***DISCLAIMER**: The Commission and Australia are publishing the texts of the Agreement following the announcement of conclusion of the negotiations on 24 March 2026. The texts are published in view of the public interest in the Agreement, for information purposes only and they may undergo further minor modifications, including as a result of the process of legal and linguistic revision. These texts are without prejudice to the final outcome of the Agreement between the EU and Australia. The texts will be final upon signature. The Agreement will become binding on the Parties under international law only after completion by each Party of its applicable legal requirements and procedures necessary for the entry into force of the Agreement.*

CHAPTER 11

DIGITAL TRADE

SECTION A

GENERAL PROVISIONS

ARTICLE 11.1

Scope

1. The Parties recognise the economic growth and opportunities provided by, and the importance of, promoting consumer confidence in digital trade.

2. This Chapter applies to measures of a Party affecting trade enabled, either wholly or partially, by electronic means.

3. This Chapter does not apply to:

(a) audio-visual services; or

(b) information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection.

4. Article 11.5 (Cross-border data flows) does not apply to a measure to the extent that such measure is not subject to Section B (Investment liberalisation) or Section C (Cross-border trade in services) of Chapter 9 (Investment liberalisation and trade in services), by reason of:

(a) Article 9.10 (Non-conforming measures and exceptions – Investment liberalisation) or Article 9.17 (Non-conforming measures – Cross-border trade in services); and

(b) entries 9 (Gambling and betting) and 35 (Foreign investment) in Appendix 9-D-2 [Australia's schedule of non-conforming measures for services and investment, future measures].

ARTICLE 11.2

Definitions

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

(a) the definitions set out in Article 9.2 (Definitions - Investment liberalisation and trade in services (Section A));

(b) "consumer" means any natural person engaging in electronic commerce transactions for other than professional purposes or, if provided for in the laws or regulations of a Party, any enterprise engaging in electronic commerce transactions;

(c) "direct marketing communication" means any form of commercial advertising by which a person communicates marketing messages directly to a user via a public telecommunications service and, for the purpose of this Agreement, covers at least electronic mail, text and multimedia messages (SMS and MMS) and phone calls;

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

(i) the electronic identification of a person; or

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

(e) "electronic seal" means data in electronic form used by a juridical person which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;

(f) "electronic signature" means data in electronic form, which is attached to or logically associated with other data in electronic form and that may be used by a signatory to sign that other data;[1]

(g) "government data" means data owned or held by the central or regional levels of government;

(h) "internet access service" means a public telecommunications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used;

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

(j) "public telecommunications service" means a public telecommunications service as defined in point (j) of Article 9.X (Investment liberalisation and trade in services Chapter (Section E.6));

(k) "trade administration documents" means forms issued or controlled by a Party that must be completed by or for an importer or exporter in connection with the import or export of goods; and

(l) "user" means any person using a public telecommunications service.

2. The definition of "customs duty" set out in point (b) of Article 1.3 (General Definitions – Initial Provisions Chapter) does not apply to this Chapter.

ARTICLE 11.3

Right to regulate

[1] In the Union, natural persons use electronic signatures and juridical persons use electronic seals.

The Parties reaffirm each Party's right to regulate within their territories in pursuit of legitimate public policy objectives, such as the protection of health, social services, public education, safety, the environment, including climate change, public morals, social or consumer protection, animal welfare, privacy and data protection, security of energy supply, the promotion and protection of cultural diversity and, in the case of Australia, the promotion and protection of the rights and interests of Australian First Nations peoples.

ARTICLE 11.4

Exceptions

For greater certainty, nothing in this Chapter prevents a Party from adopting or maintaining a measure that meets the requirements of Article 23.1 (General exceptions), Article 23.2 (Security exceptions) or Article 9.z (Measures for prudential reasons – Investment Liberalisation and Trade in Services Chapter (Section E.3)).

SECTION B

DATA FLOWS AND PERSONAL DATA PROTECTION

ARTICLE 11.5

Cross-border data flows

1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties:

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

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

(c) prohibiting storage or processing in the territory of the other 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) requiring the approval prior to the transfer of data to the territory of the other Party.[2]

2. The Parties shall keep the implementation of paragraph 1 under review and assess its functioning within three years after the date of entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions specified in paragraph 1. That request shall be accorded sympathetic consideration.

3. If a Party undertakes commitments to refrain from adopting or maintaining restrictions of cross-border data flows between that Party and a third country, further to the restrictions specified in paragraph 1, in an existing or future bilateral or multilateral trade agreement with a third country, the Parties will review the restrictions in paragraph 1 with a view to incorporating such commitments into this Article.

