Digital Cooperation Organization

MODEL DIGITAL ECONOMY AGREEMENT

with commentary

Disclaimer

The following legal disclaimer ("Disclaimer") applies to this document ("Document") and by accessing or using the Document, you ("User" or "Reader") acknowledge and agree to be bound by this Disclaimer. If you do not agree to this Disclaimer, please refrain from using the Document.

While reasonable efforts have been made to ensure accuracy and relevance of the information provided, DCO makes no representation or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability of the information contained in this Document.

The information provided in this Document is intended for general informational purposes only and should not be considered as professional advice. DCO disclaims any liability for any actions taken or not taken based on the information provided in this Document.

DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between DCO and the User.

The designations employed in this Document of the material on any map do not imply the expression of any opinion whatsoever on the part of DCO concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The use of this Document is solely at the User's own risk. Under no circumstances shall DCO be liable for any loss, damage, including but not limited to, direct or indirect or consequential loss or damage, or any loss whatsoever arising from the use of this Document.

Unless expressly stated otherwise, the findings, interpretations and conclusions expressed in this Document do not necessarily represent the views of the DCO. The User shall not reproduce any content of this Document without obtaining DCO's consent or shall provide a reference to DCO's information in all cases.

By accessing and using this Document, the Reader acknowledges and agrees to the terms of this Disclaimer, which is subject to change without notice, and any updates will be effective upon publishing.

FOREWORD

We are living through a defining chapter in the global economy; one in which digital technologies are no longer simply tools of efficiency, but engines of opportunity, power, and possibility.

In a matter of years, digital trade has redrawn the boundaries of markets, reshaped how value is created, and opened doors that once seemed firmly closed. Yet even as innovation accelerates, the rules that govern our digital future have struggled to keep pace.

Across the world, governments face a shared challenge: how to unlock the full promise of the digital economy while safeguarding trust, fairness, and inclusion. How to enable data to move, ideas to scale, and businesses to grow without leaving people, small enterprises, or entire economies behind. And how to navigate emerging technologies, from artificial intelligence to quantum computing, in ways that strengthen societies rather than fragment them.

It is in this moment that the Model Digital Economy Agreement (MDEA) comes forward.
The MDEA is a first-of-its-kind framework, designed not as a one-size-fits-all prescription, but as an adaptable foundation for countries seeking to shape their own digital futures. It offers more than legal text. It offers a shared vision: that openness and trust are not opposing forces; that innovation and protection can advance together; and that digital progress is most powerful when it is inclusive by design.

The evidence from our Member States tells a compelling story. Digital adoption is rising. Entrepreneurship is accelerating. Digital services are transforming economies at every level of income and development. But the same evidence reveals persistent barriers such as fragmented regulations, uneven capacity, and uncertainty across borders that disproportionately affect micro, small, and medium enterprises. As artificial intelligence and new digital business models reshape competition and governance, these challenges only grow more complex.

The MDEA responds directly to this reality. It provides a balanced framework that reflects global best practice in digital trade while respecting national priorities and regulatory diversity. It promotes the flow of data while safeguarding personal information. It strengthens trust in electronic transactions while reinforcing cybersecurity and consumer protection. And it places small businesses at the center, recognizing that they are not peripheral to the digital economy, but its beating heart.

As the international community moves toward deeper cooperation on digital governance, the MDEA offers a bridge between ambition and action. It translates high-level commitments into interoperable, actionable policy. It gives governments a common language for digital cooperation, and it sends a clear signal to investors, innovators, and citizens alike: that DCO Member States are ready to collectively lead toward an open, secure, and resilient digital future.

At the Digital Cooperation Organization, our commitment is clear. We will continue to support our Member States by strengthening capacity, expanding shared knowledge, and evolving our frameworks as technology evolves, so that every nation, regardless of size, geography, or income, can participate meaningfully in the digital economy as both a consumer and a creator.

The Model Digital Economy Agreement marks a milestone in that journey. It reflects a shared ambition to build a digital economy that is not only faster and more connected, but more human, more resilient, and more inclusive for generations to come.

Deemah AlYahya
Secretary General, Digital Cooperation Organization

PREFACE

The Model Digital Economy Agreement (MDEA) represents a significant milestone in our mission to equip countries with the tools they need to participate confidently and competitively in the digital economy. Developed through extensive analysis of Member States' regulatory landscapes, international treaty practice, and real-world barriers faced by businesses, the MDEA provides a coherent and adaptable foundation for modern digital trade governance.

Our work began with a simple principle: policymaking must be rooted in evidence. To understand where alignment was needed, we undertook a comprehensive mapping of national frameworks across the key policy areas that shape digital trade, including data governance and cross-border data flows to consumer protection, cybersecurity, electronic transactions, digital payments, artificial intelligence and MSME inclusion. This was complemented by insights from enterprises across our Member States, which consistently regulatory fragmentation, compliance uncertainty, and limited interoperability as persistent challenges to cross-border engagement.

These findings guided every aspect of the Agreement. The MDEA's structure reflects the policy areas where coherence matters most, where flexibility is essential, and where governments require balanced provisions that promote innovation while preserving the space to regulate in the public interest. Its articles draw on global best practices, yet remain sensitive to diverse legal systems and stages of development. The accompanying commentary explains this architecture in a clear and practical way, highlighting the legal intent of each article, relevant international trends, and the policy considerations that negotiators and regulators may weigh when adapting the Agreement.

This publication is designed to serve multiple purposes. Governments may use the MDEA as a template for future bilateral or regional negotiations. Stakeholders across academia, industry and international organizations can use the commentary as a transparent guide to how digital trade disciplines are evolving globally.

The digital economy is dynamic, and so too must be the frameworks that support it. The MDEA is not intended to be static; it is a living tool. As technologies evolve and new regulatory questions emerge, the Agreement can be updated, expanded or adapted to reflect the changing needs of economies at all stages of development. The DCO Secretariat stands ready to support Member States in interpreting, implementing and developing this model through capacity building, technical assistance and continued knowledge sharing.

It is my hope that this publication will serve as a trusted and practical resource for policymakers, negotiators and digital economy leaders. By providing clarity, consistency and a shared reference point, the Model Digital Economy Agreement empowers countries to design digital futures that are open, inclusive and grounded in trust.

Dr. Hajar El Haddaoui
Director General, Digital Cooperation Organization

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Model Digital Economy Agreement (MDEA) is a model agreement designed to help governments develop modern, interoperable rules for the digital economy. Through its Preamble and 22 provisions, it sets out common rules and cooperation frameworks for cross-border digital trade, aiming to harmonize standards, foster innovation, and safeguard public interests. The MDEA is aided with the commentary that provides an in-depth analysis to serve as a reference to policymakers and negotiators. The commentary is based on framing each policy area, mapping treaty practice, analyzing bindingness, and assessing each rule's role within the MDEA's broader objectives, maintaining a neutral and descriptive approach.

The Preamble outlines shared goals of economic growth, inclusion, trust, and responsible technology use. Core trade rules include non-imposition of customs duties on electronic transmissions, while allowing consistent internal taxes, and non-discrimination for digital products, with safeguards for intellectual property, subsidies, broadcasting, pre-existing trade deals, and existing commitments in services and investment. Legal certainty for digital trade is reinforced through domestic electronic transactions frameworks, flexible authentication and e-signature rules, and paperless trade requirements.

Data governance provisions require legal frameworks for personal information protection, allow cross-border data flows with limited public policy exceptions, and restrict data localization measures. Consumer protection rules target deceptive practices and spam, while cybersecurity and artificial intelligence commitments promote cooperation, capacity-building, and alignment with international standards. Source code protections prohibit forced disclosure except under defined conditions, and electronic payment provisions aim for safe, efficient, interoperable systems.

Digital inclusion and SMEs rules promote equal participation through skills development, best practice sharing, and targeted support. Cooperation clauses encourage ongoing policy dialogue, pilots, and stakeholder engagement. Dispute settlement favors consultations and good offices, transparency provisions require timely publication and stakeholder

ACKNOWLEDGEMENTS

This report represents a collaborative effort that would not have been possible without the dedication and contributions of numerous individuals.

We extend our sincere thanks to the members of the Digital Trade Cooperation Committee (DTCC), whose collaboration and continuous engagement made this Agreement possible. The DTCC included the following distinguished representatives from DCO Member States: from Bangladesh, Ms. Mursheda Zaman, Mr. Md. Sayed Ali and Mr. Mohammad Abdus Sadek of the Ministry of Commerce; from Cyprus, Lina Tsoumpanou of the Deputy Ministry of Research, Innovation and Digital Policy; from Djibouti, Mohamed Yacin of the Ministry of Digital Economy and Innovation; from Ghana, Edmund Barwuah of the Ministry of Communication, Digital Technology and Innovations; and from Jordan, Eng. Anoud Alabadi, Ms. Heba Al Qarara'a and Ms. Zain Haddad of the Ministry of Digital Economy and Entrepreneurship, together with Ms. Fatima Shneikat of the Ministry of Industry, Trade and Supply.

From Kuwait, Mr. Mubarak Alrajhi of the Central Agency for Information Technology and Ms. Alfajer Alfadhli of the Ministry of Commerce and Industry participated actively. From Nigeria, Engr. Salisu Kaka represented the National Information Technology Development Agency. From Oman, Ms. Azza Al Kindi of the Ministry of Commerce, Industry and Investment Promotion and Ms. Anfal Al Afani of the Ministry of Transport, Communications and Information Technology contributed to the Committee's collective work. From Pakistan, Mr. Syed Muhammad Ammar Naqvi, Barrister Dr. Mobeen Shah and Mr. Saad Zafar Sadiq of the Ministry of Information Technology and Telecommunication, and Mr. Muhammad Ashraf of the Ministry of Commerce took part in the deliberations. From Rwanda, Ms. Diana Umutoni of the Ministry of Trade and Industry and Mr. Brice Wilson Niyobuhungiro of the Ministry of ICT and Innovation were active members. From Saudi Arabia, Mr. Ibrahim Nahid and Ms. Maram Aljashi of the Ministry of Commerce participated in the drafting discussions.

We also gratefully acknowledge the contributions of policymakers, technical experts and stakeholders who participated in consultations and reviewed draft provisions, as well as the enterprises and organizations that offered insights on the broader digital trade environment.

Rao Mehroz Khan of the DCO Secretariat led the drafting of the MDEA and coordinated Member State engagement. The Committee received additional coordination support from Alina Khan, Mohammed Alhabib, and Lubna Alkhudairy of the DCO Secretariat, with drafting assistance provided by Federico Daniele and Tommaso Giardini.

Finally, the DCO extends its appreciation to the Ministers and senior officials of Member States for their continued commitment to strengthening digital cooperation. Their support provided the foundation for the development of this Agreement.

INTRODUCTION

The Model Digital Economy Agreement (MDEA) is a model legal instrument developed to support governments in designing balanced and forward looking rules for the digital economy. It responds to the growing importance of digital trade for growth, innovation and job creation, and to the parallel rise in regulatory diversity across jurisdictions. The Agreement consists of a Preamble and 22 operative provisions, organised around twelve policy areas that are central to digital trade and digital cooperation.

The desirability of promoting digital development and enhancing trade and investment has been affirmed in the Foundation Charter of the Digital Cooperation Organization. DCO's Digital Trade Acceleration Initiative (DTAI) provided the analytical foundation for the Model Digital Economy Agreement (MDEA). The Initiative uncovered a fundamental challenge: regulatory diversity in the complex digital trade landscape can become a barrier to digital trade. Divergent rules and standards can inflate compliance costs and stifle opportunities, especially for smaller economies and smaller firms. To understand these issues systematically, the DTAI documented the regulatory environment of each DCO Member State across twelve policy areas relevant to digital trade, including data protection and cross border data flows, electronic transactions, online consumer protection, cyber security, digital payments, artificial intelligence, unsolicited electronic messages, source code and algorithms, open government data, and the participation of micro, small and medium enterprises in the digital economy.

As part of this work, a survey was conducted with firms from DCO Member States to collect insights on the practical barriers faced in digital trade. More than 1,800 firms participated, providing detailed information on regulatory obstacles, costs and capacity gaps. Stakeholder consultations with government officials helped identify policy priorities, while roundtable discussions among Member States fostered ongoing dialogue. These efforts revealed shared challenges as well as complementary strengths in digital trade across DCO Member States.

DCO Member States represent a diverse array of digital economies, varying in size, infrastructure, skills, and governance structures. While this diversity enriches the global digital landscape, it also presents challenges for digital trade. Existing trade agreements often lack provisions for digital trade and data governance, which highlights the need for tailored agreements that address these gaps and promote digital trade. Countries should establish robust frameworks to enable the seamless exchange of goods, services, and data.

Recognising the importance of addressing these complexities and of enhancing cooperation on digital trade issues, DCO Member States unanimously adopted a resolution at the DCO's 4th General Assembly establishing the Digital Trade Cooperation Committee. The Committee was mandated to serve as a platform for Member States to design a framework for future digital economy agreements. Building on this mandate, the DCO launched the Model Digital Economy Agreement initiative, under which the Committee was tasked with developing a model digital economy agreement for DCO Member States. Drawing on the evidence and analysis generated by the DTAI, and informed by comparative international practice, the Committee developed the MDEA as a model instrument that can be adapted to different national and regional contexts.

The Preamble to the MDEA sets the tone for the Agreement. The 8 recitals of the Preamble present the Parties' shared vision for harnessing digital trade to support economic growth and innovation, while fostering trust, inclusion, and cooperation. From the perspective of treaty interpretation, preambles constitute context for the interpretation of treaty's provisions and presents a treaty's object and purpose, in accordance with Article 31 of the Vienna Convention on the Law of Treaties (VCLT). The Preamble to the MDEA emphasizes that regulatory framework for digital trade should safeguard personal information, ensure cybersecurity, support SMEs, and encourage responsible adoption of emerging technologies.

Articles 1 and 2 respectively provide definitions of relevant terms used in the agreement and address the MDEA scope. Article 2 recalls similar scope-framing provisions contained in other modern digital trade agreements. In particular, the provision clarifies that the MDEA does not apply to services supplied in the exercise of governmental authority, government procurement, and information held or processed by or on behalf of an MDEA Party or measures related to such information. While the commentary does not specifically address Articles 1 and 2, these provisions form an integral part of the MDEA.

The first substantive provision of the MDEA addresses the issue of customs duties and taxation of digital trade products. The treatment of customs duties on electronic transmissions has been a recurring issue in international fora and bilateral trade discussions, often linked to maintaining an open digital environment. A binding commitment to refrain from imposing customs duties on electronic transmissions reflects established practice in modern trade agreements. While prohibiting such duties outright, it preserves the right to levy internal taxes or charges on transmitted content, provided they are applied consistently with the Agreement.

Article 4 of the MDEA engages with non-discrimination of digital products. Provisions on non-discrimination on digital products are designed to prevent protectionist treatment of foreign digital goods in domestic markets. From this perspective, the MDEA requires that a Party accord no less favorable treatment to another Party's products than to like domestic or third-country products. The provision includes safeguards to exclude intellectual property obligations under other agreements, subsidies, broadcasting, and allow preferential treatment under pre-existing trade arrangements. An additional clarification ensures the rule does not require extending treatment beyond commitments already made in services or investment agreements.

Electronic transactions frameworks are a core enabler of cross-border e-commerce, providing legal certainty for paperless business activities. The MDEA requires Parties to establish a domestic legal framework for electronic transactions that aligns with international principles. This approach seeks to avoid unnecessary regulatory burdens and permit flexibility in authentication methods, while recognizing the importance of electronic transferable records. This reflects instruments such as the UNCITRAL Model Law on Electronic Commerce and supports interoperability between systems.
Another element that fosters digitization of business activities is the recognition of the legal equivalence of electronic signatures and authentication mechanisms. Authentication and e-signature rules help ensure trust and enforceability in online transactions across jurisdictions. Commitments on electronic authentication and signatures ensure that the legal validity of a signature cannot be denied solely because it is in electronic form, while protecting the freedom of parties to select authentication methods. Governments may still set performance standards for certain transactions, and Parties are encouraged to work toward mutual recognition to enable cross-border trust.

Moreover, the MDEA contains rules that seek to promote the establishment of an electronic payment framework within the Parties jurisdiction, recognizing their role as key enabler of digital trade. Electronic payments are essential for enabling secure and efficient e-commerce transactions across borders. The MDEA requires the development of electronic payment systems in ways that are safe, efficient, and interoperable, supporting digital trade and competition in payment services.
Article 8 of the MDEA introduces rules to achieve paperless trade administration procedures. Paperless trade provisions streamline customs and border processes by replacing physical paperwork with electronic submissions. Efforts to eliminate paper requirements for trade administration support the shift toward paperless trade. Parties must make trade documents available electronically and recognize them as legally equivalent to paper, except where legal or operational requirements dictate otherwise, following practices seen in the WTO Trade Facilitation Agreement.

The next set of provisions addresses trade-related domestic measures affecting the use and treatment of data. Specifically, the MDEA introduces rules relating to data protection measures, cross-border data transfers, and localization of computing facilities. Data protection measures in digital trade agreements aim to balance privacy rights with the facilitation of cross-border commerce. On personal data protection, the text of Article 9 links safeguarding personal information in electronic commerce to economic and social benefits, and to building consumer trust. Parties must adopt or maintain a legal framework that take account of international principles and publish information on protections and redress mechanisms. It also requires to strengthen enforcement authorities, as well as to promote private sector transparency through the publication of privacy policies.

Rules on cross-border data transfer address the tension between digital trade facilitation and domestic regulatory autonomy. The MDEA facilitates cross-border data transfer by requiring Parties to allow such flows for business purposes, subject to a framed legitimate public policy exceptions that must not be applied in a discriminatory or unnecessarily trade-restrictive manner.

With respect to data issues, the MDEA establishes rules on localization of computing facilities. Data localization requirements can create trade barriers by forcing businesses to mandatorily store or process data within a given jurisdiction. Rules on the location of computing facilities prohibit data localization requirements as a condition for doing business, while affirming regulatory autonomy and allowing proportionate exceptions for legitimate public policy objectives.

The next policy area addressed in the MDEA refers to consumer trust in digital environments. Consumer protection provisions address risks of fraud, misrepresentation, and other harmful practices in online markets. Commitments on online consumer protection in the MDEA combine binding requirements to maintain laws against fraudulent or deceptive practices with non-binding measures on regulatory cooperation and transparency. These cooperation and transparency rules are directed both to governments and businesses. In addition, Article 13 of the MDEA includes rules on unsolicited commercial electronic communications to limit annoyance and fraud towards consumers while preserving legitimate marketing activities. MDEA rules on unsolicited commercial electronic communications require Parties to adopt measures establishing either opt-out mechanisms from unsolicited electronic commercial communications. In addition, the provision further requires Parties to adopt or maintain measures requiring either prior consumer consent to receiving unsolicited electronic marketing communications or another mechanism that allows the minimization of unsolicited electronic marketing communications. Parties must also provide recourse against non-compliant senders and are encouraged to cooperate internationally.

Another key policy area for digital trade relates to the mitigation of domestic and international cybersecurity threats. Cybersecurity commitments in trade agreements aim to secure digital infrastructure while supporting cooperation against cyber threats. With respect to cybersecurity, the MDEA requires Parties to adopt or maintain measures to prevent cybercrime and ensure resilience, with due regard to international standards. The provision also encourages cooperation by directing Parties to strengthen capacity-building, incident response, and workforce development initiatives.
The MDEA also contains rules on artificial intelligence (AI), following a growing trend in digital trade agreements to include non-binding commitments on emerging technologies. The text encourages cooperation on governance, responsible use, and commercialization opportunities of AI technologies. This framework also seek to promote the development of ethical frameworks consistent with international principles like transparency, fairness, and human-centered values.

