply:

(a) "Unsolicited commercial electronic message" means an electronic message[1] that is sent for commercial advertising or marketing purposes directly to a user via a public telecommunications service, without the consent of the recipient or despite the explicit rejection of the recipient.

(b) "Electronic authentication" means an electronic process that enables the confirmation of:

(i) the electronic identification of a natural or legal person, or

(ii) the origin and integrity of data in electronic form.

(c) "Electronic invoicing" means the automated creation, exchange and processing of an invoice between a supplier and a buyer using a structured digital format.

(d) "Electronic signature[2]" means data in electronic form that is in, affixed to, or logically associated with other data in electronic form that may be used to identify the signatory in relation to the data in electronic form and indicate the signatory approval of the information contained therein[3].

(e) "Electronic time stamp" means data in electronic form which binds other data in electronic form to a particular date and time establishing evidence that the latter data existed at that date and time;

---

1 For greater certainty, an electronic message comprises at least text messages (Short Message Service or "SMS") and, to the extent provided for under the laws or regulations of a Party, other electronic messages such as, electronic mail, multimedia (Multimedia Message Service or "MMS") messages, and other types of electronic messages.

2 For EU electronic signature applies to natural persons and electronic seal applies to legal persons. For India the term electronic seal is not defined in its domestic laws and the term electronic signature applies to both natural and legal persons.

3 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 data in electronic form has not been altered or verifying the identity of the signatory.

(f) "Electronic trust service" means an electronic service consisting of:

(i) the creation, verification and validation of electronic signatures, electronic seals, electronic time stamps, and certificates related to those services;

(ii) the preservation of electronic signatures, seals or certificates related to those services;

(g) "Government data" means non-proprietary data owned or held by the government and by non-governmental bodies in the exercise of powers conferred on them by government;

(h) Personal data means any information or data about or relating to an identified or identifiable natural person.

(i) "User" means any natural or legal person using a public telecommunications service.

(j) "Measure of a Party" means a measure taken by:

(i) central government and authorities of that Party; or

(ii) non-governmental bodies in the exercise of powers delegated by central government or authorities of that Party.

SECTION B

PERSONAL DATA PROTECTION

ARTICLE 9.5

Privacy and Protection of personal data

1. Each Party recognises that privacy is a fundamental right and that high standards of privacy and protection of personal data contribute to trust in the digital economy and to the development of trade.

2. The right of each Party to decide on its own level of protection of personal data and privacy shall remain unaffected. Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data.

3. Each Party shall endeavour to inform the other Party about safeguards referred to in paragraph 2 that it adopts or maintains.

SECTION C

SPECIFIC PROVISIONS

ARTICLE 9.6

Paperless trading

1. With a view to creating a paperless border environment for trade in goods the parties recognize the importance of eliminating paper forms and documents for the import, export or transit of goods. Each Party shall work towards implementing initiatives which provide for the use of paperless trading, and transition toward using forms and documents in data-based formats, taking into account the principles and guidelines agreed by the World Customs Organization and other relevant international organization to which both Parties are Members.

2. Each Party shall endeavour to make trade administration documents, that it issues or controls, or that are required in the normal course of trade, and as appropriate, supporting documents, available to the public in electronic format. For the purposes of this paragraph, the term "electronic

format" includes formats, suitable for automated interpretation and electronic processing without human intervention, as well as digitised images and forms.

3. Each Party shall endeavour to accept trade administration documents submitted electronically as the legal equivalent of the paper version of those documents.

4. The Parties shall endeavour to cooperate bilaterally and in international fora, in which they are participants, to enhance acceptance of electronic versions of trade administration documents.

ARTICLE 9.7

Conclusion of contracts by electronic means

1. Unless otherwise provided for under its laws and regulations, each Party shall ensure that: contracts may be concluded by electronic means.

2. No other obstacles to the use of electronic contracts are created or maintained and contracts are not deprived of legal effect and validity solely on the ground that the contract has been made by electronic means.

ARTICLE 9.8

Electronic authentication and electronic trust services

1. Except in circumstances otherwise provided for in its law and regulation, Party shall not deny the legal effect and admissibility as evidence in legal proceedings of an authenticated electronic document, an electronic signature, an electronic seal or an electronic time stamp, solely on the ground that it is in electronic form.

2. A Party shall not adopt or maintain measures that would:

(a) prohibit parties to an electronic transaction from mutually determining the appropriate electronic authentication methods 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 trust service 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 trust service is certified by an authority accredited in accordance with its laws and regulations or meets certain performance standards which shall be objective, transparent and non-discriminatory and only relate to the specific characteristics of the category of transactions concerned.