---

[2] For greater certainty, point (e) of paragraph 1 does not prevent a Party from:

(a) subjecting the use of a specific transfer instrument or a particular cross-border transfer of data to approval on grounds relating to the protection of personal data and privacy, in accordance with Article 11.6 (Protection of personal information);

(b) requiring the certification or conformity assessment of information and communication technology products, services and processes, including Artificial Intelligence, before their commercialisation or use in its territory, to ensure compliance with laws and regulations consistent with this Agreement or for cybersecurity purposes, in accordance with Article 23.1 (General exceptions), Article 23.2 (Security exceptions), Article 9.z (Measures for prudential reasons – Investment Liberalisation and Trade in Services Chapter (Section E.3) or Article 11.6 (Protection of personal information);

(c) requiring that re-users of data protected by intellectual property rights or confidentiality obligations resulting from domestic laws and regulations consistent with this Agreement, respect such rights or obligations when transferring the data across borders, including with regard to access requests by courts and authorities of third countries, in compliance with Article 23.4 (Treatment of Information).

ARTICLE 11.6

Personal information protection

1. Each Party recognises that natural persons have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade.

2. Nothing in this Agreement shall prevent a Party from adopting or maintaining any measure to protect personal data and privacy,[3] including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application[4] for the protection of the data transferred.

3. Each Party shall inform the other Party about any measure referred to in paragraph 3 that it adopts or maintains.

SECTION C

SPECIFIC PROVISIONS

ARTICLE 11.7

Customs duties on electronic transmissions

1. A Party shall not impose customs duties on electronic transmissions between a person of a Party and a person of the other Party.

---

[3] For greater certainty, such measures include measures relating to credit information, or related personal information, of a natural person.

[4] For greater certainty, "conditions of general application" refer to conditions formulated in objective terms that apply horizontally to an unidentified number of economic operators and thus cover a range of situations and cases.

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

ARTICLE 11.8

Conclusion of contracts by electronic means

1. Each Party shall ensure that contracts may be concluded by electronic means and that its law neither creates obstacles for the use of electronic contracts nor results in contracts being deprived of either legal effect or legal validity solely on the ground that the contract has been made by electronic means.

2. Paragraph 1 does not apply to:

(a) broadcasting services;

(b) gambling services;

(c) legal representation services;

(d) services of notaries or equivalent professions involving a direct and specific connection with the exercise of public authority;

(e) contracts that establish or transfer rights in real estate;

(f) contracts requiring by law the involvement of courts, public authorities or professions exercising public authority;

(g) contracts of suretyship granted;

(h) collateral securities furnished by persons acting for purposes outside their trade, business or profession; or

(i) contracts governed by family law or by the law of succession.

ARTICLE 11.9

Electronic authentication, electronic signatures and electronic documents

1. A Party shall not deny the legal validity or legal effect, or admissibility as evidence in legal proceedings, of an electronic document or an electronic signature solely on the ground that it is in electronic form.[5]

2. A Party shall not adopt or maintain any measure that:

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

(b) prevents parties to an electronic transaction from having the opportunity to prove to judicial or administrative authorities that the use of electronic authentication or an electronic signature in their transaction complies with the applicable legal requirements.

3. Notwithstanding paragraph 2, a Party may require that, for a particular category of transactions, an electronic signature or the method of electronic authentication is certified by an authority accredited in accordance with the Party's law or meets certain performance standards which shall be objective, transparent and non-discriminatory and shall only relate to the specific characteristics of the category of transaction concerned.

4. A Party shall, to the extent provided for in its laws and regulations, apply paragraphs 1 to 3 to other electronic processes or means of facilitating or enabling electronic transactions, such as electronic seals, electronic time stamps, electronic registered delivery services or website authentication.

---

[5] For Australia, paragraph 1 applies subject to its laws or regulations that require certain documents or signatures be in a non-electronic form, such as those relating to bills of lading, warehouse receipts, foreign exchange transactions and property transfers.

ARTICLE 11.10

No prior authorisation

1. A Party shall not require prior authorisation solely on the ground that a service is provided online, or adopt or maintain any other requirement having an equivalent effect.[6]

2. Paragraph 1 does not apply to:

(a) telecommunications services;

(b) broadcasting services;

(c) gambling services;

(d) legal representation services; or

(e) services of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority.

ARTICLE 11.11

Online consumer trust

1. Recognising the importance of enhancing consumer trust 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 measures that:

(a) proscribe fraudulent and deceptive commercial practices;

[6] A service is provided online when it is provided by electronic means and without the parties being simultaneously present.

(b) require suppliers of goods and services to act in good faith and abide by fair commercial practices, including through the prohibition of charging consumers for unsolicited goods and services;

(c) require suppliers of goods or services to provide consumers with clear and thorough information regarding their identity and contact details,[7] as well as regarding the goods or services, the transaction and applicable consumer rights; and

(d) grant consumers access to redress for breaches of their rights, including a right to remedies in cases where goods or services are paid and not delivered or provided as agreed.