MDEA also seeks to promote international commitments for the protection of source codes. This policy area stands at the crossroad between private interests and legitimate regulatory concern regarding safety and trustworthiness of digital products. In this sense, source code provisions protect intellectual property and incentives innovation, while allowing legitimate regulatory access. The source code clause prohibits mandatory transfer or access as a market-access condition, with exceptions for specific regulatory or judicial processes under confidentiality safeguards. Article 16 further clarifies that voluntary sharing of source codes under open-source or contractual arrangements does not fall within the scope of the provision.

Contemporary digital trade rules increasingly recognize the role of Small Medium Enterprises (SMEs) in the digital economy and the need to ensure that digital trade is inclusive towards vulnerable and underrepresented communities. Digital inclusion and SME provisions ensure that all segments of society can benefit from digital trade opportunities. The MDEA seeks to advance digital inclusion and SMEs support through cooperation in removing barriers to participation, sharing best practices, and improving professional skills in digital environments. In this context, Article 17 encourages the adoption of tailored measures for SMEs to access platforms, finance, and procurement opportunities.

Cooperation clauses promote ongoing dialogue and technical engagement between Parties to adapt to technological change. Article 18 of the MDEA pursues cooperation between Parties through non-mandatory information exchange on domestic policies, the creation of joint pilot projects, efforts towards interoperability, collaborative support for SMEs, inclusive participation initiatives, and collaborative activities in regional or multilateral for a. The provision further encourages the involvement of the private sector and other relevant stakeholders.

The MDEA also contains a provision on dispute settlement in the evet of disagreement regarding the interpretation or application of the MDEA, as well as for situations of alleged breaches of obligations. Article 19 envisages dispute settlement procedures that seek to achieve resolution of disputes through consultations. Parties also retain the option of resorting to good offices, if consultations fail. The mandates that dispute settlement proceedings are confidential and without prejudice to the rights of either Party in any future proceedings.

The MDEA includes rules on transparency for domestic regulatory activities, so as to foster predictability of regulatory frameworks. Transparency obligations in Article 20 require the publication of relevant measures and, where possible, advance notice and opportunities for public comment, thereby increasing predictability and stakeholder engagement.

Article 21, the closing provision of the MDEA, addresses the need to provide technical assistance and capacity building between the Parties. Technical assistance and capacity-building seek to bridge digital divides through training, infrastructure support, SME digitalization programs, skills development for under-represented groups, and joint research, coordinated through mechanisms matching needs with resources and expertise.

Lastly, this document includes an annex that recapitulate in full the findings of previous DCO works related to international trends and DCO members existing commitments in each policy areas covered in the MDEA.

METHODOLOGY USED TO DRAFT THE COMMENTARY

The commentary is developed through a structured analytical approach designed to situate each provision of the Model Digital Economy Agreement (MDEA) within its broader policy and legal context. The starting point is to frame the policy area covered by the provision, identifying its scope, underlying objectives, and relevance in the regulation of digital trade.

The framing exercise also includes outlining the potential tensions between trade liberalization objectives and domestic regulatory autonomy, as these tensions frequently shape the drafting and interpretation of commitments.

Once the policy area is framed, the analysis assesses trends in scholarly literature, drawing on academic debates to identify the main drivers, benefits, and risks associated with the topic. This literature review is not exhaustive, but it distils key positions and conceptual frameworks that have informed digital trade law and policy.

The methodology then involves a comparative review of existing trade agreements that include provisions on electronic commerce and digital trade. This comparative mapping identifies common drafting patterns, innovative elements, and areas of divergence. Where relevant, the commentary references specific articles in other agreements (e.g., CPTPP, DEPA, USMCA, WTO frameworks) to provide concrete examples of alternative formulations or interpretative precedents.

This allows the analysis to highlight both the novelty and the continuity of the MDEA's approach relative to the evolving corpus of digital trade law. The Commentary also includes the comments and perspectives of the members of the Digital Trade Cooperation Committee.

Each provision is then unpacked paragraph by paragraph, and where relevant, subparagraph by subparagraph. The commentary describes the operative language, assesses its degree of bindingness, and examines its potential operational and interpretative consequences.

This granular analysis ensures that both the overarching policy intent and the specific legal effects are clearly articulated. The method also identifies built-in safeguards, exceptions, and carve-outs, and explains their interaction with other commitments either within the MDEA or in other agreements to which the Parties may be bound.

Finally, each commentary concludes with synthesized observations that draw together the key features of the provision, situate them within the MDEA's architecture, and assess their potential contribution to the Agreement's object and purpose. This structure ensures that the analysis is descriptive and neutral, while offering sufficient depth to serve as a reference for negotiators and policymakers.

MODEL DIGITAL ECONOMY AGREEMENT

MODEL DIGITAL ECONOMY AGREEMENT

Preamble

The Parties to this Agreement,

***RECOGNISING** the transformative potential of digital trade to drive economic growth, innovation, and social prosperity across their jurisdictions;*

***DESIRING** to establish a sound and flexible framework that promotes digital trade, fosters consumer trust, and enhances cross-border cooperation in the digital economy;*

***ACKNOWLEDGING** the importance of protecting personal information, ensuring cybersecurity, and promoting transparent and inclusive digital practices to build confidence in electronic commerce;*

***COMMITTED** to eliminating barriers to digital inclusion, supporting small and medium-sized enterprises (SMEs), and facilitating access to digital economy opportunities for all persons and businesses;*

***EMPHASISING** the need for interoperable and secure electronic transactions, payments, and authentication mechanisms to enable seamless and trustworthy digital trade;*

***ENCOURAGING** the responsible use and development of emerging technologies, such as artificial intelligence, to support ethical, safe, and inclusive digital economies;*

***RESOLVED** to promote paperless trade administration, combat fraudulent practices, and minimize unsolicited commercial electronic communications to enhance the efficiency and integrity of digital trade;*

***DETERMINED** to cooperate in sharing knowledge, best practices, and technical expertise to advance digital inclusion, cybersecurity, and innovation in electronic payments and digital services;*

Article 1: Definitions

For the purposes of this Agreement, unless otherwise provided in this Agreement:

1. 'customs duty' includes any duty or charge of any kind imposed on or in connection with the importation of a good, and any surtax or surcharge imposed in connection with such importation, but does not include any:

a. charge equivalent to an internal tax imposed consistently with Article III:2 of GATT 1994;

b. fee or other charge in connection with the importation commensurate with the cost of services rendered; or

c. antidumping or countervailing duty;

2. 'days' means calendar days;

3. 'enterprise' means any entity constituted or organised under applicable law, whether or not for profit, and whether privately or governmentally owned or controlled, including any corporation, trust, partnership, sole proprietorship, joint venture, association or similar organisation;

4. 'existing' means in effect on the date of entry into force of this Agreement;

5. 'goods' means any merchandise, product, article or material;

6. 'measure' includes any law, regulation, procedure, requirement or practice;

7. 'Party' means any State or separate customs territory for which this Agreement is in force;

8. 'person' means a natural person or an enterprise;

9. 'person of a Party' means a national or an enterprise of a Party;

10. 'personal information' means any information, including data, about an identified or identifiable natural person;

11. ‘SME’ means a small and medium-sized enterprise, including a micro-sized enterprise;

12. ‘computing facilities’ means computer servers and storage devices for processing or storing information;

13. ‘digital certificates’ means electronic documents or files that are issued or otherwise linked to a person who is a party to an electronic communication or transaction for the purpose of establishing the identity of the person;

14. ‘digital payment’ means a transfer by a payer of a monetary value acceptable to a payee made through electronic means;

15. ‘digital trade’ means digitally enabled transactions of trade in goods and services that can either be digitally or physically delivered, and that involve natural and juridical persons;

16. ‘digital product’ means an electronic programme, text, video, image, sound recording, or any other product that is digitally encoded, that is produced for commercial sale or distribution, and that can be transmitted electronically except for a digitised representation of a financial instrument, including money;

17. ‘electronic authentication’ means the process or act of verifying the identity of a party to an electronic communication or transaction, that ensures the integrity of an electronic communication;

18. ‘electronic signature’ means a digitally encrypted stamp of authentication on digital information such as an electronic message or document that confirms that the information originated from the signer and has not been altered;

19. ‘Electronic Trust Services’ means an electronic service consisting of the creation, verification, validation of electronic invoices, electronic signatures, time stamps, certified electronic delivery, and website authentication certificates.

20. 'trade administration documents' means forms issued or controlled by a State Party that must be completed by or for an importer or exporter in connection with the import or export of goods;

21. 'transmitted electronically' means the transfer of digital products using authorised digital networks and interchange systems consisting of, but not limited to, mobile and computer networks; and

22. 'unsolicited commercial electronic communications' means any electronic communication whose primary purpose is the commercial advertisement or promotion of a commercial good or service, sent without the consent of the recipient or despite the explicit refusal of the recipient.

23. 'Content' means any data or information communicated or made available by electronic means, including in the form of text, audio, images, video, software, or other digital signals, whether supplied on a carrier medium or by electronic transmission.

24. 'Covered person' means (a) a natural person of a Party engaged in activities covered by this Agreement; and (b) an enterprise constituted or organized under the laws of a Party.

Article 2: Scope

1. This Agreement shall apply to measures adopted or maintained by a Party that affect trade by electronic means, including digital trade in goods and services, whether delivered digitally or physically. It encompasses all sectors of digital trade unless otherwise specified in this Article or other provisions of the Agreement.

2. This Agreement shall not apply to:

a. services supplied in the exercise of a governmental authority;

b. government procurement, except as otherwise provided in specific provisions of this agreement;

c. information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection, storage, or processing for governmental purposes.

Article 3: Digital Economy Taxation and Custom Duties [1]

1. This Agreement shall apply to measures adopted or maintained by a Party that affect trade 1. No Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of one Party and a person of another Party.

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

3. Such taxes or charges shall not be applied in a manner which affords protection to domestic digital products or services or discriminates, either directly or indirectly, against like digital products or services of another Party.

Article 4: Non-discriminatory Treatment of Digital Products [2]

1. Neither Party shall accord less favourable treatment to a digital product created, produced, published, contracted for, commissioned or first made available on commercial terms in the territory of the other Party, or to a digital product of which the author, performer, producer, developer or owner is a person of the other Party, than it accords to other like digital products.

[1] For the purposes of this Agreement, 'internal taxes or charges' means taxes, fees, or other charges applied on or in connection with the sale, distribution, consumption or use of goods or services (including those supplied by electronic means) within the territory of a Party, other than customs duties or charges upon importation.

[2] The Parties note that any exception to the obligations in this Article shall be interpreted and applied in a manner which is not arbitrary or unjustifiable discrimination, nor a disguised restriction on trade, and shall be construed narrowly in light of the object and purpose of this Agreement.

2. Paragraph 1 shall not apply to the extent of any inconsistencies with a Party's rights and obligations concerning intellectual property contained in another international agreement a Party is party to.

3. The Parties understand that this Article does not apply to subsidies or grants provided by a Party, including government-supported loans, guarantees and insurance.

4. This Article shall not apply to [broadcasting].

5. Notwithstanding Paragraph 1, a Party may adopt or maintain any measure that accords differential treatment to digital products of another Party or a non-Party:

- **a.** under any bilateral or multilateral international agreement in force or signed prior to the date of entry into force of this agreement; or
- **b.** as part of a wider process of economic integration or trade liberalization under prior agreement.

6. For greater certainty, nothing in this Article shall be construed to require a Party to accord treatment to digital products, or to a person involved in their creation, development, or distribution, that would be inconsistent with, or exceed, the rights, obligations, limitations, or conditions undertaken by that Party under any provisions relating to trade in services or investment in any other international agreement to which it is a Party.

Article 5: Domestic Electronic Transaction Framework

1 Each Party shall endeavour to maintain a legal framework governing electronic transactions consistent with international principles.

2. Each Party should:

- **a.** avoid any unnecessary regulatory burden on electronic transactions;
- **b.** avoid limiting the recognition of authentication technology, methods and implementation models; and

3. The Parties recognise the importance of facilitating the use of electronic transferable records.

Article 6: Electronic Authentication and Signature

1. No Party shall deny the legal validity of a signature solely on the basis that the signature is in digital or electronic form, except in circumstances provided for under its law.

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

- **a.** prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction; or

b. prevent parties to an electronic transaction from having the opportunity to establish before judicial or administrative authorities that their transaction complies with any legal requirements with respect to authentication.

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

4. The Parties should work towards the mutual recognition of electronic signatures.

Article 7: Electronic Payments

1. To facilitate the rapid growth of electronic payments, in particular those provided by non-bank, non-financial institution and FinTech enterprises, the Parties recognise the importance of developing an efficient, safe and secure environment for cross-border electronic payments, including by:

a. fostering the adoption and use of internationally accepted standards for electronic payments;

b. promoting interoperability and the interlinking of electronic payment infrastructures; and

c. encouraging innovation and competition in electronic payments services.

2. The Parties further recognise the importance of upholding safety, efficiency, trust and security in electronic payment systems through regulations, and that the adoption and enforcement of regulations and policies should be proportionate to the risks undertaken by the payment service providers.

3. Each Party should:

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

b. endeavour to finalise decisions on regulatory or licensing approvals in a timely manner;

c. not arbitrarily or unjustifiably discriminate between financial institutions and non-financial institutions in relation to access to services and infrastructure necessary for the operation of electronic payment systems;

d. adopt, for relevant electronic payment systems, international standards for electronic payment messaging, for electronic data exchange between financial institutions and services suppliers to enable greater interoperability between electronic payment systems;

e. facilitate the use of open platforms and architectures such as tools and protocols provided for through Application Programming Interfaces ("APIs") and encourage payment service providers to safely and securely make APIs for their products and services available to third parties, where possible, to facilitate greater interoperability, innovation and competition in electronic payments; and

f. facilitate innovation and competition and the introduction of new financial and electronic payment products and services in a timely manner, such as through adopting regulatory and industry sandboxes.

Article 8: Paperless Trading

1. The Parties recognise the importance of eliminating paper forms and documents required for the import, export or transit of goods, to create a paperless border environment for trade.

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

3. Each Party shall accept trade administration documents submitted electronically as the legal equivalent of the paper version of those documents, except where:

- **a.** that Party is subject to a domestic or international legal requirement to the contrary; or
- **b.** doing so would reduce the effectiveness of the trade administration process.

Article 9: Data Protection

1. The Parties recognize the economic and social benefits of safeguarding personal information of users of electronic commerce, acknowledging that such protection is fundamental to enhance consumer confidence and trust in electronic commerce.

2. To this end, each Party shall adopt or maintain a legal framework that safeguards the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party may consider principles and guidelines of relevant international bodies.

3. Each Party shall publish information on the personal information protections it provides to users of electronic commerce, including how:

- **a.** the mechanisms available to individuals for seeking redress in cases of non-compliance; and
- **b.** the obligations imposed on enterprises to ensure compliance with applicable legal requirements.

4. Each Party should:

- **a.** establish national data protection authorities or other relevant bodies responsible for the enforcement of personal data protection laws:
- **b.** build capacities of their national data protection authorities or other relevant bodies responsible for the enforcement of personal data protection laws
- **c.** maintain dialogue on personal data protection and sharing of knowledge, research and best practices with other State Parties.

5. Each Party shall promote the publication, by businesses in its territory, of their policies and procedures related to the protection of personal information.

Article 10: Cross-border Data Transfers

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

2. Each Party shall, subject to an Annex on Cross-border Data Transfers, allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of business of a covered person.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

- **a.** is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
- **b.** does not impose restrictions on transfers of information greater than are required to achieve the objective.

4. Parties shall craft an Annex on Cross-border Data Transfers, which shall, among others, set out legitimate public policy objectives, lay out how data may be used, modalities of trusted data transfers, restrictions on sharing of data to third parties, including, among others, data protection regulations that may be applied by regulators.

Article 11: Location of Computing Facilities

1. The Parties acknowledge that each Party may establish its own regulatory requirements for the use of computing facilities, including measures to safeguard the security and confidentiality of communications.

2. No Party shall mandate that a covered person use or locate computing facilities within its territory as a prerequisite for conducting business in that territory.

3. Nothing in paragraph 2 shall prevent a Party from adopting or maintaining measures to achieve a legitimate public policy objective, including: (a) protection of personal data and privacy; (b) financial stability and prudential supervision (including effective regulatory and supervisory access); (c) protection of essential security interests; (d) integrity and resilience of critical information infrastructure; (e) protection of public health; or (f) compliance with lawful access obligations in criminal matters; provided that such measures are not applied in a manner constituting arbitrary or unjustifiable discrimination or a disguised restriction on trade, and are not more restrictive than necessary to achieve the objective.

4. A Party shall not require a covered financial service supplier to use or locate computing facilities in its territory as a condition for conducting business, provided that the Party's competent authorities have immediate, direct, complete and ongoing access, on a timely basis and in a usable form, to information processed or stored outside its territory that they are entitled to obtain for regulatory or supervisory purposes, subject to appropriate confidentiality and data-protection safeguards.

5. Each Party shall list in the Annex on Computing Facilities Safeguards any sector-specific or measure-specific localization requirement it maintains, indicating the objective pursued and the applicable conditions and safeguards; a Party may modify its listing upon notification to the other Parties.

Article 12: Online Consumer Protection

1. The Parties recognise the importance of maintaining and adopting transparent and effective measures to protect consumers from fraudulent or deceptive commercial practices in electronic commerce.

2. To this end, each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.

3. The Parties shall exchange information and experiences related to national approaches for the protection of consumers engaging in electronic commerce.

4. The Parties recognise the importance of cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border electronic commerce in order to enhance consumer welfare.

5. Each Party should publish information on the consumer protection it provides to users of electronic commerce.

6. The Parties should encourage businesses to publish their policies and procedures related to online consumer protection

Article 13: Unsolicited Commercial Electronic Communications

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

- **a.** require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages;
- **b.** require either:

i. consent, as specified according to the laws and regulations of each Party, of recipients to receive commercial electronic messages; or

ii. supplier of unsolicited commercial electronic to provide for the minimization of unsolicited commercial electronic messages.

2. Each Party shall provide recourse against suppliers of unsolicited commercial electronic communications that do not comply with the measures adopted or maintained pursuant to paragraph 1.

3. The Parties should cooperate in the regulation of unsolicited commercial electronic communications.

Article 14: Cybersecurity

1. The Parties have a shared vision to promote secure digital trade to achieve global prosperity and recognise that cybersecurity underpins the digital economy.

2. The Parties shall adopt or maintain measures to ensure cybersecurity to prevent and address cybercrime within its jurisdiction. In the developing or maintaining such measures, each Party shall have due regards to standards, guidelines, and best practice set forth in relevant international instruments.

3. The Parties recognise that threats to cybersecurity undermine confidence in digital trade and shall endeavour to:

a. build the capabilities of their national entities responsible for computer security incident response;

b. using existing collaboration mechanisms to cooperate to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties; and

c. workforce development in the area of cybersecurity, including through possible initiatives relating to the training and development of youths, improving diversity and mutual recognition of qualifications.

Article 15: Artificial Intelligence

1. The Parties recognise that the use and adoption of Artificial Intelligence (AI) technologies have grown increasingly widespread in the digital economy. The Parties should cooperate, in accordance with their respective relevant policies, through:

a. sharing 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; and

c. encouraging commercialisation opportunities and collaboration between researchers, academics and industry.