4. The Parties shall endeavour to mutually recognise electronic signatures in accordance with their laws and regulatory frameworks.

ARTICLE 9.9

Transfer of or access to source code

1. A Party shall not require the transfer of, or access to, the source code of software owned by a natural or legal person of the other Party as a condition for the import, export, distribution, sale or use of such software, or of products containing such software, in or from its territory.[4]

2. For greater certainty:

[4] This Article does not preclude a Party from requiring that access be provided to source code of software used for critical infrastructure, to the extent required to ensure the effective functioning of such critical infrastructure, subject to safeguards against unauthorised disclosure.

(a) Article 19.7 (General exceptions), Article 19.8 (Security exceptions) and Article 8-C.3 (Prudential carve-out) may apply to measures of a Party adopted or maintained in the context of transfer of or access to source code including of certification procedure;

(b) Paragraph 1 does not apply to the voluntary transfer of, or granting of access to, source code of software by a natural or juridical person of the other Party on a commercial basis, such as in the context of a public procurement transaction or other freely negotiated contracts and

(c) Paragraph 1 does not affect the right of regulatory, law enforcement or judicial bodies administrative tribunal or conformity assessment bodies of a Party to require the modification of source code of software to comply with its laws or regulations that are not inconsistent with the Agreement.

3. Nothing in this Article shall affect:

(a) The right of regulatory authorities, law enforcement, administrative tribunal judicial or conformity assessment bodies[5] of a Party to require the transfer of, or access to, source code of software, as a condition for import, export, distribution, sale or use of such software, for investigation, inspection or examination, enforcement action or judicial proceeding purposes, to secure compliance with its laws or regulations pursuing legitimate public policy objectives,[6] subject to safeguards against unauthorised disclosure;

---

[5] For the purpose of this Article, 'conformity assessment body' refers to a relevant governmental body or authority of a Party, or non-governmental body in the exercise of powers delegated by a governmental body or authority of the Party, carrying out the procedures of assessment of conformity with applicable laws or regulations of that Party.

[6] For the purpose of this Article, "legitimate public policy objective" shall be interpreted in an objective manner and shall enable the pursuit of objectives such as to protect public security, public morals, or human, animal or plant life or health, to maintain public order, to protect other fundamental interests of society such as online safety, cybersecurity, safe and trustworthy artificial intelligence, or protecting against the dissemination of disinformation, or other similar objectives of public interest, taking into account the evolving nature of digital technologies and related challenges.

(b) The requirements by a court, administrative tribunal, competition authority, or other relevant body of a Party to remedy a violation of competition law, or requirements pursuant to a Party's laws or regulations that are not inconsistent with the Agreement to provide proportionate and targeted access to the source code of software that is necessary to address barriers to entry in digital markets, to ensure digital markets remain competitive, fair, open and transparent; and

(c) The protection and enforcement of intellectual property rights;

ARTICLE 9.10

Online consumer trust and protection

1. Recognising the importance of enhancing consumer trust and protection in digital trade, each Party shall adopt or maintain measures to ensure the effective protection of consumers engaging in electronic commerce transactions, including but not limited to transparent and effective measures that:

(a) Proscribe misleading, fraudulent and deceptive commercial practices;

(b) Require suppliers or sellers of goods and services to act in good faith and abide by fair commercial or trade practices;

(c) Require suppliers or sellers of goods or services to provide consumers with clear and thorough information, including when they act through intermediary service suppliers, regarding their identity and contact details, the transaction concerned, including the main characteristics of the goods or services and the full price inclusive of all applicable charges. In the case of intermediary service suppliers, this includes enabling the provision of such information by the supplier or seller of goods or services;

(d) Grant consumers access to redress for breaches of their rights, including a right to remedies if goods or services are paid for and are not delivered or provided as agreed; and

(e) Ensure the safety of goods during normal or reasonably foreseeable use.

2. The Parties recognise the importance of entrusting their consumer protection agencies or other relevant bodies with adequate enforcement powers and the importance of cooperation between their agencies in order to protect consumers and enhance online consumer trust.

ARTICLE 9.11

Unsolicited commercial electronic messages

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

(a) Require the consent, as specified in its laws and regulations, of the users that are natural persons to receive a commercial electronic message;

(b) Require a supplier of commercial electronic messages to facilitate the ability of users that are natural persons to prevent ongoing reception of those messages; or

(c) Otherwise provide for the minimisation of unsolicited commercial electronic messages.