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 11.12

Unsolicited direct marketing communications

1. Each Party shall ensure that users are effectively protected against unsolicited direct marketing communications.

2. Each Party shall ensure that:

(a) direct marketing communications are not sent to users who are natural persons unless they have given their consent[8] to receiving those communications; or

[7] In the case of intermediary service suppliers, this also includes the identity and contact details of the actual supplier of the good or the service.

[8] Consent shall be defined in accordance with each Party's law.

(b) users who are natural persons may prevent the reception of direct marketing communications.[9]

3. Notwithstanding paragraph 2, each Party may allow persons who have collected, in accordance with its law, the contact details of a user in the context of the supply of goods or services, to send direct marketing communications to that user for their own similar goods or services.

4. Each Party shall ensure that direct marketing communications are 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.

5. Each Party shall provide users with access to redress against suppliers of direct marketing communications that do not comply with any measure adopted or maintained pursuant to paragraphs 1 to 4.

ARTICLE 11.13

Source code

1. The Parties recognise the increasing social and economic importance of the use of digital technologies, and the importance of the safe and responsible development and use of those technologies, including in respect of source code of software, to foster public trust.

2. A Party shall not require the transfer of, or access to, the source code of software[10] owned by a person of the other Party. This paragraph does not apply to the voluntary transfer of or granting of access to source code on a commercial basis by a person of the other Party, for instance in the context of a government procurement transaction or a freely negotiated contract.

---

[9] For Australia, paragraphs 2 and 4 only apply to the extent required by its spam and telemarketing laws and regulations.

[10] For greater certainty, "software" includes, *inter alia*, products containing such software or software used in the supply of services.

3. This Article does not preclude a Party from requiring that access be provided to software used for critical infrastructure, in order to ensure the effective functioning of critical infrastructure, subject to safeguards against unauthorised disclosure.

4. Nothing in this Article shall be construed to prevent a person of a Party from licencing its software on a free and open source basis.

5. Nothing in this Article shall affect:

(a) the right of a Party's regulatory, law enforcement or judicial authorities or conformity assessment bodies to access source code of software at any time for an investigation, inspection or examination, enforcement action or a judicial or administrative proceeding pursuant to its laws and regulations consistent with this Agreement, including those relating to non-discrimination and the prevention of bias, subject to safeguards against unauthorised disclosure;

(b) requirements by a competition authority to remedy a violation of competition law;

(c) the protection[11] and enforcement of intellectual property rights; and

(d) the right of a Party to take measures in accordance with the security and general exceptions provided for in Chapter 13 (Government procurement).

ARTICLE 11.14

Open internet access

Each Party recognises the benefits of users in its territory, subject to applicable policies, laws and regulations, being able to:

[11] For greater certainty, for the purposes of this Article, protection includes matters affecting the availability, acquisition, scope and maintenance of intellectual property rights.

(a) access, distribute and use services and applications of their choice available on the internet, subject to reasonable network management which does not block or slow down traffic based on commercial reasons;

(b) connect devices of their choice to the internet, provided that those devices do not harm the network; and

(c) access information on network management practices of their internet access service suppliers.

ARTICLE 11.15

Paperless trading

Each Party shall endeavour to:

(a) make publicly available electronic versions of all existing publicly available trade administration documents; and

(b) accept trade administration documents submitted electronically as the legal equivalent of the paper version of those documents, except if:

(i) there are domestic or international legal requirements to the contrary; or

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

ARTICLE 11.16

Open government data

1. The Parties recognise that facilitating public access to and use of government data contributes to stimulating economic and social development, 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 the data is:

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

(b) in a machine-readable and spatially-enabled format which contains descriptive metadata that is as standardised as possible;

(c) made available via reliable, user-friendly and freely available application programming interfaces;

(d) regularly updated;

(e) not subject to use conditions that are discriminatory or that unnecessarily restrict re-use; and

(f) made available for re-use in full compliance with that Party's personal data protection law.

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

4. This Article only applies to the regional level of government to the extent that the law of a regional government requires or permits publication of government data.

ARTICLE 11.17

Cooperation and information exchange on digital trade

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

(a) the recognition and facilitation of interoperable electronic authentication services and other electronic processes or means of facilitating or enabling electronic transactions;

(b) the treatment of direct marketing communications;

(c) the protection of consumers;

(d) e-government;

(e) challenges for SMEs in the use of electronic commerce;

(f) private sector-developed methods of self-regulation that foster electronic commerce, including codes of conduct, model contracts, guidelines and enforcement mechanisms; and

(g) any other matter relevant for the development of digital trade.

2. The Parties recognise the importance of cooperating on cybersecurity matters relevant for digital trade.