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

3. To this end, the Parties should promote the adoption of ethical and governance frameworks that support the trusted, safe and responsible use of AI technologies (AI Governance Frameworks). In adopting AI Governance Frameworks, the Parties should take into consideration internationally recognised principles or guidelines, including explainability, transparency, fairness and human-centred values.

4. The Parties shall, where appropriate and consistent with domestic law, promote transparency and accountability in the use of automated decision-systems and algorithmic tools in trade-related administrative processes (e.g., customs, licensing, certification), including sharing best practices on explainability, human oversight and redress mechanisms.

Article 16: Source Code

1. The Parties shall not require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.

2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure and to the following conditions:

a. A regulatory body or judicial authority of a State Party, requiring transfer or access to a source code or algorithm thereof under this Article, shall protect the source code of the software or an algorithm expressed in that source code preserved and availed to them by a person of the State Party against unlawful access, acquisition, or appropriation by a third party.

b. Any such access shall be: (i) necessary to achieve the stated purpose and not applied in a manner constituting arbitrary or unjustifiable discrimination or a disguised restriction on trade; (ii) strictly limited in scope, format and duration to what is required; (iii) subject to legally enforceable confidentiality and use-limitation obligations no less protective than those applicable to undisclosed information under the Party's law; (iv) implemented through secure review arrangements avoiding disclosure to competitors; and (v) without prejudice to the information's status as a trade secret, where claimed by the trade secret owner.

3. For greater certainty, paragraph 1 does not apply to the voluntary transfer of, or granting of, access to a source code owned by a person of another Party under open-source licenses, such as in the context of open-source coding, or on a commercial basis, such as in the context of a freely negotiated contract.

4. Before requiring access under paragraph 2, the authority shall provide prior written notice stating legal basis, purpose, and scope; consider less intrusive means proposed by the affected person; issue a reasoned decision within a reasonable period (ordinarily within 90 days of complete submission, unless justified by case complexity); and ensure access to prompt and impartial review or appeal, with appropriate remedies.

Article 17: SMEs and Digital Inclusion

1. The Parties recognise the importance of digital inclusion to ensure that all people 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.

3. To this end, the Parties should cooperate on matters relating to digital inclusion, including:

a. 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. 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

f. other areas as jointly agreed by the Parties.

4. The Parties recognise the role played by SMEs in economic growth and job creation, and the need to address the barriers to participation in digital trade for those entities. To this end, the Parties should:

a. foster close cooperation on digital trade between SMEs of the Parties;

b. encourage their participation in platforms that help link them with international suppliers, buyers, and other potential business partners; and

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

Article 18: Cooperation

1. The Parties recognize the importance of strengthening cooperation to support the development of a trusted, secure, and open digital economy. The Parties shall cooperate to advance the objectives of this Agreement through dialogue, information exchange, and jointly agreed activities.

2. The parties shall endeavor to cooperate on matters related to this Agreement, including:

a. policy and regulatory exchanges on digital trade, personal data protection, cybersecurity, and trust frameworks;

b. pilots and regulatory sandboxes, including on digital identity, e-invoicing, and cross-border payments;

c. interoperability work on standards, conformity assessment, and mutual recognition where appropriate;

d. SME support, including matchmaking platforms and access to finance tools;

e. initiatives that promote participation of women, youth, persons with disabilities, and rural communities in the digital economy;

f. participation and joint proposals in relevant regional and multilateral fora.

3. The Parties shall encourage participation, as appropriate, by private sector, academia, technical bodies, and civil society in cooperation activities.

Article 19: Dispute Settlement

1. The Parties shall at all times endeavor to agree on the interpretation and application of this Agreement, and shall make every attempt through cooperation and consultations to arrive at a mutually satisfactory resolution of any matter that might affect its operation or application.

2. This Article shall apply to any dispute between the Parties concerning the interpretation, application, or a Party's failure to carry out its obligations under this Agreement.

3. Cooperation and Consultations:

a. a Party may request consultations with another Party with respect to any matter covered by this Agreement.

b. The requesting Party shall submit a written request to the other Party, specifying the measure at issue and the legal basis for its complaint.

c. The requested Party shall respond to the request within thirty (30) days of its receipt and shall enter into consultations in good faith within sixty (60) days of the date of the request.

d. The Parties shall make every effort to resolve the dispute through these consultations, including through the exchange of information and best practices.

4. Use of Good Offices:

a. If the Parties fail to resolve the dispute through consultations within sixty (60) days of the date of the request, either Party may request the good offices of a mutually agreed-upon party.
b. The purpose of good offices is to assist the Parties in resuming direct negotiations or to find a mutually acceptable method of pacific settlement.
c. The good offices process is voluntary and shall be undertaken only with the consent of both disputing Parties.
d. The proceedings and any information shared during the good offices shall be strictly confidential and without prejudice to the rights of either Party in any future proceedings.

5. If the matter has not been resolved within 90 days of receipt of the request for consultations (or such other period as the Parties may agree), the Parties may submit the dispute to arbitration in writing. The forum, procedural rules, place (seat) of arbitration, language, and the method of appointment of arbitrators shall be agreed by the Parties in writing for the purposes of that dispute.

6. An arbitral award rendered pursuant to paragraph 19.5 shall be final and binding on the Parties to the arbitration. The award shall set out the tribunal's findings of fact, its determinations on the issues in dispute, and the reasons for its determinations. Unless the Parties agree otherwise, each Party shall bear its own costs, and the costs of the tribunal shall be shared equally.

Article 20: Transparency

1. Each Party shall promptly publish, or otherwise make publicly available, its laws, regulations, procedures, and administrative rulings of general application relating to matters covered by this Agreement, in a manner that enables interested persons and other Parties to become acquainted with them.

2. When possible, a Party shall:

a. publish in advance proposed measures of general application; and
b. provide a reasonable opportunity for interested persons to comment.

Article 21: Technical Assistance and Capacity Building

1. The Parties recognize that technical assistance and capacity building support effective implementation of this Agreement and help narrow digital divides.

2. Subject to the availability of resources and on mutually agreed terms, cooperation may include:

- **a.** training for officials and regulators on digital trade, data governance, cybersecurity, and competition in digital markets;
- **b.** support for interoperable digital public infrastructure and secure networks;
- **c.** SME digitalization programs, including e-payments, digital IDs, and logistics solutions;
- **d.** initiatives that advance digital skills and literacy for under-represented groups;
- **e.** joint research, pilots, and testbeds with the private sector and technical bodies.

3. The Parties shall coordinate assistance and may mobilize a DCO MDEA Implementation Facility under the discipline of the Digital Space Accelerators (DSA) to match priority needs with funding and expertise.

Article 22: Relationship with Other Agreements

1. In respect of matters within the scope of this Agreement, each Party reaffirms its rights and obligations under other agreements to which one or more other Parties are party, including under the WTO Agreement.

2. Nothing in this Agreement shall be construed to derogate from any right or obligation a Party has under existing agreements to which one or more other Parties are party, including under the WTO Agreement.

COMMENTARY

PREAMBLE TO THE MDEA

Context and Scope

(1) Preambles in treaties serve as introductory statements that articulate the general objectives, motivations, and principles guiding the agreement. While they do not contain binding obligations, preambles provide essential context for understanding the overall purpose of the treaty. They often highlight shared values, policy goals, and areas of cooperation, thereby helping to situate the operative provisions within a broader normative framework. As such, preambles can contribute to shaping the interpretation of treaty terms, particularly in cases where provisions are ambiguous or open to multiple readings.

(2) Under international law, including Article 31(2) of the Vienna Convention on the Law of Treaties (VCLT), the preamble forms part of the "context" to be considered when interpreting treaty terms. This means that preambular language may inform the meaning of specific provisions by clarifying the intention of the Parties. Moreover, the preamble is where parties express the object and purpose of the treaty. Together with the context, a treaty's object and purpose serve to shed light on the ordinary meaning of treaty text in accordance with Article 31 of the VCLT. While it cannot override explicit operative language, a preamble can assist in resolving interpretive uncertainties or reinforcing a particular reading consistent with the treaty's broader aims. As such, preambles play a central role in treaty interpretation and application.

Preamble to the MDEA

The Parties to this Agreement,
RECOGNISING the transformative potential of digital trade to drive economic growth, innovation, and social prosperity across their jurisdictions;
DESIRING to establish a sound and flexible framework that promotes digital trade, fosters consumer trust, and enhances cross-border cooperation in the digital economy;
ACKNOWLEDGING the importance of protecting personal information, ensuring cybersecurity, and promoting transparent and inclusive digital practices to build confidence in electronic commerce;
COMMITTED to eliminating barriers to digital inclusion, supporting small and medium-sized enterprises (SMEs), and facilitating access to digital economy opportunities for all persons and businesses;

EMPHASISING the need for interoperable and secure electronic transactions, payments, and authentication mechanisms to enable seamless and trustworthy digital trade;

ENCOURAGING the responsible use and development of emerging technologies, such as artificial intelligence, to support ethical, safe, and inclusive digital economies;

RESOLVED to promote paperless trade administration, combat fraudulent practices, and minimize unsolicited commercial electronic communications to enhance the efficiency and integrity of digital trade;

DETERMINED to cooperate in sharing knowledge, best practices, and technical expertise to advance digital inclusion, cybersecurity, and innovation in electronic payments and digital services;

Have agreed as follows:

Commentary

(3) The Preamble to the MDEA sets out the shared objectives and normative foundations that guide its substantive provisions. While not legally binding, the preamble offers crucial interpretive value under Article 31 VCLT, helping to contextualize the rights and obligations that follow. The structure of the Preamble to the MDEA weaves together economic, technological, and societal aims, presenting digital trade not only as a tool for market access but also as a driver of inclusive growth, innovation, and cross-border collaboration. The text mirrors similar language found in the preambles of the Digital Economy Partnership Agreement (DEPA), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), reflecting a growing international convergence around the role of digital trade in sustainable development and economic transformation.

(4) The first recital recognizes digital trade as a transformative force for economic growth, innovation, and social prosperity. This framing reflects a consensus seen in other international digital trade instruments that position digitalization as essential to competitiveness and long-term prosperity. The second recital expresses a desire to build a flexible yet predictable regulatory framework to support digital trade, foster consumer trust, and deepen international cooperation. Its emphasis on adaptability acknowledges the dynamic nature of the digital economy and the need for resilient regulatory responses. The third recital introduces trust-enhancing pillars (data protection, cybersecurity, and transparency) as prerequisites for a stable digital environment.

(5) The fourth recital brings attention to digital inclusion and the participation of SMEs, recognizing their centrality to equitable digital transformation. The fifth recital highlights the technical foundations of digital trade (interoperable and secure infrastructures) and highlights the shared objective of creating a regulatory environment for digital trade that favors interconnectivity and resilience. The sixth recital introduces emerging technologies, with a specific focus on artificial intelligence, and encourages their responsible use.

(6) The seventh recital underscores operational aspects of digital trade, including the promotion of paperless trade, anti-fraud efforts, and limits on unsolicited digital communications. The final recital expresses a determination to cooperate on knowledge-sharing and technical capacity-building, particularly in areas such as cybersecurity and digital payments.

(7) Together, these recitals form a cohesive vision of digital trade as a multidimensional policy space, requiring a balance of market openness, technological development, consumer protection, and inclusive governance. The preamble highlights both the ambitions and the values that shape this agreement and reflects the influence of recent digital trade instruments while adding emphasis on inclusion and cooperation. It thereby serves as an important interpretive aid, clarifying the intent behind the commitments and signaling the Parties' collective direction in shaping the digital economy.

DIGITAL ECONOMY TAXATION AND CUSTOMS DUTIES

Context and Scope

(1) Domestic regulatory policies on digital economy taxation and customs duties increasingly address the challenge of adapting traditional fiscal frameworks to the realities of cross-border digital trade. In particular, one key area of focus has been the treatment of electronic transmissions, such as software, e-books, or audiovisual content delivered online. Many jurisdictions have opted not to impose customs duties on these transmissions, aligning with the long-standing WTO moratorium and similar commitments in regional trade agreements. At the same time, however, governments retain the ability to impose internal taxes, such as Value Added Tax (VAT), on content transmitted electronically, provided such measures are applied in a non-discriminatory and transparent manner. Regulatory approaches in this area seek to strike a balance between preserving open digital trade flows and maintaining domestic fiscal policy space, particularly as digital consumption continues to grow across borders.

Article 3 – Digital Economy Taxation and Customs Duties

1. No Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of one Party and a person of another Party.

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

3. Such taxes or charges shall not be applied in a manner which affords protection to domestic digital products or services or discriminates, either directly or indirectly, against like digital products or services of another Party.

Commentary

(2) This provision sets out the Parties' shared commitment to ensuring the free flow of electronic transmissions across borders by prohibiting the imposition of customs duties on such transmissions. It addresses a foundational aspect of digital trade governance: the treatment of intangible digital goods and services – such as software, data, audiovisual content, or cloud-based products – when transmitted electronically. The objective is to support an open, predictable, and non-discriminatory environment for digital commerce by shielding it from the trade-restrictive effects of tariff barriers. The provision reflects a widely supported norm in international digital trade negotiations and reinforces the moratorium first adopted by WTO Members in 1998 and regularly extended since.[3]

(3) Paragraph 1 contains the core obligation: no Party shall impose customs duties on electronic transmissions between a person of one Party and a person of another Party. This applies not only to the digital transmission itself but also to the content transmitted electronically. The language mirrors similar provisions in most regional and multilateral digital trade agreements.[4] By using "shall not," the obligation is clearly binding, and its effect is to prevent the use of customs duties as a barrier to digital trade. This is particularly relevant for countries considering the treatment of digital goods and services under their customs codes, as the provision ensures that such intangible transmissions are not subject to traditional import tariffs. The widespread adoption in trade agreements of a prohibition on custom duties on electronic transmission makes this binding obligation generally accepted as standard practice.

[3] WTO Ministerial Conference, Declaration on Global Electronic Commerce, WT/MIN(98)/DEC/2, adopted on 20 May 1998. WTO Members consistently renewed the practice of not imposing custom duties on electronic transmissions at every Ministerial Conference. Last renewal: WTO Ministerial Conference, Work Programme on Electronic Commerce, WT/MIN(24)/38, adopted on 4 March 2024.

[4] EU-Chile Framework Agreement, Chapter 26, Article 7; EU-Japan EPA, Chapter 8, Article 72; EU-New Zealand FTA, Chapter 12, Article 6(1); EU-UK TCA, Article 203(2); EU-Mexico Global Agreement, Chapter 16, Article 3(1); EU-Singapore, Chapter 8, Article 58; EU-Vietnam FTA, Chapter 8, Article 51; AfCFTA Digital Trade Protocol, Article 6(1); DEPA, Module 3, Article 2(2); Australia-Singapore DEA, Article 5(1); CPTPP, Chapter 14, Article 3(1); USMCA, Chapter 19, Article 3(1); RCEP, Chapter 12, Article 11(1); US-Morocco FTA, Chapter 14, Article 3(1); US-Bahrain FTA, Chapter 13, Article 3(1); GCC-Singapore FTA, Chapter 7, Article 4(1); EU-Canada CETA, Chapter 16, Article 3(1); Jordan-Canada, Chapter 3, Article 1(1); WTO ECA, Article 11(3).

(4) Paragraph 2 introduces a clarifying exception, preserving the Parties' ability to impose internal fiscal measures on digital products, provided these measures are applied consistently with the agreement's broader commitments. Specifically, while customs duties are prohibited, internal taxes, fees, or charges are permitted so long as they are not inconsistent with other obligations contained in the MDEA. This distinction is consistent with WTO law, particularly the GATT distinction between border measures (Article II) and internal measures (Article III). Similar language can be found in other trade agreements to balance liberalization with domestic revenue needs.[5] The paragraph allows Parties to maintain their fiscal sovereignty over digital goods and services consumed domestically while preventing the use of border measures as disguised barriers to trade.

(5) Paragraph 3 maintains that although the parties of the agreement have the right to impose internal taxation or charges, they should not be applied in a manner that discriminates against like products or services of another party. This reinforces the notion that domestic taxes are not applied in a manner which can act as a disguised restriction on trade.

(6) Taken together, this provision seeks to foster a liberal and non-discriminatory digital trade environment while recognizing the legitimate role of governments in domestic taxation of digital content. It reduces legal uncertainty for businesses, especially SMEs and digital service providers, by affirming that cross-border digital transactions will not be subject to unpredictable customs duties. At the same time, it ensures that governments can still collect internal taxes in a manner consistent with the agreement's rules. In the broader context of digital trade governance, this rule helps to maintain the openness of the global digital economy and avoid fragmentation caused by unilateral digital tariffs—especially as international debates on the taxation of the digital economy (e.g., under the OECD Inclusive Framework) continue to evolve.

[5] EU-New Zealand FTA, Chapter 12, Article 6(2); EU-Mexico Global Agreement, Chapter 16, Article 3(2); AfCFTA Digital Trade Protocol, Article 6(2); US-Oman FTA, Chapter 14, Article 3(1); DEPA, Module 3, Article 2(1); Australia-Singapore DEA, Article 5(2); CPTPP, Chapter 14, Article 3(2); USMCA, Chapter 19, Article 3(2); RCEP, Chapter 12, Article 11(5); EU-Canada CETA, Chapter 16, Article 3(2); Jordan-Canada, Chapter 3, Article 1(2); WTO ECA, Article 11(4).

Non-Discriminatory Treatment of Digital Products

Context and Scope

(1) Provisions on the non-discriminatory treatment of digital products in digital trade agreements are designed to ensure that digital content and software – such as e-books, digital music, videos, software applications, and games – are treated no less favorably than their domestic or third-country equivalents. These provisions have emerged as features of modern digital economy agreements, addressing a gap left by older trade frameworks which did not foresee the emergence of intangible digital goods. The primary objective is to prevent protectionist measures that could distort trade in digital products, such as the imposition of discriminatory taxes, regulatory hurdles, or market access restrictions based on the origin or ownership of the product.

Article 4 – Non-Discrimination of Digital Products [6]

1.Neither Party shall accord less favourable treatment to a digital product created, produced, published, contracted for, commissioned or first made available on commercial terms in the territory of the other Party, or to a digital product of which the author, performer, producer, developer or owner is a person of the other Party, than it accords to other like digital products.

2. Paragraph 1 shall not apply to the extent of any inconsistencies with a Party's rights and obligations concerning intellectual property contained in another international agreement a Party is party to.

3. The Parties understand that this Article does not apply to subsidies or grants provided by a Party, including government-supported loans, guarantees and insurance.

4. This Article shall not apply to [broadcasting].

5. Notwithstanding Paragraph 1, a Party may adopt or maintain any measure that accords

[6] The Parties note that any exception to the obligations in this Article shall be interpreted and applied in a manner which is not arbitrary or unjustifiable discrimination, nor a disguised restriction on trade, and shall be construed narrowly in light of the object and purpose of this Agreement.

differential treatment to digital products of another Party or a non-Party:

a. under any bilateral or multilateral international agreement in force or signed prior to the date of entry into force of this agreement; or

b. as part of a wider process of economic integration or trade liberalization under prior agreement.

6. For greater certainty, nothing in this Article shall be construed to require a Party to accord treatment to digital products, or to a person involved in their creation, development, or distribution, that would be inconsistent with, or exceed, the rights, obligations, limitations, or conditions undertaken by that Party under any provisions relating to trade in services or investment in any other international agreement to which it is a Party.