2. Notwithstanding paragraph 1, a Party shall allow natural or legal persons who have collected, in accordance with conditions laid down in the law of that Party, the contact details of a user in the context of the supply of goods or services, to send commercial electronic messages to that user for their own similar goods or services.

3. Each Party shall ensure that commercial electronic messages clearly identifiable as such, clearly disclose on whose behalf they are made and contain the necessary information to enable users to request cessation free of charge and at any moment.

4. Each Party shall provide users with access to redress against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained pursuant to paragraphs 1 to 3.

5. To the extent provided for under its laws or regulations, a Party shall apply Paragraph 1 to 4 to other forms of commercial electronic message that is sent for commercial advertising, such as electronic mail and text and multimedia messages (SMS and MMS).

ARTICLE 9.12

Open government data

1. The Parties recognise that facilitating public access to, and use of government data contributes to stimulating economic and social welfare, competitiveness, productivity and innovation.

2. To the extent that a Party chooses to make government data accessible to the public, it shall endeavour to ensure to the extent practicable, that such data:

(a) Is in a format that allows it to be searched, retrieved, used, reused, and redistributed

(b) Is in a machine-readable format;

(c) Contains descriptive metadata, which is as standard as possible;

(d) Is made available via reliable, user-friendly and freely available Application Programming Interfaces;

(e) Is regularly updated;

(g) Is made available for re-use in full compliance with the Parties' respective personal data protection rules.

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

4. The Parties recognise the benefit of making data held by regional or local government digitally available for public access and use in a manner consistent with paragraphs 1 to 3.

ARTICLE 9.13

Cooperation on regulatory and technical issues

The Parties recognise the importance of cooperation and information exchange on digital trade. Where agreed by the Parties, the Parties shall exchange information on the following regulatory and technical issues in the context of digital trade:

(a) The recognition and facilitation of interoperable electronic authentication and electronic trust services;

(b) Unsolicited commercial electronic messages;

(c) Challenges for small and medium-sized enterprises in digital trade;

(d) Digital government;

(e) Online consumer trust and protection; and

(f) Any other area relevant for the development of digital trade as mutually agreed by the Parties.

ARTICLE 9.14

Digital identities

1. The Parties recognise that cooperation between the Parties on digital identities is important to promote connectivity and further growth of digital trade, while recognising that each Party may take different legal and technical approaches to digital identities. Accordingly, the Parties support ongoing work, in particular, under India-EU Trade and Technology Council to pursue mechanisms to promote interoperability between their respective digital identity Framework.

2. The Parties shall endeavour to facilitate initiatives to promote interoperability, which may include:

(a) Supporting the development of international frameworks and standards for digital identity;

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

(c) 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 9. 15

Cyber-security

1. The Parties have a shared vision to promote secure digital trade and recognise that threats to cybersecurity undermine confidence in digital trade. In order to identify and mitigate those threats and thereby facilitate digital trade, the Parties recognise the importance of:

(a) Building the capabilities of their appropriate competent authorities responsible for cybersecurity incident response; including through exchange of best practices;

(b) Using existing collaboration mechanisms, as appropriate, to anticipate, identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks of Parties and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness; and

(c) Promoting the development of a strong public and private workforce in the area of cybersecurity.

2. Given the evolving nature of cybersecurity threats and their negative impact on digital trade, the Parties recognise that risk-based approaches are generally effective in addressing those threats and minimising trade barriers. Accordingly, each Party shall endeavour to employ, and shall encourage enterprises within its jurisdiction to use, risk-based approaches that rely on open and transparent standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity incidents.

ARTICLE 9. 16

Electronic invoicing

1. The Parties recognise the importance of promoting the adoption of electronic invoicing systems and its role in increasing the efficiency, accuracy and reliability of commercial transactions.

2. To this end, the Parties shall endeavour to:

(a) Promote, encourage, support or facilitate the adoption of electronic invoicing by enterprises;

(b) Promote the existence of policies, standards, infrastructure and processes that support electronic invoicing;

(c) Generate awareness of, and build capacity for, electronic invoicing; and

d) Share best practices and take into account the relevant international electronic invoicing systems.

3. Each Party shall encourage the development of measures related to electronic invoicing to support cross-border interoperability, including by taking into account international standards, guidelines or recommendations; as appropriate.

ARTICLE 9.17

Review

The Parties shall reassess within five years of the date of entry into force of this Agreement the need for inclusion of additional provisions, including on the free flow of data, into this Agreement.