Commentary

(2) This provision establishes a non-discrimination obligation for digital products, aiming to prevent a Party from according less favorable treatment to digital products associated with the other Party than to like digital products of domestic or third-party origin. The clause reflects a commitment to treating digital content and products on a level playing field. It combines binding commitments with specified limitations and exceptions to ensure regulatory flexibility and policy space, particularly in relation to intellectual property, subsidies, and pre-existing international agreements. The final paragraph further clarifies that this obligation does not override existing commitments in services or investment disciplines in other international agreements, reinforcing internal coherence across a Party's treaty commitments.

(3) Paragraph 1 introduces the central non-discrimination obligation, requiring each Party to treat digital products of the other Party no less favorably than like digital products of any origin. The scope of this clause encompasses a broad range of connections to the other Party, including the location of commercial availability and the nationality or residence of creators, developers, or owners. This language mirrors provisions found in digital trade chapters of agreements such as the CPTPP and the USMCA, which similarly prohibit discriminatory treatment based on origin.[7] This obligation is binding and represents a key discipline to prevent digital protectionism, thereby fostering an open digital market environment. The reference to "like digital products" means that the obligation applies to foreign digital products that compete in the Party's market with either domestic digital products or those from other countries.

[7] CPTPP, Chapter 14; Article 4(1); USMCA, Chapter 19; Article 4(1); DEPA; Module 3, Article 3(1); Australia-Singapore DEA, Article 6(1). For Non-discrimination clauses using a different language and structure, see also: GCC-Singapore FTA, Chapter 7, Article 4(3) and 4(4); US-Oman FTA, Chapter 14, Article 3(3) and 3(4); US-Bahrain FTA, Chapter 13, Article 4; AfCFTA Digital Trade Protocol, Article 7(1) and 7(2);

(4) Paragraph 2 qualifies the scope of the non-discrimination obligation by carving out inconsistencies related to a Party's intellectual property rights and obligations under other international agreements. This safeguard acknowledges the complexity of overlapping treaty regimes and avoids conflicts where intellectual property commitments might otherwise be undermined. This type of clause is common in digital trade disciplines and serves to preserve coherence with existing international obligations, such as those under the TRIPS Agreement or WIPO treaties. The CPTPP, the DEPA, and the Australia-Singapore DEA contain equivalent exemption. [8]

(5) Paragraph 3 confirms that the non-discrimination obligation does not extend to subsidies or grants, including those provided through government-supported financial instruments. This language is consistent with digital trade provisions in the CPTPP and the DEPA, where subsidies are excluded from the scope of non-discrimination rules, allowing governments to support domestic digital industries and innovation through public funding without contravening trade obligations.[9] It reinforces regulatory flexibility and reflects standard practice in international economic agreements.

(6) Paragraph 4 explicitly excludes broadcasting from the scope of this provision. The term remains bracketed, suggesting that Parties have the option to include any sector within the scope of this exemption. Exclusions for broadcasting are present in several free trade agreements, such as the Australia–Singapore DEA and the CPTPP, where cultural policy sensitivities around audiovisual services necessitate carve-outs.[10]

(7) Paragraph 5 provides two exceptions allowing differential treatment under certain circumstances. Subparagraph (a) permits such treatment when consistent with pre-existing international agreements signed before this agreement's entry into force. Subparagraph (b) extends the exception to differential treatment applied as part of broader processes of economic integration or trade liberalization under prior agreement. These exceptions ensure that the non-discrimination rule does not inadvertently override long-standing arrangements or commitments in other integration frameworks, including customs unions or regional trade agreements.

---

[8] CPTPP, Chapter 14, Article 4(2); Australia-Singapore DEA, Article 6(2); DEPA; Module, 3, Article 3(2); USMCA, Chapter 19, Article 4(2).

[9] USMCA, Chapter 19, Article 4(2); CPTPP, Chapter 14, Article 4(3); Australia-Singapore DEA, Article 6(3); DEPA; Module, 3, Article 3(3)

[10] Australia-Singapore DEA, Article 6(4); CPTPP, Chapter 14, Article 4(4); DEPA; Module 3, Article 3(4).

(8) Paragraph 6 introduces an important interpretative safeguard. It clarifies that Article 4 does not require the Parties to grant most favorable nation treatment to digital products originating from non-Parties nor to act in contravention to obligations they have undertaken in other international agreements. Paragraph 6 does not contain any obligations but provides interpreting guidance on the scope of the provision. This ensures consistency across treaty regimes and protects a Party from being compelled to extend trade or investment liberalization beyond its existing commitments. Language fulfilling a similar purpose can be found, for example, in the US-Oman FTA and the US-Bahrain FTA, where obligations under digital trade chapters are expressly subordinated to non-conforming measures and exceptions in investment and services chapters.[11] However, unlike those agreements, where the electronic commerce chapter forms part of a broader trade agreement containing explicit services and investment chapters, the MDEA is a standalone instrument focused exclusively on digital trade. As such, the carve-out could not rely on cross-references to other chapters within the same agreement. Instead, the provision achieves a comparable result by establishing a general safeguard clause that exempts from the scope of the non-discrimination obligation any treatment exceeding the rights, obligations, limitations, or conditions a Party has undertaken in the context of other international agreements on services or investment. This drafting approach seeks to ensure legal coherence across different treaty frameworks.

(9) Parties retain the sovereign right to define and regulate what constitutes unethical, obscene, or harmful content in accordance with their domestic laws, cultural norms, and policy objectives. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures to restrict or regulate such content, consistent with the legitimate public-policy exceptions provided elsewhere in this Agreement.

(10) Taken together, this provision articulates a circumscribed commitment to non-discriminatory treatment of digital products. It reflects established practice in digital trade agreements while incorporating necessary carve-outs to preserve domestic regulatory autonomy and treaty coherence. The clause seeks to strike a balance between openness and flexibility, ensuring that liberalization commitments in digital trade do not undermine pre-existing rights or impose unintended obligations in overlapping legal frameworks.

[11] US-Oman FTA, Chapter 14, Article 3(5); US-Bahrain FTA, Chapter 13, Article 4(3);

ELECTRONIC TRANSACTIONS

Context and Scope

(1) Regulatory policies regarding electronic transactions play a fundamental role in enabling trusted, secure, and efficient digital commerce. At their core, these policies aim to establish a legal framework that gives electronic communications and transactions the same validity and enforceability as their paper-based counterparts. This typically involves enacting domestic legislation that recognizes contracts formed electronically, ensures the legal equivalence of electronic and traditional signatures, and provides clarity on the use of digital records. Such frameworks are essential for reducing legal uncertainty, encouraging private sector adoption of digital tools, and fostering consumer confidence in online transactions.

(2) A critical dimension of these frameworks involves regulating electronic authentication and electronic signatures, both of which underpin the legal validity and security of online transactions. Electronic authentication refers to the technical and legal processes used to verify the identity of the parties involved in a transaction, which may include passwords, biometric data, or digital certificates. Regulatory approaches vary: some countries adopt technology-neutral models, allowing parties to choose the authentication method that best suits their needs, while others prescribe performance-based standards or certification requirements, particularly for high-risk transactions. Similarly, electronic signature regulation involves determining when and how such signatures are legally recognized. Most modern frameworks distinguish between simple electronic signatures and digital or advanced electronic signatures, the latter typically requiring encryption and certification by a recognized authority. By providing legal recognition and regulatory clarity, these measures facilitate cross-border interoperability and ensure that electronic transactions are both reliable and enforceable within and between jurisdictions.

Article 5 – Domestic Electronic Transactions Framework

1. Each Party shall endeavour to maintain a legal framework governing electronic transactions consistent with international principles.

2. Each Party should:

a. avoid any unnecessary regulatory burden on electronic transactions;

b. avoid limiting the recognition of authentication technology, methods and implementation models; and

3. The Parties recognise the importance of facilitating the use of electronic transferable records.

Commentary

(3) This provision establishes a foundational framework for the legal recognition and facilitation of electronic transactions. By using soft legal obligation, encourages Parties to adopt and maintain electronic transaction regimes that are consistent with international principles, while encouraging regulatory approaches that are technology-neutral, innovation-friendly, and supportive of emerging practices such as the use of electronic transferable records. The provision blends binding obligations (e.g., maintaining a legal framework) with non-binding guidance (e.g., avoiding unnecessary burdens), reflecting a pragmatic approach to digital trade regulation that accommodates differing levels of regulatory maturity while encouraging convergence toward global best practices.

(4) Paragraph 1 introduces a soft obligation for each Party to "endeavour to maintain a legal framework governing electronic transactions consistent with international principles." The term "endeavour to" recognizes different domestic readiness levels and recognizes capacity variance. These instruments promote the functional equivalence between paper and electronic documents and signatures, and endorse technology neutrality – key attributes for legal interoperability. This paragraph echoes similar commitments found in other agreements, albeit with a soft legal obligation through the use of terms "shall endeavour" to.Other agreements, such as the CPTPP and the USMCA, also require Parties to establish electronic transaction regimes consistent with international standards, and they always explicitly refer to the UNCITRAL Model Law on Electronic Commerce and/or the United Nations Convention on the Use of Electronic Communications in International Contracts.[12]

(5) Paragraph 2 sets out soft obligations, recommending that Parties adopt good regulatory practices when implementing their legal frameworks for electronic transactions. Subparagraph (a) encourages Parties to avoid "unnecessary regulatory burden," a formulation that supports streamlined, enabling environments for digital trade. This aligns with regulatory approaches found in several electronic commerce and digital trade chapters in international agreements, which equally seek to minimize regulatory burdens on electronic transactions.[13] Subparagraph (b) highlights the principle of technology neutrality by discouraging limitations on authentication technologies or implementation models. This language promotes market-driven adoption of technologies such as electronic signatures, digital certificates, or blockchain-based methods, and avoids regulatory adherence to specific solutions.

[12] CPTPP, Chapter 14, Article 5(1); USMCA, Chapter 19, Article 5(1); DEPA, Module 2, Article 3(1); Australia-Singapore DEA, Article 8(2); RCEP, Chapter 12, Article 10(1); WTO ECA, Article 4(1).
[13] DEPA; Module 2, Article 3(3)(a); Australia-Singapore DEA, Article 8(3)(a); CPTPP, Chapter 14, Article 5(2)(a); USMCA, Chapter 19, Article 5(2)(a); RCEP, Chapter 12(2); WTO ECA, Article 4(2)(a).

(6) Paragraph 3 shifts attention to the emerging area of electronic transferable records, recognizing their growing significance in digitizing international trade documents such as bills of lading, promissory notes, and warehouse receipts. The reference to "facilitating the use" of these records signals a soft commitment that aligns with developments under trade agreements such as the DEPA and the Australia-Singapore DEA. The recognition of transferable records here places the provision at the frontier of digital trade law, supporting paperless trade and trade finance digitization initiatives.

(7) Overall, this provision plays a pivotal role in establishing the legal infrastructure needed for digital trade. It aims to promote regulatory coherence, innovation, and international legal interoperability. By grounding domestic electronic transaction laws in internationally accepted principles and encouraging openness to new technologies, the provision fosters both legal certainty and adaptability. It also contributes to broader digital economy goals, such as reducing transaction costs, enhancing trust in online commerce, and accelerating the dematerialization of trade documentation. While it allows regulatory flexibility, the provision signals a clear signal toward harmonized, innovation-enabling legal frameworks for digital trade.

Article 6 – Electronic Authentication and Signatures

1. No Party shall deny the legal validity of a signature solely on the basis that the signature is in digital or electronic form, except in circumstances provided for under its law.

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

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

b. prevent parties to an electronic transaction from having the opportunity to establish before judicial or administrative authorities that their transaction complies with any legal requirements with respect to authentication.

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

4. The Parties should work towards the mutual recognition of electronic signatures.

[14] DEPA, Module 2, Articles 2(6) and 3(2); Australia-Singapore DEA, 8(4). See also: AfCFTA Digital Trade Protocol, Article 17; UK-Singapore FTA, as modified by Annex A on Digital Trade and the Digital Economy, Chapter 8, Article 60(3); WTO ECA, Article 4(3).

(8) This provision sets out the legal foundations for the recognition and interoperability of electronic signatures and authentication methods in the context of electronic transactions. It aims to ensure that electronic signatures are not excluded from legal recognition solely due to their digital form, while preserving regulatory flexibility for specific sectors or high-risk transactions. It promotes user autonomy in determining appropriate authentication methods and calls for eventual mutual recognition of electronic signatures among the Parties. The provision is consistent with provisions found in most digital trade agreements such as the CPTPP, USMCA, DEPA, and the Singapore–UK DEA. [15]

(9) Paragraph 1 establishes a baseline obligation for non-discrimination against electronic or digital signatures. It prevents Parties from denying the legal validity of a signature solely on the grounds that it is in electronic form, except where domestic law provides otherwise. This formulation ensures a degree of legal certainty for electronic commerce while preserving national discretion in limited cases, such as wills, real estate, or court documents, which may still require handwritten signatures under domestic law. This language is consistent with UNCITRAL's principle of "functional equivalence,"[16] and is found in numerous digital trade instruments, including the CPTPP, the USMCA, and the EU-Japan EPA. [17]

(10) Paragraph 2 aims to safeguard party autonomy in the choice of authentication technologies. Subparagraph (a) prohibits Parties from mandating specific authentication methods, allowing businesses or individuals to determine what is appropriate for their transactions. Subparagraph (b) ensures that parties to an electronic transaction have the opportunity to demonstrate compliance with authentication requirements before competent authorities, regardless of the method used. This promotes technology neutrality, innovation, and legal due process, and reduces the risk of state-imposed monopoly standards. The language mirrors equivalent provisions in trade agreements [18] and it is consistent with the UNCITRAL Model Law on Electronic Signatures' preference for open-ended recognition criteria rather than closed lists of approved technologies.[19]

---

[15] EU-Japan EPA, Chapter 8, Article 77; EU-New Zealand FTA, Chapter 12, Article 9; EU-UK TCA, Article 206; EU-Mexico Global Agreement, Chapter 16, Article 6; AfCFTA Digital Trade Protocol, Article 8; Australia-Singapore DEA, Article 9; CPTPP, Chapter 14, Article 6; USMCA, Chapter 19, Article 6; RCEP, Chapter 12, Article 6; WTO ECA, Article 5.

[16] UNCITRAL, Model Law on Electronic Commerce with Guide to Enactment, New York, (1998), pp. 20-21.

[17] EU-Japan EPA, Chapter 8, Article 77(1); EU-New Zealand FTA, Chapter 12, Article 9(1); EU-UK TCA, Article 206(1); EU-Mexico Global Agreement, Chapter 16, Article 6(1); AfCFTA Digital Trade Protocol, Article 8; Australia-Singapore DEA, Article 9(1); CPTPP, Chapter 14, Article 6(1); USMCA, Chapter 19, Article 6(1); RCEP, Chapter 12, Article 6(1); WTO ECA, Article 5(2).

[18] EU-Chile Framework Agreement, Chapter 26, Article 10(2); EU-Japan EPA, Chapter 8, Article 77(2); EU-New Zealand FTA, Chapter 12, Article 9(2); EU-UK TCA, Article 206(2); EU-Mexico Global Agreement, Chapter 16, Article 6(2); AfCFTA Digital Trade Protocol, Article 9(a) and (b); Australia-Singapore DEA, Article 9(2); CPTPP, Chapter 14, Article 6(2); USMCA, Chapter 19, Article 6(2); RCEP, Chapter 12, Article 6(2)(a) and (c); WTO ECA, Article 5(3).

[19] UNCITRAL, Model Law on Electronic Signatures with Guide to Enactment, New York, (2001), p. 38.

(11) Paragraph 3 introduces a narrowly drawn exception to the principles in paragraph 2. It allows Parties to require specific performance standards or accredited certifications for certain categories of transactions, such as those involving financial services, public procurement, or cross-border exchanges of official documents. This acknowledges the legitimate interest of governments in maintaining trust and security in sensitive or high-risk sectors, while limiting such requirements to defined use cases. This balance between flexibility and security reflects the approach taken in several other digital trade instruments.[20]

(12) Paragraph 4 is forward-looking and encourages regulatory convergence. By recommending that the Parties work towards mutual recognition of electronic signatures, it aims to reduce barriers to cross-border digital transactions and improve interoperability of trust services. Agreements like the EU-Mexico Global Agreement, the Singapore–UK DEA and the DEPA contain similar language, often referencing the potential role of mutual recognition frameworks or conformity assessment mechanisms to bridge domestic regulatory differences. [21]

(13) In sum, this provision sets a balanced and future-oriented framework for the legal recognition of electronic signatures and authentication. It combines firm commitments to non-discrimination and technology neutrality with limited regulatory carve-outs and aspirational goals for international cooperation. The approach supports legal certainty and innovation in electronic transactions while respecting legitimate policy space for high-risk sectors. Its structure reflects a convergence around key international legal norms, and its emphasis on interoperability positions it as a core element of any modern digital trade agreement.

[20] EU-Chile Framework Agreement, Chapter 26, Article 10(3); EU-Japan EPA, Chapter 8, Article 77(3); EU-New Zealand FTA, Chapter 12, Article 9(3); EU-K TCA, Article 206(3); EU-Mexico Global Agreement, Chapter 16, Article 6(3) first sentence; Australia-Singapore DEA, Article 9(3); CPTPP, Chapter 14, Article 6(3); USMCA, Chapter 19, Article 6(3); RCEP, Chapter 12, Article 6(3); WTO ECA, Article 5(4).

[21] EU-Mexico Global Agreement, Chapter 16, Article 6(4); UK-Singapore FTA, as modified by Annex A on Digital Trade and the Digital Economy, Chapter 8, Article 61(4); Australia-Singapore DEA, Article 9(4); CPTPP, Chapter 14, Article 6(4); USMCA, Chapter 19, Article 6(4); RCEP, Chapter 12, Article 6(4); WTO ECA, Article 5(6).

ELECTRONIC PAYMENTS

Context and Scope

(1) The regulation of electronic payments falls within a broader policy area at the intersection of financial regulation, digital infrastructure governance, and trade facilitation. This area encompasses the legal and institutional frameworks that oversee the provision of payment services, the operation of payment systems, and the development of secure, interoperable infrastructures that enable the transfer of funds across digital channels. It includes regulatory regimes for the licensing and supervision of both traditional financial institutions and non-bank entities, such as FinTech firms, that offer payment-related services. These regimes typically address authorization requirements, prudential and operational standards, risk management, and consumer protection obligations, reflecting the critical role that electronic payments play in modern financial ecosystems.

(2) In addition to institutional oversight, this policy area includes the establishment of technical and operational standards that support interoperability and security across domestic and cross-border payment networks. This involves the adoption of internationally recognized messaging protocols, data formats, and cybersecurity frameworks that enable efficient and reliable communication between systems and providers. The regulatory scope also extends to competition and innovation policy—promoting open access to payment infrastructures, enabling the use of APIs for third-party service integration, and facilitating regulatory approaches such as sandboxes to support the development and testing of new payment technologies. Together, these policies ensure that electronic payment systems are not only efficient and secure but also inclusive, adaptable, and aligned with international best practices.

Article 7 – Electronic Payments

1. To facilitate the rapid growth of electronic payments, in particular those provided by non-bank, non-financial institution and FinTech enterprises, the Parties recognise the importance of developing an efficient, safe and secure environment for cross-border electronic payments, including by:

a. fostering the adoption and use of internationally accepted standards for electronic payments;

b. promoting interoperability and the interlinking of electronic payment infrastructures; and

c. encouraging innovation and competition in electronic payments services.

2. The Parties further recognise the importance of upholding safety, efficiency, trust and security in electronic payment systems through regulations, and that the adoption and enforcement of regulations and policies should be proportionate to the risks undertaken by the payment service providers.

3. Each Party should:

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

b. endeavour to finalise decisions on regulatory or licensing approvals in a timely manner;

c. not arbitrarily or unjustifiably discriminate between financial institutions and non-financial institutions in relation to access to services and infrastructure necessary for the operation of electronic payment systems;

d. adopt, for relevant electronic payment systems, international standards for electronic payment messaging, for electronic data exchange between financial institutions and services suppliers to enable greater interoperability between electronic payment systems;

e. facilitate the use of open platforms and architectures such as tools and protocols provided for through Application Programming Interfaces ("APIs") and encourage payment service providers to safely and securely make APIs for their products and services available to third parties, where possible, to facilitate greater interoperability, innovation and competition in electronic payments; and

f. facilitate innovation and competition and the introduction of new financial and electronic payment products and services in a timely manner, such as through adopting regulatory and industry sandboxes.

Commentary

(3) This provision sets out a comprehensive framework aimed at fostering the rapid development of cross-border electronic payments, with a special focus on enabling participation by non-bank, non-financial institutions, and FinTech enterprises. It reflects a modern approach to digital trade, emphasizing regulatory cooperation and innovation facilitation rather than just market liberalization. For a Party undertaking this obligation, the provision a non-binding obligation to consider adopting or maintaining domestic regulations governing electronic payment systems and financial services in a way that supports innovation, maintains financial integrity, and promotes interoperability. It goes beyond the approach adopted in earlier agreements[22] by introducing more targeted, granular requirements, similar to those in the Australia-Singapore DEA, without introducing binding obligations on Parties.[23]

[22] See for example: ASEAN Agreement on Electronic Commerce, Article 9.

[23] Australia-Singapore DEA, Article 11.

(4) The first clause encourages the creation of a regulatory environment conducive to the growth of cross-border electronic payments. It places an emphasis on integrating FinTech and non-bank players into the formal ecosystem. For a Party, this would likely require revisions to its regulatory perimeter to formally recognize non-bank PSPs (Payment Service Providers) and extend relevant oversight, licensing, and supervisory rules to them. Sub-clause (a) on adopting internationally accepted standards implies a non-binding obligation to update and harmonize domestic technical standards to global benchmarks. Sub-clause (b), calling for interoperability and interlinking of payment infrastructure, would require national regulators to pursue cross-border cooperation agreements and develop shared or interoperable digital rails with other countries. Sub-clause (c) stresses the need to foster innovation and competition, prompting a reevaluation of licensing barriers, capital requirements, and anti-competitive practices that may disproportionately disadvantage emerging firms. The language of Paragraph 1 reflects the wording used in the DEPA.[24]

(5) The second clause introduces a principle of proportionality in regulation, encouraging a risk-based approach tailored to the size, nature, and business model of the payment service provider. For domestic regulatory authorities, this requires the development of tiered frameworks that differentiate between large incumbents and smaller, technology-driven firms. Regulators may need to conduct public consultations and introduce supervisory guidelines that outline how proportionality will be applied across different categories of service providers. The language of Paragraph 2 aligns with approach followed by the Australia-Singapore DEA.[25]

(6) The third clause sets out several implementation-focused obligations that significantly affect how domestic frameworks should function. Sub-clause (a) fosters transparency in the formulation and publication of electronic payment regulations, including licensing and technical standards. It obliges regulators to publish all relevant rules in an accessible and timely manner, which may require digitizing and consolidating regulatory information. Sub-clause (b), on timely decision-making, promotes clear procedural timeframes and performance benchmarks within licensing and approval processes.

(7) Sub-clause (c) introduces a non-discrimination commitment, encouraging Parties to refrain from arbitrary or unjustified restrictions that favor financial institutions over non-financial or FinTech entities in accessing essential payment infrastructure. For many jurisdictions, this would require a review and potential revision of existing rules governing access to clearing systems, real-time gross settlement systems, and central

[24] DEPA, Module 2, Article 7(1).
[25] Australia-Singapore DEA, Article 11(3).

bank-managed platforms to ensure equal access rights. Sub-clause (d), calling for the adoption of international standards for messaging and data exchange, reinforces the push toward interoperability and may require regulators to work closely with industry to implement uniform technical protocols.

(8) Sub-clause (e) is especially forward-looking, advocating for the use of open platforms and APIs (Application Programming Interfaces). It suggests that PSPs should be encouraged to offer secure access to their systems via APIs, allowing third parties to develop new services and products. For countries without a legal or policy framework on open banking, this would necessitate the development of standards governing data access, cybersecurity, liability, and consent. Sub-clause (f) reinforces the importance of innovation by recommending the establishment of mechanisms such as regulatory sandboxes, which allow emerging payment technologies to be tested in controlled environments. This would require legislative authority or regulatory discretion, alongside inter-agency collaboration to administer such initiatives effectively.

(9) The DEPA and the Australia-Singapore DEA include similar language with respect to measure relating to electronic payments. However, the implementation-focused obligations in the Australia-Singapore DEA are binding, while the DEPA opted for a non-binding approach.

(10) Overall, the provision provides for a change in the nature of trade obligations, moving from passive commitments to active regulatory reforms. For a Party, fulfilling these obligations would mean aligning domestic payment regulations with international best practices, reducing discriminatory barriers, embracing open technology architectures, and supporting a more dynamic, competitive ecosystem. Compared to earlier instruments which lack a provision to foster the creation of a domestic framework for electronic payments, Article 7 promotes regulatory convergence, particularly in areas like API frameworks, open standards, and innovation facilitation. It reflects the growing centrality of digital payments to global trade and economic development and would require a coordinated, cross-sectoral regulatory response from financial, trade, competition, and technology authorities alike.

[26] DEPA; Module 2, Article 2(2); Australia-Singapore DEA, Article 11(2).

TRADE FACILITATION WITH DIGITAL MEANS

Context and Scope

(1) Domestic policy measures relating to paperless trading sit at the intersection of trade facilitation, digital governance, and customs modernization. As international commerce increasingly relies on digital technologies, governments have been adapting their legal and regulatory frameworks to reduce or eliminate paper-based documentation in import, export, and transit procedures. These policies aim to streamline border processes, reduce administrative costs, and enhance the speed and predictability of trade operations. The context is shaped by broader commitments under international agreements such as the WTO Trade Facilitation Agreement (TFA), which encourages the use of electronic submissions and acceptance of digital copies, and by national digital transformation strategies that seek to enhance the competitiveness of domestic businesses, especially SMEs.

(2) The scope of domestic measures in this area typically includes the digitization of trade-related documents (e.g., customs declarations, licenses, certificates of origin), the establishment of electronic submission platforms (such as single windows), and the legal recognition of electronic documents as equivalent to their paper counterparts. These policies often require coordination across multiple agencies, such as customs authorities, trade ministries, port operators, and depend on the existence of robust legal frameworks governing electronic transactions and data protection. While the objective is to create a seamless and interoperable digital trade environment, the implementation of paperless trade policies must also account for legal constraints, infrastructure readiness, and the need to maintain the integrity and security of trade processes.

Article 8 – Paperless Trade

1. The Parties recognise the importance of eliminating paper forms and documents required for the import, export or transit of goods, to create a paperless border environment for trade.

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

3. Each Party shall accept trade administration documents submitted electronically as the legal equivalent of the paper version of those documents, except where:

- **a. that Party is subject to a domestic or international legal requirement to the contrary; or**
- **b. doing so would reduce the effectiveness of the trade administration process.**

Commentary

(3) This provision contributes to the broader objective of trade facilitation by promoting the digitization of trade administration procedures. It reflects a growing international consensus that reducing reliance on paper-based processes enhances the efficiency, speed, and transparency of cross-border trade. Rules on paperless trading represent a policy area increasingly addressed in international trade instruments through biding and non-binding commitments.[27] Article 8 furthers the commitments under instruments such as the WTO Trade Facilitation Agreement (TFA)[28] and echoes equivalent provisions in digital economy agreements such as the DEPA and the Australia-Singapore DEA.[29] The provision pursues the objective of digitalization of trade administration documents by establishing a binding obligation on Parties to recognize the legal equivalence of electronically submitted trade administration documents. Other trade agreements like the CPTPP opt for a non-binding approach to paperless trading provisions.[30]

(4) Paragraph 1 sets the normative foundation by recognizing the importance of eliminating paper forms and documents in border procedures. This recognition signals an intent to move toward a paperless trading environment. The emphasis here is not only on digitization but also on streamlining administrative burdens for importers, exporters, and transit operators.

(5) Paragraph 2 introduces a binding obligation for Parties to make trade administration documents (e.g. customs declarations, certificates of origin, and shipping manifests) publicly available in electronic form. This obligation enhances transparency and supports better access to regulatory requirements, particularly for SMEs that often face challenges navigating complex documentation processes. Moreover, the development of digital custom systems could also favor the creation of interoperable frameworks.

(6) Paragraph 3 further strengthens the digitization of trade administration procedures by requiring Parties to accept electronically submitted trade documents as legally equivalent to their paper counterparts. However, the provision includes two important exceptions. Subparagraph (a) acknowledges that domestic or international legal requirements may, in some cases, prevent full recognition of electronic documents. Subparagraph (b) introduces a functional safeguard, allowing Parties to decline electronic submissions when they would reduce the effectiveness of trade administration, for example due to technological limitations or verification concerns. In these two instances, the obligation to

[27] EU-New Zealand FTA, Chapter 12, Article 15(1); DEPA, Module 2, Article 2; Australia-Singapore DEA, Article 12; CPTPP, Chapter 14, Article 9; WTO ECA, Article 8(2) first sentence.
[28] WTO TFA, Articles 10(2) and 10(4).
[29] DEPA, Module 2, Article 2(1) and 2(3); Australia-Singapore DEA, Article 12(1) and 12(2).
[30] CPTPP, Chapter 14, Article 9. See also: USMCA, Chapter 19, Article 9; RCEP, Chapter 12, Article 5.

recognize electronically submitted trade documents as legally equivalent to their paper counterparts does not apply. These exemptions are similar in spirit to the carve-outs found in the DEPA, the Australia-Singapore DEA, and the WTO ECA.[31] Other digital trade instruments, such as the AfCFTA Digital Trade Protocol, establish a mandatory obligation to accept electronic versions of trade administration documents but do not provide for any exceptions.[32]

(7) Overall, this provision facilitates a digital-first approach to border management while allowing for regulatory flexibility where necessary. It balances legal recognition of digital documentation with the preservation of process integrity and compliance with broader legal regimes. As such, it contributes to advancing seamless, secure, and efficient administration of trade.

[31] DEPA, Module 2, Article 2(3); Australia-Singapore DEA, Article 12(2); WTO ECA, Article 8(7) and 8(9).
[32] AfCFTA Digital Trade Protocol, Article 10.

DATA PROTECTION

Context and Scope

(1) Data protection refers to a Party's internal legal and institutional framework that governs how personal information is collected, stored, used, transferred, and deleted. It includes rules, principles, and enforcement mechanisms that aim to safeguard individuals' personal information from misuse or unauthorized access.

(2) Strong domestic data protection frameworks support international trade by enabling trusted cross-border data flows, reducing legal uncertainty, and enhancing consumer and business confidence. They allow countries to meet international standards, facilitating participation in modern trade agreements and boosting competitiveness in digital services. In contrast, the absence of such frameworks can create barriers to market access, discourage foreign investment, and expose countries to data transfer restrictions.

Article 9 – Data Protection

1. The Parties recognize the economic and social benefits of safeguarding personal information of users of electronic commerce, acknowledging that such protection is fundamental to enhance consumer confidence and trust in electronic commerce.

2. To this end, each Party shall adopt or maintain a legal framework that safeguards the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party may consider principles and guidelines of relevant international bodies.

3. Each Party shall publish information on the personal information protections it provides to users of electronic commerce, including how:

a. the mechanisms available to individuals for seeking redress in cases of non-compliance; and

b. the obligations imposed on enterprises to ensure compliance with applicable legal requirements.

4. Each Party should:

a. establish national data protection authorities or other relevant bodies responsible for the enforcement of personal data protection laws:

b. build capacities of their national data protection authorities or other relevant bodies responsible for the enforcement of personal data protection laws

c. maintain dialogue on personal data protection and sharing of knowledge, research and best practices with other State Parties.

5. Each Party shall promote the publication, by businesses in its territory, of their policies and procedures related to the protection of personal information.

Commentary

(3) This provision addresses the protection of personal information in the context of electronic commerce, recognizing it as a fundamental component of consumer trust and digital trade governance. The article reflects the growing international consensus that robust data protection frameworks support both economic growth and individual rights in the digital economy. Structured with a mix of binding and non-binding language, the provision offers flexibility for Parties to maintain regulatory autonomy while aligning with shared principles. It draws on global trends in digital trade agreements, such as the CPTPP, the DEPA, the EU-New Zealand Free Trade Agreement (FTA), the EU-UK Trade and Cooperation Agreement (TCA), the African Continental Free Trade Area (AfCFTA) Digital Trade Protocol, all of which link strong privacy protections to the facilitation of digital trade.[33]

(4) Paragraph 1 establishes the policy premise of the article in that it affirms that protecting personal information yields economic and social benefits and fosters trust in digital markets. The use of the term "recognize" signals a shared understanding among Parties without creating a binding obligation. This introductory provision sets the normative tone, positioning privacy protection as essential to sustainable digital trade. The language recalls similar introductory clauses found in the EU-New Zealand FTA, the DEPA, the CPTPP and the Australia-Singapore DEA, which likewise frame privacy as a prerequisite for consumer confidence.[34]

(5) Paragraph 2 introduces a binding obligation requiring that each Party "shall adopt or maintain a legal framework" that safeguards personal information. This is a departure from "should"-based models and brings the MDEA closer to the structure of agreements like the USMCA or the CPPP, which also mandate Parties to adopt a legal privacy framework.[35] However, the provision preserves implementation flexibility by allowing different regulatory models (comprehensive, sectoral, or hybrid) and referencing "principles and guidelines of relevant international bodies" rather than mandating adherence to any one standard.

---

[33] EU-New Zealand FTA, Chapter 12, Article 5; EU-UK TCA, Article 202; AfCFTA Digital Trade Protocol, Article 21; DEPA, Module 4, Article 2; CPTPP, Chapter 14, Article 8. See also: Australia-Singapore DEA, Article 17; USMCA, Chapter 19, Article 8; RCEP, Chapter 12, Article 8.

[34] EU-New Zealand FTA, Chapter 12, Article 5(1), EU-UK TCA, Article 202(1); DEPA, Module 4, Article 2(1); CPTPP, Chapter 14, Article 8(1); Australia-Singapore DEA, Article 17(1). See also: EU-Japan Economic Partnership Agreement, Chapter 8, Article 78(3); USMCA, Chapter 19, Article 8(1); WTO Electronic Commerce Agreement, Article 16(2).

[35] USMCA, Chapter 19, Article 8(2); CPTPP, Chapter 14, Article 8(2). See also: AfCFTA Digital Trade Protocol, Article 21(2); DEPA, Module 4, Article 2(2); Australia-Singapore DEA, Article 17(2); RCEP, Chapter 12, Article 8(1); EU-Canada Comprehensive Economic and Trade Agreement, Chapter 16, Article 4 (non-binding formulation: "should adopt or maintain");

(6) Paragraph 3 introduces a transparency obligation, requiring each Party to publish information on its data protection regime. This includes, under subparagraph (a), the mechanisms individuals can use to seek redress, and under subparagraph (b), the obligations placed on businesses. While framed with binding "shall" language, the paragraph focuses on disclosure rather than substantive regulatory outcomes. This approach is consistent with digital trade instruments such as the EU-New Zealand FTA, the DEPA, and the CPTPP's emphasis on transparency in data governance.[36] This transparency obligation is particularly valuable for cross-border stakeholders, users, consumers, and businesses, who must navigate varying regulatory environments.

(7) Paragraph 4 outlines recommended actions for institutional development and international cooperation. Subparagraphs (a) and (b) encourage the establishment and strengthening of national data protection authorities, which are crucial for enforcement and oversight. Subparagraph (c) promotes dialogue, knowledge-sharing, and research collaboration among Parties. The use of "should" here allows Parties to develop these capacities in accordance with their resources and legal traditions.

(8) Paragraph 5 encourages Parties to promote the publication by businesses of their personal data protection policies and procedures. This reflects a recognition that transparency in the private sector complements public regulation. While this obligation is non-binding, it supports voluntary compliance mechanisms, such as privacy notices, certification schemes, and corporate codes of conduct. Comparable language can be found in other digital trade agreements, which encourage the use of business-led mechanisms to enhance consumer trust without imposing burdensome requirements, especially on small and medium-sized enterprises (SMEs).[37]

(9) Taken together, the structure of the article provides a balanced regulatory approach: Paragraphs 2 and 3 contain binding obligations relating to the existence and transparency of legal frameworks, while Paragraphs 4 and 5 use non-binding "should" language to encourage institutional development and private sector transparency. This hybrid approach mirrors the flexibility built into other digital economy agreements, enabling broad participation regardless of Parties' levels of regulatory maturity.

(10) In conclusion, this article offers a pragmatic framework that strengthens personal data protection in the digital economy while preserving national regulatory flexibility. By blending binding commitments with cooperative mechanisms, the provision fosters trust among consumers, legal certainty for businesses, and policy space for regulators. It reflects a broader international trend toward the convergence of privacy principles without harmonization, providing a foundation for dialogue and interoperability in a rapidly evolving digital trade landscape.

---

[36] EU-New Zealand FTA, Chapter 12, Article 5(4); DEPA, Module 4, Article 2(5); CPTPP, Chapter 14, Article 8(4). See also: AfCFTA Digital Trade Protocol, Article 21(3); Australia-Singapore DEA, Article 17(5); USMCA, Chapter 19, Article 8(5); RCEP, Chapter 12, Article 8(4); WTO Electronic Commerce Agreement, Article 16(6).

[37] AfCFTA Digital Trade Protocol, Article 21(4); Australia-Singapore DEA, Article 17(6); RCEP, Chapter 12, Article 8(4).

CROSS-BORDER DATA TRANSFERS

Context and Scope

(1) The transfer of information across borders, whether personal or not personal information, is a key enabler of digital trade. Cross-border data transfers facilitate access to markets, streamline the conduct of international business and help organizing value chains. While it concurrently raises significant challenges to data protection, to intellectual property rights, and to security, cross-border data flow increases productivity and fosters innovation.

Article 10 – Cross-Border Data Transfers

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

2. Each Party shall, subject to an Annex on Cross-border Data Transfers, allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of business of a covered person.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

a. is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

b. does not impose restrictions on transfers of information greater than are required to achieve the objective.

4. Parties shall craft an Annex on Cross-border Data Transfers, which shall, among others, set out legitimate public policy objectives, lay out how data may be used, modalities of trusted data transfers, restrictions on sharing of data to third parties, including, among others, data protection regulations that may be applied by regulators.

Commentary

(2) The purpose of Article 10 is to reconcile the fundamental importance of free cross-border data flows with the sovereign right of Parties to regulate such flows to achieve legitimate public policy objectives. It promotes the cross-border transfer of information by electronic means, including personal information, when such transfer is for the conduct of business by a covered person. At the same time, the Article recognizes that Parties may need to adopt or maintain measures that limit data transfers to protect legitimate public interests. This exception is carefully circumscribed by cumulative conditions designed to prevent misuse or disguised protectionism. From an overarching perspective, the provision proposes a commitment that balances the desire to permit free cross-border transfers of information by electronic means among Parties, without unduly restraining the Parties' regulatory autonomy to pursue a legitimate public policy objective.

(3) Paragraph 1 serves as a policy acknowledgment that Parties have diverse regulatory approaches to the transfer of information by electronic means. The verb "recognise" signals respect for the differing domestic legal frameworks without imposing substantive obligations. This approach aligns closely with language found in the CPTPP[38] and the DEPA,[39] the Australia-Singapore DEA,[40] and the Regional Comprehensive Economic Partnership (RCEP),[41] all of which similarly acknowledge regulatory diversity while fostering cooperation. The AfCFTA Digital Trade Protocol also similarly recognizes the diversity of the parties' regulatory frameworks by establishing a general right to regulate to safeguard public welfare, promote sustainable development, protect essential security interests and pursue legitimate public policy objectives. However, this provision of the AfCTA Digital Trade Protocol informs the interpretation of the whole protocol.[42]

(4) Paragraph 2 establishes a binding obligation by requiring that "each Party shall allow" the cross-border transfer of information, including personal data, when conducted for business purposes by a covered person. The use of the verb "shall" signals a mandatory commitment, differentiating this provision from softer "should" or "encourage" language found in other trade texts. This aligns the provision with contemporary digital trade agreements that prioritize open data flows as a core trade facilitator.[43]

[38] CPTPP, Chapter 14, Article 11(1).
[39] DEPA, Module 4, Article 3(1).
[40] Australia – Singapore DEA, Article 23(1).
[41] RCEP, Chapter 12, Article 15(1).
[42] AfCFTA Digital Trade Protocol, Article 4.
[43] CPTPP, Chapter 14, Article 11(2); DEPA, Module 4, Article 3(2); AfCFTA Digital Trade Protocol, Article 20(1); USMCA, Chapter 19, Article 11(1), Australia -Singapore DEA, Article 23(2).

(5) The scope of paragraph 2, subject to the Annex on Cross border Data Transfers, encompasses information transferred electronically in a cross-border context, explicitly including personal information, thus intersecting with domestic data protection frameworks. The limitation of transfers "for the conduct of business" confines the obligation to commercial activities and excludes non-commercial or governmental data flows. The inclusion of personal information in the general prohibition on cross-border data flow restrictions replicates the wording of several international trade agreements, reflecting thus a growing consensus among States on the scope of application of cross-border data transfers provisions in modern digital trade agreements.[44]

(6) The obligation of allowing cross-border data flow is subject to the Annex on Cross-border Data Transfers. A careful calibration has to be struck between safeguarding the free flow of data for the benefit of businesses, and on the other hand, preserving the sovereign right of each party to regulate such flows in pursuit of legitimate policy objectives. To make this process more predictable, the Annex on Cross-border Data Transfers is suggested that will allow Parties to agree on the restrictions or regulatory requirements that may be imposed on the cross-border data transfer. The Annex will allow Parties to pre-define clearly any safeguards that may be applied for sensitive sectors, in a transparent and reviewable manner. This is further referenced in paragraph 4 where reference is made to the fact that parties of the agreement shall draft the Annex on Cross-border Data Transfers. Such an approach has been taken in AfCFTA Digital Trade Protocol.

(7) The DCO Interoperability Mechanism for Cross-Border Data Flows is a multilateral framework designed to enable trusted, secure, and predictable movement of data between DCO Member States by harmonizing core safeguards while respecting national legal differences. The Mechanism consists of three integrated components: the DCO Privacy Principles, adopted by the DCO Member States, which establish baseline privacy and data protection standards across Member States; the DCO Model Contractual Clauses (DCO MCCs), a standardized legal instrument that facilitates compliant and accountable cross-border data transfers between public and private entities (especially in the absence of adequacy); and the Member State Accreditation Process, which assesses the adequacy of national privacy, data protection, and regulatory enforcement frameworks to ensure alignment with DCO standards and global best practices. Together, these components provide a coherent and practical foundation for trusted digital trade and cross-border Data flows across the DCO membership. Through the Mechanism, parties can craft the referenced Annex on Cross-border Data Transfers, clearly articulating narrowly tailored safeguards to allow trusted data flows amongst parties to the agreement.

[44] CPTPP, Chapter 14, Article 11(2); DEPA, Module 4, Article 3(2); AfCFTA Digital Trade Protocol, Article 20(1); USMCA, Chapter 19, Article 11(1); Australia – Singapore DEA, Article 23(2). Notably, RCEP Article 12.15(2) does not explicitly include personal information in the scope of application of the provision.

(8) Paragraph 3 provides an important exception, allowing Parties to maintain or adopt measures inconsistent with paragraph 2 where necessary to achieve a legitimate public policy objective. However, this exception is not without limits. To qualify, such measures must cumulatively:

- Serve a legitimate public policy objective, such as cybersecurity, privacy protection, or financial stability;
- Be applied in a manner that is neither arbitrary nor unjustifiably discriminatory, nor a disguised restriction on trade (paragraph 3(a));
- Not impose restrictions greater than necessary to achieve the objective (paragraph 3(b)).

(9) The reference to "a legitimate public policy objective" is deliberately open-ended rather than exhaustive. This flexible drafting enables Parties to address a range of societal and regulatory priorities, including emerging challenges, without being confined to a predetermined list. This reflects the approach taken in major agreements such as the CPTPP, USMCA, DEPA and the Australia-Singapore DEA.[45] Nonetheless, the exceptions are tempered by the requirements of non-discrimination and proportionality, which act as safeguards against protectionist abuse disguised as public policy measures.[46]

(10) The tests set forth in subparagraphs 3(a) and 3(b) echo well-established principles embodied in the general exception clauses of the General Agreement on Tariffs and Trade (GATT) and the General Agreement on Trade in Services (GATS), emphasizing necessity, proportionality, and good faith.[47] This formulation seeks to create a balanced framework that protects legitimate regulatory space while preventing the misuse of public policy justifications for trade restrictions. This language aligns with parallel provisions in the AfCFTA Digital Trade Protocol, the Australia-Singapore DEA, and others, reflecting a growing consensus in international digital trade governance.[48]

(11) Parties retain the sovereign right to define and regulate what constitutes unethical, obscene, or harmful content in accordance with their domestic laws, cultural norms, and policy objectives. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures to restrict or regulate such content, consistent with the legitimate public-policy exceptions provided elsewhere in this Agreement.

---

[45] CPTPP, Chapter 14, Article 11(3); USMCA, Chapter 19, Article 11(2); DEPA, Module 4, Article 3(3); AfCFTA Digital Trade Protocol Article 20(2); Australia – Singapore DEA, Article 23(3); RCEP, Chapter 12, Article 15(3).

[46] Please note that AfCFTA Digital Trade Protocol Article 20(2) and RCEP Article 12.15(3)(b) also include essential security interests as an additional ground for invoking the exception.

[47] GATT, Chapeau to Article XX; GATS, Chapeau to Article XIV.

[48] CPTPP, Chapter 14, Article 11(3)(a) and (b); USMCA, Chapter 19, Article 11(2)(a) and (b); DEPA, Module 4, Article 3(3)(a) and b); AfCFTA Digital Trade Protocol Article 20(2); Australia – Singapore DEA, Article 23(3)(a) and (b); RCEP, Chapter 12, Article 15(3)(a).

(12) Overall, Article 10 embodies a binding and balanced approach to cross-border data transfers. It commits Parties to enable data flows essential for digital commerce, while respecting each Party's sovereign right to regulate according to domestic priorities and public policy needs. By combining a clear general obligation with a calibrated exception, the Article strikes a pragmatic balance between digital openness and regulatory autonomy. This model is consistent with contemporary trade agreements that seek to foster digital trade without undermining national regulatory frameworks.

(13) The language reflects an attempt to prevent protectionist misuse of public policy justifications while preserving legitimate regulatory space. The structure of Article 10 thus reflects a binding model entailing a general prohibition on data transfers restrictions that seeks to promote digital openness without unduly interfering with the Parties sovereign right to regulate. The text also emphasizes that commitments should not disregard the distinct regulatory framework adopted by each Party. The provision creates an obligation that the Parties would not restrict cross-border transfer of information by electronic means among Parties when the transfer is made in connection with business activities. However, paragraph 3 provides nonetheless for a broad exception clause to address legitimate public policy objectives. Paragraph 2 and 3 strike a balance between promoting digital openness and protecting the right of states to regulate in the public interest. Paragraph 4 allows parties to clearly enumerate the restrictions that may be imposed in pursuit of achieving their legitimate public policy objectives. Article 10 draws upon models, such as the CPTPP, the DEPA, the USMCA, the AfCTA Digital Trade Protocol, and the Australia – Singapore DEA, following the general prohibitions on data transfer restrictions approach applicable across every sector. [49]

[49] CPTPP, Chapter 14, Article 11; USMCA, Chapter 19, Article 11; DEPA, Module 4, Article 3; AfCFTA Digital Trade Protocol Articles 4 and 20; Australia – Singapore DEA, Article 23; RCEP, Chapter 12, Article 15.

LOCATION OF COMPUTER FACILITIES

Context and Scope

(1) Data localisation requirements refer to domestic laws or regulations that mandate the storage or processing of data within a country's territorial borders. These requirements may oblige businesses to use local servers, establish local data centers, or refrain from transferring certain types of data abroad. Data localization requirements may apply to all types of data or be specific to certain sectors.

(2) Data localization can create a significant barrier to digital trade because of burdensome procedural requirements and costs. Specifically, data localization requirements impact digital trade with regard to market access and compliance cost due to regulatory diversity.

Article 11 – Location of computer Facilities

1. The Parties acknowledge that each Party may establish its own regulatory requirements for the use of computing facilities, including measures to safeguard the security and confidentiality of communications.

2. No Party shall mandate that a covered person use or locate computing facilities within its territory as a prerequisite for conducting business in that territory.

3. Nothing in paragraph 2 shall prevent a Party from adopting or maintaining measures to achieve a legitimate public policy objective, including: (a) protection of personal data and privacy; (b) financial stability and prudential supervision (including effective regulatory and supervisory access); (c) protection of essential security interests; (d) integrity and resilience of critical information infrastructure; (e) protection of public health; or (f) compliance with lawful access obligations in criminal matters; provided that such measures are not applied in a manner constituting arbitrary or unjustifiable discrimination or a disguised restriction on trade, and are not more restrictive than necessary to achieve the objective.

4. A Party shall not require a covered financial service supplier to use or locate computing facilities in its territory as a condition for conducting business, provided that the Party's competent authorities have immediate, direct, complete and ongoing access, on a timely basis and in a usable form, to information processed or stored outside its territory that they are entitled to obtain for regulatory or supervisory purposes, subject to appropriate confidentiality and data-protection safeguards.

5. Each Party shall list in Annex Computing Facilities Safeguards any sector-specific or measure-specific localization requirement it maintains, indicating the objective pursued and the applicable conditions and safeguards; a Party may modify its listing upon notification to the other Parties.

Commentary

(3) This provision seeks to introduce a prohibition on domestic localization of computing facilities, following the "prohibition with exceptions" model. Its scope is limited to situations where regulatory measures condition market access on the use or location of computing infrastructure within a Party's territory. The text, first, underlines regulatory diversity between Parties, acknowledging the Parties' right to regulate; secondly, it establishes a general prohibition on data localization requirements; thirdly, set forth a list of legitimate public policy objectives that may be employed by the parties to impose measures; and fourthly, through the Annex allows parties to enumerate the restrictions. Overall, the provision seeks to reduce unnecessary barriers to digital trade, while preserving sufficient regulatory space for legitimate policy interests.

(4) Paragraph 1 serves a contextual and descriptive function. It acknowledges that each Party may adopt its own regulatory requirements governing the use of computing facilities, particularly in areas that are instrumental to preserving security and confidentiality of communications. This recognition highlight the regulatory diversity among Parties and affirms their sovereign right to pursue national priorities in this domain. As such, this paragraph does not impose binding obligations. The formulation "acknowledge that each Party may establish its own regulatory requirements" reflects the balancing approach adopted in modern digital trade agreements, such as the CPTPP and the DEPA, which similarly recognize regulatory autonomy without creating enforceable commitments at this stage.[50]

(5) Paragraph 2 introduces a binding obligation prohibiting a Party from requiring the use or location of computing facilities within its territory as a condition for conducting business. The use of "shall not mandate" expresses an enforceable prohibition. This provision aims to eliminate data localization mandates that could hinder cross-border digital services or raise operational costs, particularly for small and medium enterprises (SMEs). The obligation supports digital openness and commercial flexibility, allowing covered persons to deploy or acquire local infrastructure based on business needs rather than jurisdictional requirements.

[50] CPTPP, Chapter 14, Article 13(1); DEPA, Module 4, Article 4(1). See also: Australia-Singapore DEA, Article 23(1), RCEP, Chapter 12, Article 14(1); ASEAN Agreement on Electronic Commerce (ASEAN E-Commerce Agreement), Article 7(6)(a); AfCFTA Digital Trade Protocol, Article 4; RCEP, Chapter 12, Article 14(1).

(6) The structure and substance of paragraph 2 replicate the treaty text of the CPTPP the DEPA, the AfCFTA Digital Trade Protocol, the USMCA, and the Australia-Singapore DEA, all of which prohibit mandatory localization of computing infrastructure, subject to specific exceptions.[51]

(7) Paragraph 3 introduces a public policy exception that allows Parties to implement or maintain measures inconsistent with paragraph 2, provided certain conditions are met. The exception is structured to preserve regulatory space while guarding against protectionist misuse. Specifically, measures must:

- Serve a legitimate public policy objective, as enumerated in paragraph 3;
- Not be applied in a manner that constitutes arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
- Not impose more restrictive requirements than necessary to achieve the stated objective.

(8) Paragraph 3 also enumerates list of public policy objectives that may be employed by Parties when requiring data localization. Enumerating objectives mitigates interpretive uncertainty ex ante and provides clearer guidance to regulators and tribunals ex post, yet remains aligned to the structure used in modern instruments that balance openness with a preserved "right to regulate." The open-textured reference to "a legitimate public policy objective" provides necessary flexibility for Parties to address emerging or evolving concerns, while the cumulative conditions act as safeguard mechanisms. The CPTPP, the DEPA, and the AfCFTA Digital Trade Protocol provide for equivalent requirements, affirming its role as a common template in the design of digital trade exception clauses.[52]

(9) The proportionality test laid out in paragraph 3echo well-established principles embodied in the general exception clauses of the GATT and the GATS, emphasizing necessity, proportionality, and good faith.[53] This formulation seeks to create a balanced framework that protects legitimate regulatory space while preventing the misuse of public policy justifications for trade restrictions. This language aligns with parallel provisions in the AfCFTA Digital Trade Protocol, the Australia-Singapore DEA, and other modern international digital trade agreements, reflecting a growing consensus in international digital trade governance.[54]

---

[51] CPTPP, Chapter 14, Article 13(2); DEPA, Module 4, Article 4(2); AfCFTA Digital Trade Protocol, Article 22(1); Australia-Singapore DEA, 24(2); USMCA, Chapter 19, Article 12. Please note that, while the USMCA prohibits domestic localisation of computer facilities, it does not include an exception clause thus representing an absolute prohibition on data localisation requirements.

[52] CPTPP, Chapter 14, Article 13(3); DEPA, Module 4, Article 4(3); Australia-Singapore DEA, Article 24(3); AfCFTA, Digital Trade Protocol, Article 22(2). Please note that AfCTA Digital Trade Protocol, also includes the protection of essential security interests as a valid ground to invoke the exception.

[53] GATT, Chapeau to Article XX; GATS, Chapeau to Article XIV.

[54] CPTPP, Chapter 14, Article 13(3)(a) and (b); DEPA, Module 4, Article 4(3)(a) and (b); AfCFTA Digital Trade Protocol, Article 22(2); Australia-Singapore DEA, Article 24(3)(a) and (b);

(10) Paragraph 4 restricts the requirement of mandating data localization for the businesses providing financial services, subject to the condition that the relevant authorities will have access to the information that is stored outside of its territory including access to how the data is being processed. This access by the relevant authorities is subject to confidentiality and data protection safeguards.

(11) Paragraph 5 then allows parties to enumerate clearly through the use of an Annex the type of restrictions that may be imposed with respect to specific data. It also allows parties with the right to change the measures of restrictions that may be imposed, providing the parties with flexibility to adapt to the developments in the digital economy, subject to notification to the other parties.

(12) In sum, this provision affirms a liberalizing approach to digital infrastructure regulation, prohibiting forced localization while ensuring Parties retain adequate flexibility to safeguard public interest objectives. By combining a clear prohibition with a framed exception, Article 11 aligns with the broader architecture of modern digital trade agreements that seek to promote interoperability, reduce fragmentation, and support cross-border digital business models.

ONLINE CONSUMER PROTECTION AND UNSOLICITED COMMERCIAL ELECTRONIC COMMUNICATIONS

Context and Scope

(1) Online Consumer Protection refers to a regulatory domain focused on safeguarding individuals engaging in digital transactions from deceptive, unfair, or harmful practices. Measures within this scope typically address transparency of commercial terms, accuracy of information, dispute resolution mechanisms, and the legal prohibition of fraudulent or misleading online conduct. Consumer protection frameworks in this area often require businesses to clearly display their terms of service, privacy policies, and complaint procedures, as well as to offer remedies for non-compliant or defective digital goods and services. These rules are especially important in cross-border e-commerce, where consumers may have limited recourse under foreign laws.

(2) A related regulatory area is the control of unsolicited commercial electronic communications, commonly referred to as "spam". These measures include legal obligations for businesses to obtain consumer consent before sending marketing messages, ensure clear identification of the sender, and provide easy options to opt-out of future communications. Domestic regulations may also require service providers to take reasonable steps to prevent the transmission of spam and allow for sanctions or recourse mechanisms against non-compliant senders. Together, these policy instruments aim to foster trust in digital environments by ensuring that online marketing practices are consent-based, respectful of user preferences and transparent.

Article 12 – Online Consumer Protection

1. The Parties recognise the importance of maintaining and adopting transparent and effective measures to protect consumers from fraudulent or deceptive commercial practices in electronic commerce.

2. To this end, each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.

3. The Parties shall exchange information and experiences related to national approaches for the protection of consumers engaging in electronic commerce.

4. The Parties recognise the importance of cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border electronic commerce in order to enhance consumer welfare.

5. Each Party should publish information on the consumer protection it provides to users of electronic commerce.

6. The Parties should encourage businesses to publish their policies and procedures related to online consumer protection

Commentary

(3) This provision establishes a framework within the MDEA for the protection of consumers engaged in electronic commerce, reflecting a shared commitment among the Parties to build trust in digital markets. It blends binding obligations with soft-law cooperation measures: while certain elements use imperative language ("shall adopt," "shall exchange"), others frame policy coordination and transparency goals using non-binding formulations. Collectively, the provision outlines a normative structure for consumer protection in the digital economy that require Parties to establish a protection framework for consumers engaging in online activities allowing the Parties to choose the best regulatory approach to comply with the obligation. Article 12 combines emerging trends in digital trade agreements and innovative approaches to online consumer protection.

(4) Paragraph 1 lays the normative foundation by acknowledging the importance of transparent and effective consumer protection in the online context. The recognition reflects the reality that consumers are especially vulnerable to deceptive or fraudulent conduct in digital settings, where transactions may occur across jurisdictions and with limited information. The use of "recognise the importance" is a common formulation found in agreements, such as the EU–Chile Framework Agreement, the EU–Japan Economic Partnership Agreement (EPA), the EU-New Zealand FTA, the EU-UK Trade and Cooperation Agreement (TCA), the EU-Mexico Global Agreement, the US-Oman FTA, the Australia–Singapore DEA, the USMCA, and the WTO Electronic Commerce Agreement (ECA), indicating wide alignment with broader trade efforts to support safe and trusted digital environments without creating a binding obligation.[55]

[55] EU-Chile Framework Agreement, Chapter 26, Article 11(1); EU-Japan EPA, Chapter 8, Section F, Article 78(1); EU-New Zealand FTA, Chapter 12, Article 12(1); EU-UK TCA, Article 208(1); EU-Mexico Global Agreement, Chapter 16, Article 7(1); US-Oman FTA, Chapter 14, Article 4; Australia–Singapore DEA, Article 15(1); USMCA, Chapter 19, Article 7(1); CPTPP, Chapter 14, Article 7(1); DEPA, Module 6, Article 3(1); RCEP, Chapter 12, Article 7(1); WTO ECA, Article 14(2).

(5) Paragraph 2 introduces a binding commitment requiring each Party to "adopt or maintain" consumer protection laws against fraudulent and deceptive commercial practices. The use of "shall" creates a clear legal obligation and reflects evolving best practices in digital trade frameworks such as CPTPP, the USMCA, the AfCTA Digital Trade Protocol, and the Australia-Singapore DEA.[56] While the MDEA avoids listing specific practices, as seen in the AfCTA Digital Trade Protocol or in the DEPA,[57] the obligation covers activities that cause or may cause harm to consumers, giving the provision both preventative and remedial reach. This formulation allows Parties to frame what constitutes fraudulent and deceptive commercial activities in connection with their domestic legal framework.

(6) Paragraph 3 furthers international cooperation by mandating that the Parties "shall exchange" information and experiences regarding national consumer protection approaches. This binding obligation strengthens regulatory dialogue and mutual learning, enabling Parties to align strategies, anticipate emerging threats, and coordinate responses to deceptive digital practices.[58] This marks a step forward towards cooperation and dialogue between the Parties with a view of strengthening online consumer protection in light of the inherent cross-border nature of online consumer protection in digital trade.

(7) Paragraph 4 builds on this cooperative theme by recognizing the importance of collaboration between national consumer protection agencies or equivalent bodies. The focus on "enhancing consumer welfare", as seen in the CPTPP, offers a broader framing as opposed to the wording "consumer trust" seen in comparable agreements, such as the EU–Chile Framework Agreement.[59] The recognition of institutional cooperation, without introducing a mandatory obligation, preserves flexibility while endorsing best practices and creating a reasonable expectation between the Parties. This approach resembles similar provisions in the CPTPP, the DEPA, the EU-Japan EPA, and the Australia–Singapore DEA, which promote cross-border enforcement coordination in digital markets.[60]

[56] CPTPP, Chapter 14, Article 7(2); USMCA, Chapter 19, Article 7(2); Australia–Singapore DEA, Article 15(3). See also: DEPA, Module 6, Article 3(3); EU-Chile Framework Agreement, Chapter 26, Article 11(1) second sentence; EU-New Zealand FTA, Chapter 12, Article 12(1); EU-UK TCA, Article 208(1); EU-Mexico Global Agreement, Chapter 16, Article 7(2); RCEP, Chapter 12, Article 7(2)

[57] AfCTA Digital Trade Protocol, Article 27(1)(a) to (d); DEPA, Module 6, Article 3(3). See also EU-New Zealand FTA, Chapter 12, Article 12(1)(a) to (c); EU-UK TCA, Article 208(1)(a) and (b); Australia–Singapore DEA, Article 15(2)(a) to (c). EFTA-Turkey Agreement, Annex XIII, Article 6(4).

[57] CPTPP, Chapter 14, Article 7(3); EU-Chile Framework Agreement, Chapter 26, Article 11(2);

[58] CPTPP, Chapter 14, Article 7(3); USMCA, Chapter 19, Article 7(3); Australia–Singapore DEA, Article 15(4); DEPA, Module 6, Article 3(2); EU-Japan EPA, Chapter 8, Article 78(2). See also: RCEP, Chapter 12, Article 7(2); USMCA, Chapter 19, Article 7(3); EU-New Zealand FTA, Chapter 12, Article 12(3); EU-UK TCA, Article 208(2); EU-Mexico Global Agreement, Chapter 16, Article 7(3).

[59] CPTPP, Chapter 14, Article 7(3); EU-Chile Framework Agreement, Chapter 26, Article 11(2);

[60] CPTPP, Chapter 14, Article 7(3); USMCA, Chapter 19, Article 7(3); Australia–Singapore DEA, Article 15(4); DEPA, Module 6, Article 3(2); EU-Japan EPA, Chapter 8, Article 78(2). See also: RCEP, Chapter 12, Article 7(2); USMCA, Chapter 19, Article 7(3); EU-New Zealand FTA, Chapter 12, Article 12(3); EU-UK TCA, Article 208(2); EU-Mexico Global Agreement, Chapter 16, Article 7(3).

(8) Paragraph 5 encourages transparency by stating that each Party "should publish" information about the consumer protection it affords in the digital space. This expectation supports both consumer awareness and regulatory predictability, enabling users and businesses – especially SMEs – to make informed decisions. While not binding, the provision echoes transparency norms found in the WTO and in digital economy agreements like the DEPA and the RCEP which, however, adopted a binding approach through the use of the wordings "shall make publicly available" and "shall publish".[61] In essence, while the language of Paragraph 5 establishes a non-binding obligation, it nonetheless seeks to promote and reinforce a transparent approach to consumer protection in order to foster consumers' awareness and access to redress mechanisms.

(9) Paragraph 6 complements the state-focused transparency obligation by encouraging businesses to disclose their consumer protection policies and procedures. This reflects a soft law approach to fostering self-regulation, accountability, and trust.[62] Paragraph 6 is in line with emerging global standards that promote transparency in terms and conditions.[63] By encouraging businesses to publish their procedures and policies related to online consumer protection, the provision indirectly fosters dialogue between Parties and businesses located within their territories. This approach may in turn promote the adoption of best practices in terms of transparency of businesses' procedures and policies related to online consumer protection.

(10) Overall, this provision represents a balanced and forward-looking approach to consumer protection in electronic commerce. It reinforces common principles, such as transparency, regulatory cooperation, and institutional engagement,- while preserving the flexibility necessary for Parties to tailor their approaches to domestic legal frameworks. The inclusion of both binding and non-binding commitments signals a strong normative convergence on consumer protection as a public policy imperative and a necessary condition for a trustworthy digital trade environment. As with other provisions in the MDEA, it draws on established models from leading agreements, while moderately updating the balance between mandatory commitments and sovereignty.

[61] DEPA, Module 6, Article 3(6) although adopting a binding formulation: "shall make publicly available"; RCEP, Chapter 12, Article 4 also adopting a binding formulation: "shall publish".
[62] Australia-Singapore DEA, Article 17.
[63] See for example: DEPA, Module 6, Article 3(6) and 3(8);

Article 13 – Unsolicited Commercial Electronic Communication

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

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

b. require either:

i. consent, as specified according to the laws and regulations of each Party, of recipients to receive commercial electronic messages; or

ii. supplier of unsolicited commercial electronic to provide for the minimization of unsolicited commercial electronic messages.

2. Each Party shall provide recourse against suppliers of unsolicited commercial electronic communications that do not comply with the measures adopted or maintained pursuant to paragraph 1.

3. The Parties should cooperate in the regulation of unsolicited commercial electronic communications.

Commentary

(11) This provision establishes a regulatory baseline for the control of unsolicited commercial electronic communications (commonly referred to as "spam") in the context of electronic commerce. It reflects a commitment by the Parties to adopt or maintain legal frameworks that reduce the burden of such communications on consumers and businesses, while preserving regulatory flexibility through alternative approaches to compliance. The structure combines binding obligations, Paragraphs 1 and 2, with cooperative ambitions in Paragraph 3, thereby aligning with international best practices on digital consumer protection and responsible marketing.

(12) Paragraph 1 sets out a mandatory obligation for each Party to adopt or maintain legal measures targeting unsolicited commercial electronic messages. This binding obligation requiring the adoption of measures regarding unsolicited commercial electronic communications is common in most digital trade agreements, including those where DCO Members are parties.[64] Rather than mandating a single regulatory model, the provision offers a menu of compliance options, allowing each Party to pursue: Subparagraph (a) opt-out mechanisms; and Subparagraph (b)(i) opt-in consent regimes; or Subparagraph (b)(ii) designed to minimize unsolicited messages. This flexibility accommodates different legal traditions, acknowledging regulatory diversity among Parties.

---

[64] EU – Chile Framework Agreement, Chapter 26, Article 12(2); EU-New Zealand FTA, Chapter 12, Article 13(1); EU-Mexico Global Agreement, Chapter 16, Article 8(1); AfCFTA Digital Trade Protocol, Article 28(1); WTO ECA, Article 15(2). See also: DEPA, Module 6, Article 2(1); Australia-Singapore DEA, Article 19(1); CPTPP, Chapter 14, Article 14(1); USMCA, Chapter 19, Article 13(1).

(13) Subparagraph (a) requires that suppliers of unsolicited commercial electronic messages facilitate recipients' ability to prevent continued receipt. This binding obligation requires Parties to impose to provider of unsolicited commercial electronic communications the adoption of mechanisms that enable recipients to inhibit receipt of such communications. This reflects the principle of user control and aligns with global norms requiring clear unsubscribe mechanisms, as found in agreements like EU-Chile Framework Agreement, the AfCFTA Digital Trade Protocol, the CPTPP, the USMCA, and the DEPA.[65] Such mechanisms are central to opt-out regimes, where the burden is placed on users to indicate their preference not to receive further communications.

(14) In addition to the requirement in Subparagraph (a), Subparagraph (b) provides for two alternative options. Subparagraph (b)(i) permits Parties to require recipients' consent, defined in accordance with each Party's domestic framework, prior to the delivery of commercial electronic messages. This aligns with opt-in models referenced in trade instruments like the EU-Chile Framework Agreement, the EU-Japan EPA, and the CPTPP.[66] While the provision does not define "consent," the flexibility granted to Parties allows alignment with broader domestic privacy frameworks.

(15) Alternatively, Subparagraph (b)(ii) offers an open-ended alternative, enabling Parties to adopt other measures aimed at minimizing unsolicited messages. This language ensures regulatory flexibility, acknowledging that effective anti-spam approaches may vary and evolve, particularly as technologies and threats develop. Comparable flexibility is found in the AfCFTA Digital Trade Protocol, the CPTPP the RCEP, the DEPA, and the WTO ECA, which all provide similar catch-all clauses for addressing spam without prescribing specific compliance mechanisms.[67]

(16) Paragraph 2 complements the obligation in paragraph 1 by requiring that each Party provide legal recourse against non-compliant suppliers. This ensures that anti-spam measures are not purely aspirational but are enforceable, enabling individuals or authorities to hold violators accountable. While the provision does not specify the nature of recourse (e.g., administrative penalties, civil remedies, or criminal sanctions), the obligation reinforces the expectation that anti-spam regimes must include meaningful enforcement pathways. This approach mirrors those found in the EU-Japan EPA, the EU-New Zealand FTA, the AfCFTA Digital Trade Protocol, the USMCA, and the CPTPP.[68]

[65] EU-Chile Framework Agreement, Chapter 26, Article 12(2)(a); EU-Japan EPA, Chapter 8, Article 79(1)(a); EU-Mexico Global Agreement, Chapter 16, Article 8(1)(a); AfCFTA Digital Trade Protocol, Article 28(1)(b); DEPA, Module 6, Article 2(1)(a); Australia-Singapore DEA, Article 19(1)(a); CPTPP, Chapter 14, Article 14(1)(a); USMCA, Chapter 19, Article 13(2)(a); RCEP, Chapter 12, Article 9(1)(a); WTO ECA, Article 15(2)(a).

[66] EU-Chile Framework Agreement, Chapter 26, Article 12(2)(b); EU-Japan EPA, Chapter 8, Article 79(1(b); CPTPP, Chapter 14, Article 14(1)(b). See also: EU-Mexico Global Agreement, Chapter 16, Article 8(1)(b); DEPA, Module 6, Article 2(1)(b); Australia-Singapore DEA, Article 19(1)(b); USMCA, Chapter 19, Article 13(2(b); RCEP, Chapter 12, Article 9(1)(b); WTO ECA, Article 15(2)(b).

[67] AfCFTA Digital Trade Protocol, Article 28(1)(c); CPTPP, Chapter 14, Article 14(1)(c); RCEP, Chapter 12, Article 9(1)(c); th DEPA, Module 6, Article 2(1)(c); WTO ECA, Article 15(2)(c).

[68] EU-Japan EPA, Chapter 8, Article 79(3); EU-New Zealand FTA, Chapter 12, Article 13(5) ; AfCFTA Digital Trade Protocol, Article 28(2); CPTPP, Chapter 14, Article 14(2); USMCA, Chapter 19, Article 13(4). See also: EU-UK TCA, Article 209(5); EU-Mexico Global Agreement, Chapter 16, Article 8(3); DEPA, Module 6, Article 2(2); Australia-Singapore DEA, Article 19(3); RCEP, Chapter 12, Article 9(2); WTO ECA, Article 15(4).

(17) Paragraph 3 introduces a non-binding commitment to regulatory cooperation in the governance of unsolicited commercial electronic communications. Given the cross-border nature of spam and the difficulty of enforcement against foreign-based senders, international cooperation is essential. The use of "should" reflects a soft obligation that echoes other digital trade agreements, such as the EU-Mexico Global Agreement, the AfCFTA Digital Trade Protocol, the DEPA, and the CPTPP, which similarly promote cooperation between enforcement bodies, the exchange of information, and coordinated action, albeit using a more binding language.[69] This provision seeks to foster future regulatory convergence and shared capacity-building in the face of evolving challenges in the digital marketing ecosystem.

(18) This provision supports a layered approach to the regulation of unsolicited commercial messages, combining enforceable baseline commitments with regulatory flexibility and intergovernmental cooperation. It reflects widely accepted international standards while allowing Parties to maintain or tailor domestic legal models offering alternatives to this end, whether consent-based, complaint-based, or hybrid.

[69] EU-Mexico Global Agreement, Chapter 16, Article 8(4): "shall endeavour to cooperate"; AfCFTA Digital Trade Protocol, Article 28(3): "shall cooperate"; DEPA, Module 6, Article 2(3): "shall cooperate"; CPTPP, Chapter 14, Article 14(3): "shall endeavour to cooperate". See also: Australia-Singapore DEA, Article 19(4): "shall endeavour to cooperate"; USMCA, Chapter 19, Article 13(5): "shall endeavour to cooperate"; RCEP, Chapter 12, Article 9(3): "shall endeavour to cooperate"; WTO ECA, Article 15(5): "shall endeavour to cooperate".

CYBERSECURITY

Context and Scope

(1) Cybersecurity regulatory policies have emerged as a critical area of governance in response to the increasing reliance on digital infrastructure and the growing frequency and sophistication of cyber threats. As governments, businesses, and individuals become more interconnected, the risks posed by data breaches, ransomware attacks, and disruptions to critical infrastructure have intensified. Regulatory frameworks seek to mitigate these risks by setting legal obligations and technical standards to ensure the integrity, availability, and confidentiality of digital systems. This includes sector-specific rules (e.g., for finance, energy, or healthcare), national cybersecurity strategies, and mandatory incident reporting requirements. Many countries also align their policies with international standards and best practices to promote interoperability and cross-border trust.

(2) The scope of cybersecurity regulation typically encompasses multiple layers of digital resilience. It may include the protection of critical information infrastructure, the establishment of national Computer Security Incident Response Teams (CSIRTs), risk management obligations for private sector operators, and measures to enhance public-private cooperation. Increasingly, regulations also address emerging challenges such as supply chain security, cloud computing risks, and the role of artificial intelligence in cyber defense. Beyond enforcement, modern regulatory approaches emphasize capacity building, workforce development, and international collaboration to respond to the global nature of cyber threats. The result is a multifaceted policy domain that intersects with privacy law, digital trade, national security, and innovation policy.

Article 14 –Cybersecurity

1. The Parties have a shared vision to promote secure digital trade to achieve global prosperity and recognise that cybersecurity underpins the digital economy.

2. The Parties shall adopt or maintain measures to ensure cybersecurity to prevent and address cybercrime within its jurisdiction. In the developing or maintaining such measures, each Party shall have due regards to standards, guidelines, and best practice set forth in relevant international instruments.

3. The Parties recognise that threats to cybersecurity undermine confidence in digital trade and shall endeavour to:

a. build the capabilities of their national entities responsible for computer security incident response;

b. using existing collaboration mechanisms to cooperate to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties; and

c. workforce development in the area of cybersecurity, including through possible initiatives relating to the training and development of youths, improving diversity and mutual recognition of qualifications.

Commentary

(3) This provision reflects a growing recognition in international digital trade law of the foundational role that cybersecurity plays in enabling trust, resilience, and economic growth in the digital economy. It balances binding commitments with aspirational cooperation by combining obligations to adopt or maintain cybersecurity measures with softer language encouraging capacity building, collaboration, and human capital development. The structure of the provision reflects a layered approach: Paragraph 1 expresses a high-level vision; Paragraph 2 establishes binding national-level commitments; and Paragraph 3 seeks to foster cooperative initiative.

(4) Paragraph 1 sets the normative tone by articulating a shared vision among the Parties. The recognition that cybersecurity "underpins" the digital economy aligns with similar acknowledgments in recent trade agreements, such as the DEPA and the Australia-Singapore DEA.[70] These agreements similarly emphasize the importance of cybersecurity to safeguard digital ecosystems and facilitate secure cross-border data flows. The mention of "global prosperity" links digital resilience to broader development goals, suggesting that security is not only a technical concern but also a global economic priority.

(5) Paragraph 2 introduces a binding obligation for each Party to "adopt or maintain measures to ensure cybersecurity", targeting both prevention and response to cybercrime. This language follows a functional approach, granting Parties flexibility in how to implement such measures while ensuring a common baseline of regulatory action. Paragraph 2 mirrors the language used in the AfCFTA Digital Trade Protocol.[71] The reference to "cybercrime" introduces a link with domestic and international criminal law instruments, like the Budapest Convention on Cybercrime.[72]

[70] DEPA, Module 5, Article 1(1); and Australia-Singapore DEA, Article 34(1). Other Agreements, such as USMCA, Chapter 19, Article 15(1) and the WTO ECA, Article 17(1) adopt a different programmatic language: "The Parties recognize that threats to cybersecurity undermine confidence in electronic commerce".

[71] AfCFTA Digital Trade Protocol, Article 25(1).

[72] Council of Europe, Convention on Cybercrime, Budapest, European Treaty Series- No. 185, 23 November 2001.

(6) A key element of paragraph 2 is the requirement that such measures have "due regard to standards, guidelines, and best practice set forth in relevant international instruments." This phrase promotes convergence with global norms without mandating adherence to specific standards. It recalls the language used in the AfCFTA Digital Trade Protocol, which reference regional, continental, and internationally recognized instruments, as well as the adoption of bet practices by enterprises.[73] By avoiding specific enumeration, the provision leaves room for regulatory evolution while encouraging interoperability and good practice alignment.

(7) Paragraph 3 shifts from domestic obligations to international cooperation. It recognizes that cybersecurity threats are inherently transboundary, and thus, no single Party can effectively ensure cybersecurity in isolation. The clause commits Parties to "endeavour to" take certain steps—this is soft-law language that signals intent without creating a binding legal obligation. The areas listed (incident response, collaboration, and workforce development) reflect the multidimensional nature of cybersecurity governance. This approach aligns with several digital trade agreements such as the AfCFTA Digital Trade Protocol, the DEPA, the Australia-Singapore DEA, the CPTPP, the USMCA, the RCEP, and the WTO ECA.[74] However, it is important to note that the DEPA, the Australia-Singapore DEA, and the CPTPP adopt a lesser binding language by establishing that "the Parties recognize the importance"

(8) Subparagraph (a) emphasizes capacity building for national computer security incident response teams (CSIRTs). This mirrors equivalent clauses in the AfCFTA Digital Trade Protocol, the DEPA, the Australia-Singapore DEA, the CPTPP, the USMCA, the RCEP, and the WTO ECA all of which encourage Parties to enhance their incident response frameworks.[75] However, it is important to note that the DEPA, the Australia-Singapore DEA, and the CPTPP all use a lesser binding language Strengthening CSIRTs improves domestic cyber resilience and facilitates cross-border coordination in times of crisis.

(9) Subparagraph (b) supports operational collaboration through existing mechanisms, such as regional cybersecurity platforms, public-private partnerships, or information-sharing agreements. The focus on malicious intrusions or code dissemination responds to real-world threats (e.g., ransomware attacks, botnets) that have significant cross-border effects. This subparagraph recalls the language used in several international agreements.[76]

[73] EU-Japan EPA, Chapter 8, Article 80(2); AfCFTA Digital Trade Protocol, Article 25(1) and 25(3).
[74] AfCFTA Digital Trade Protocol, Article 25(2); DEPA, Module 5, Article 1(2); Australia-Singapore DEA, Article 34(2); CPTPP, Chapter 14, Article 16; USMCA, Chapter 19, Article 15(1); RCEP, Chapter 12, Article 13; WTO ECA, Article 17(2).
[75] AfCFTA Digital Trade Protocol, Article 25(2)(a); DEPA, Module 5, Article 1(2)(a); Australia-Singapore DEA, Article 34(2)(a); CPTPP, Chapter 14, Article 16(a); USMCA, Chapter 19, Article 15(1)(a); RCEP, CHapter 12, Article 13(a); WTO ECA, Article 17(2)(a).
[76] AfCFTA Digital Trade Protocol, Article 25(2)(c); DEPA, Module 5, Article 1(2)(b); Australia-Singapore DEA, Article 34(2)(b); CPTPP, Chapter 14, Article 16(b); USMCA, Chapter 19, Article 15(1(b); RCEP, Chapter 12, Article 13(b).

(10) Subparagraph (c) addresses a critical but often underrepresented dimension: cybersecurity workforce development. By including references to training, diversity, and mutual recognition of qualifications, the provision aligns with sustainable development and inclusion agendas. This is a relatively innovative feature in digital trade chapters—complementing the more technical focus of previous agreements with a long-term human capital strategy.[77]

(11) Overall, the provision combines binding and aspirational elements to build both national regulatory resilience and international cooperation in cybersecurity. While it avoids prescribing specific technical standards or enforcement mechanisms, it encourages Parties to move toward a shared model of preparedness and cross-border support. This approach reflects current trends in digital trade instruments, especially the approaches adopted by the DEPA, and the AfCFTA Digital Trade Protocol, which similarly view cybersecurity not merely as a technical or criminal matter, but as a pillar of trust in digital trade.[78]

[77] AfCFTA Digital Trade Protocol, Article 25(2)(b) also provides for a capacity building mechanism but without identifying specific policy areas where capacity building is a key aspect.
[78] AfCFTA Digital Trade Platform, Article 25; DEPA, Module 5, Article 1.

ARTIFICIAL INTELLIGENCE

Context and Scope

(1) Artificial intelligence regulatory policies are developing in response to the rapid deployment of AI technologies across virtually all sectors of the economy and society. As AI systems increasingly influence decision-making in areas such as healthcare, finance, employment, law enforcement, and public services, concerns have grown over issues such as transparency, accountability, bias, discrimination, and the protection of fundamental rights. Policymakers are working to ensure that the development and use of AI is safe, ethical, and aligned with democratic values.

(2) The scope of AI regulation typically includes governance frameworks that address risk assessment, human oversight, data quality, algorithmic transparency, and accountability mechanisms. In addition to binding rules, governments promote soft law instruments such as ethical guidelines, voluntary codes of conduct, and sandboxes for innovation. Cooperation between public authorities, academia, civil society, and industry is key to developing

Article 15 – Artificial Intelligence

1. The Parties recognise that the use and adoption of Artificial Intelligence (AI) technologies have grown increasingly widespread in the digital economy. The Parties should cooperate, in accordance with their respective relevant policies, through:

a. sharing 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; and

c. encouraging commercialisation opportunities and collaboration between researchers, academics and industry.

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

3. To this end, the Parties should promote the adoption of ethical and governance frameworks that support the trusted, safe and responsible use of AI technologies (AI Governance Frameworks). In adopting AI Governance Frameworks, the Parties should take into consideration internationally recognised principles or guidelines, including explainability, transparency, fairness and human-centred values.

4. The Parties shall, where appropriate and consistent with domestic law, promote transparency and accountability in the use of automated decision-systems and algorithmic tools in trade-related administrative processes (e.g., customs, licensing, certification), including sharing best practices on explainability, human oversight and redress mechanisms.

Commentary

(3) This provision marks the inclusion of Artificial Intelligence (AI) as a distinct regulatory theme within digital trade frameworks, recognizing its increasing role in shaping innovation, competitiveness, and governance in the digital economy. While the language remains primarily aspirational and non-binding, the text reflects a clear policy direction: to foster cooperation, align ethical and governance frameworks, and promote responsible AI adoption across borders. The approach is consistent with emerging digital economy agreements that treat AI as both a strategic opportunity and a regulatory challenge.[79]

(4) Paragraph 1 establishes a cooperation-oriented objective, acknowledging the growing adoption of AI technologies and encouraging the Parties to collaborate through non-binding measures. The formulation "should cooperate… through" signals a soft obligation, reflecting the early-stage nature of international AI governance. As similarly seen in the DEPA and the Australia-Singapore DEA, the three subparagraphs articulate the areas of cooperation in terms of:

- Sharing of research and industry practices responds to the need for knowledge exchange and regulatory learning. It parallels the objective set forth in the DEPA.
- Promoting the responsible use of AI across both business and society.
- Encouraging commercialization and research-industry collaboration links AI governance with innovation policy. This reflects a dual mandate: enabling innovation while managing risk.[80]

(5) Paragraph 2 provides the normative underpinning of the provision by recognizing the importance of ethical and governance frameworks to ensure the trusted, safe, and responsible use of AI technologies. The paragraph further introduces a cross-border

[79] DEPA, Module 8, Article 2.
[80] Australia-Singapore DEA, Article 31(1)(a) to (c); DEPA, Module 8, Article 2(2).

dimension by emphasizing the benefits of international alignment. This anticipates future interoperability of AI regimes, drawing a parallel with the DEPA, which highlights the value of harmonized governance in emerging technologies.[81]

(6) Importantly, this recognition acknowledges that while AI development is largely domestic, its economic and societal impact is global. By calling for mutual understanding, the text encourages a convergence pathway—complementary to ongoing work in standard-setting bodies such as the ISO/IEC JTC 1/SC 42 (Artificial Intelligence).

(7) Paragraph 3 moves from recognition to policy direction, introducing an endeavour obligation to promote the adoption of AI Governance Frameworks. While the obligation is not binding ("shall endeavour"), it sets clear expectations about the substance of these frameworks. The inclusion of internationally recognised principles, such as explainability, transparency, fairness, and human-centered values, mirrors the core values promoted by the OECD AI Principles, the UNESCO Recommendation on the Ethics of AI (2021), and the EU's AI Act. The use of the term "AI Governance Frameworks" as a defined concept signals the emerging consensus that AI regulation should not only address technical standards, but also institutional, ethical, and procedural safeguards.The explicit reference to "explainability" and "human-centred values" places the provision in line with risk-based approaches to AI governance, which emphasize impact on individuals and society.

(8) Paragraph 4 focuses on trade-related administrative processes, areas where algorithmic decision-systems increasingly play a role, such as customs risk assessment, licensing, certification and compliance procedures. The article encourages transparency and accountability in these uses, subject to domestic law and appropriate circumstances. The language encourages the exchange of best practices related to explainability, human oversight, auditability and mechanisms for redress. This approach promotes trust among traders and users while supporting the modernization of public administration.

(9) Overall, the provision adopts a forward-looking and principled approach to AI, recognizing its transformative potential while highlighting the need for cooperation, ethics, and responsible governance. While its legal effect is not prescriptive, the provision plays an important role in anchoring AI governance within the broader architecture of digital trade. Similar to provisions found in the DEPA, and the UK–Singapore DEA, it reflects a global trend: embedding AI into trade policy to ensure that innovation is pursued in a manner that is trustworthy, transparent, and inclusive.[82]

[82] DEPA Module 8, Article 2; UK-Singapore DEA, Article 8.61-R.

SOURCE CODE

Context and Scope

(10) Regulatory policies on source code govern the conditions under which domestic authorities can request, access, or require disclosure of the underlying code that drives software and digital products. These policies have become increasingly relevant in the context of digital trade and cybersecurity, where national interests in security, enforcement, and oversight intersect with commercial concerns around innovation, intellectual property, and confidentiality. At the domestic level, a legal or regulatory framework on source code typically addresses whether authorities may require disclosure of source code as a condition for market access or during regulatory oversight procedures. In many jurisdictions, this framework is shaped by data protection, competition, and consumer safety laws, and balanced against the protection of intellectual property rights.

(11) From a trade policy perspective, domestic regulations that require the mandatory transfer or access to source code, for example as a condition for import, sale, or use of software or products containing software, are often viewed as barriers to trade and innovation, unless they are narrowly tailored and subject to appropriate safeguards. From this perspective, source code regulation reflects a sensitive balancing act between state oversight and the preservation of commercial trust, protection of intellectual property rights, and technological openness.

Article 16 – Source Code

1. The Parties shall not require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.

2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure and to the following conditions:

a. A regulatory body or judicial authority of a State Party, requiring transfer or access to a source code or algorithm thereof under this Article, shall protect the source code of the software or an algorithm expressed in that source code preserved and availed to them by a person of the State Party against unlawful access, acquisition, or appropriation by a third party.

b. Any such access shall be: (i) necessary to achieve the stated purpose and not applied in a manner constituting arbitrary or unjustifiable discrimination or a disguised restriction on trade; (ii) strictly limited in scope, format and duration to what is required; (iii) subject to legally enforceable confidentiality and use-limitation obligations no less protective than those applicable to undisclosed information under the Party's law; (iv) implemented through secure review arrangements avoiding disclosure to competitors; and (v) without prejudice to the information's status as a trade secret, where claimed by the trade secret owner.

3. For greater certainty, paragraph 1 does not apply to the voluntary transfer of, or granting of, access to a source code owned by a person of another Party under open-source licenses, such as in the context of open-source coding, or on a commercial basis, such as in the context of a freely negotiated contract.

4. Before requiring access under paragraph 2, the authority shall provide prior written notice stating legal basis, purpose, and scope; consider less intrusive means proposed by the affected person; issue a reasoned decision within a reasonable period (ordinarily within 90 days of complete submission, unless justified by case complexity); and ensure access to prompt and impartial review or appeal, with appropriate remedies.

Commentary

(12) This provision establishes a baseline prohibition on requiring the transfer of, or access to, software source code or algorithms as a condition for market access, while carving out narrowly framed, safeguard-heavy exceptions for legitimate regulatory and judicial functions. Its objective is to protect intellectual property and trade secrets, support innovation, and reduce barriers to software trade, without depriving authorities of the tools needed to enforce domestic law. Provisions of this type have become common in modern digital trade agreements. This provision provides for a general ban on forced disclosure, confined exceptions for defined proceedings and strong confidentiality and due-process guarantees.

(13) Paragraph 1 contains the core obligation. It prevents Parties from requiring transfer of, or access to, a "source code of software owned by a person of another Party, or to an algorithm expressed in that source code," as a condition for the import, distribution, sale or use of that software, or of products containing that software. By covering both software and "products containing that software," and explicitly referring to "an algorithm expressed in that source code," the provision protects not only stand-alone programs but also embedded and AI-driven systems. This responds to concerns that compulsory disclosure could operate as disguised protectionism, or lead to the unauthorized dissemination of commercially sensitive logic, models and training architectures, thereby undermining incentives to innovate.

(14) Paragraph 2, together with its subparagraphs (a) and (b) qualifies the general prohibition by setting out tightly controlled circumstances in which a regulatory body or judicial authority may require preservation of, and access to, source code or algorithms. The chapeau to paragraph 2 confines such access to a "specific investigation, inspection, examination, enforcement action, or judicial proceeding," and subjects it to safeguards against unauthorized disclosure as well as to the additional conditions listed in subparagraphs (a) and (b). Subparagraph 2(a) obliges the authority to protect any source code or algorithm made available against "unlawful access, acquisition, or appropriation by a third party," maintaining that the exceptional access must preserve source code.

(15) Subparagraph 2(b) then codifies a series of substantive conditions: access must be necessary to achieve the stated purpose and not applied in a manner constituting arbitrary or unjustifiable discrimination or a disguised restriction on trade; strictly limited in scope, format and duration; subject to legally enforceable confidentiality and use-limitation obligations no less protective than those applicable to undisclosed information; implemented through secure review arrangements avoiding disclosure to competitors; and without prejudice to the information's status as a trade secret where that status is claimed. This cluster of safeguards mirrors emerging treaty practice that combines necessity/proportionality, non-discrimination and trade-secret protection, and reflects best-practice proposals for operationalizing "secure review" through controlled environments, escrow or tool-assisted review. Collectively, the conditions signal that source code access should be exceptional, purpose-bound and rights-preserving.

(16) The explicit reference in paragraph 2(b)(iv) to "secure review arrangements avoiding disclosure to competitors" is particularly significant. It translates confidentiality principles into an operational standard by requiring that any review mechanism be designed so as not to reveal sensitive code or algorithms to commercial rivals, even indirectly. This responds to concerns in the literature that, without such modalities, access rights, even when limited to defined proceedings, could chill innovation or expose trade secrets beyond what is necessary for oversight. At the same time, the provision recognises that effective governance of software and AI-enabled technologies may require targeted insight into the underlying logic, and thus strikes a calibrated balance between enforcement needs and protection of proprietary assets.

(17) Paragraph 3 addresses voluntary transfers. It clarifies that the obligation in paragraph 1 does not apply where source code is shared freely under open-source licences or on a commercial basis under freely negotiated contracts. This ensures that the prohibition on compelled disclosure does not inadvertently constrain open-source ecosystems.

(18) Paragraph 4 adds a further layer of administrative-law safeguards around the exercise of access powers under paragraph 2. Before requiring access, authorities must provide prior written notice stating the legal basis, purpose and scope of the request; consider less intrusive means proposed by the affected person; issue a reasoned decision within a reasonable period (ordinarily within 90 days of complete submission, unless justified by complexity); and ensure access to prompt and impartial review or appeal, with appropriate remedies. Few existing digital trade agreements spell out these due-process elements directly in the source-code clause itself, although they are often implicit in broader transparency and review obligations. Their inclusion here proceduralises access in a way that makes it exceptional, reviewable and accountable, thereby providing clearer legal certainty for firms and addressing concerns about open-ended or opaque demands.

(19) Taken together, Article 16 is aligned with the emerging consensus that digital trade rules should neither hard-wire unconditional secrecy (which could unduly weaken enforcement) nor permit generalised, ex ante disclosure mandates (which could deter innovation and investment). Instead, it establishes a clear baseline prohibition on forced transfer or access as a condition for market entry, narrowly carves out access for defined public-interest functions, and embeds confidentiality, trade-secret protection, secure-review mechanisms and due-process safeguards. In doing so, the Article seeks to give regulators the tools they need for targeted oversight, while offering businesses a predictable and rights-conscious framework for the treatment of one of their most sensitive digital assets.

SMEs AND DIGITAL INCLUSION

Context and Scope

(1) Domestic regulatory policies on digital inclusion and support for small and medium-sized enterprises (SMEs) aim to ensure that all individuals and businesses can effectively participate in and benefit from the digital economy. As digital technologies become essential to economic growth, employment, and public services, governments are increasingly focused on removing barriers to access, affordability, connectivity, and digital literacy. Digital inclusion policies typically address the needs of underrepresented or vulnerable groups by promoting equitable access to digital tools, services, and infrastructure. These policies often include programs for digital skills development, subsidies or public-private partnerships to expand broadband coverage, and frameworks for collecting disaggregated data to track digital divides.

(2) In parallel, many governments have developed targeted strategies to help SMEs leverage digital trade opportunities. Given that SMEs form the backbone of most economies but often lack the scale, resources, or expertise to digitize, public policies support their digital transformation through measures such as access to digital platforms, e-commerce capacity building, simplified regulatory procedures, and financial tools for innovation and adaptation. Regulatory frameworks may also promote SME participation in international value chains through initiatives like digital marketplaces, digital government procurement access, or cross-border cooperation schemes. Together, digital inclusion and SME digitalization policies form a critical part of a broader agenda for inclusive digital trade, helping to distribute the benefits of the digital economy more evenly and sustain long-term, equitable growth.

Article 17 – SMEs and Digital Inclusion

1. The Parties recognise the importance of digital inclusion to ensure that all people 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.

3. To this end, the Parties should cooperate on matters relating to digital inclusion, including:

a. 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. 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

f. other areas as jointly agreed by the Parties.

4. The Parties recognise the role played by SMEs in economic growth and job creation, and the need to address the barriers to participation in digital trade for those entities. To this end, the Parties should:

a. foster close cooperation on digital trade between SMEs of the Parties;

b. encourage their participation in platforms that help link them with international suppliers, buyers, and other potential business partners; and

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

Commentary

(3) This provision introduces a cooperation-based framework aimed at enhancing digital inclusion, defined as ensuring that individuals, communities, and businesses—particularly those underrepresented or underserved—have the necessary tools, skills, and opportunities to participate meaningfully in the digital economy. It reflects a growing consensus in digital trade policy that economic growth must be inclusive and that digital transformation should not exacerbate existing inequalities. Similar commitments appear in the DEPA, the AfCFTA Digital Trade Protocol, and the Australia-Singapore DEA.[83]

(4) Paragraph 1 affirms the Parties' shared recognition of digital inclusion as a strategic and developmental priority. The paragraph is declaratory in nature, establishing a common value baseline but not creating binding obligations.

(5) Paragraph 2 builds on this value statement by linking inclusion to the removal of barriers to digital opportunity, framing access as a function not only of infrastructure but also of regulatory and socio-economic environments. The language here mirrors elements of the DEPA, which places explicit emphasis on reducing barriers to the access to digital economy opportunities.[84] While the clause remains non-binding, it implies that the Parties should evaluate and address systemic impediments such as affordability, connectivity gaps, and digital literacy deficits.

[83] DEPA, Module 10, Article 1 and 2; and Module 11, Article 1 AfCFTA Digital Trade Protocol, Articles 30 and 31; Australia-Singapore DEA, Articles 36 and 37.

[84] DEPA, Module 11, Article 11(2) first sentence.

(6) Paragraph 3 provides the operational content of the provision by outlining a menu of cooperative activities. These include knowledge-sharing mechanisms, capacity-building initiatives, and support for data collection frameworks.

- Subparagraph (a) encourages the exchange of best practices and expert cooperation. The Australia-Singapore DA and the AfCFTA Digital Trade Protocol contain similar language but, contrary to the MDEA, hey establish a binding obligation in this area.[85]
- Subparagraph (b) explicitly links inclusion to inclusive and sustainable economic growth This reflects the growing trend of integrating development objectives into trade frameworks.
- Subparagraph (c) refers to addressing barriers to access to digital trade opportunities and outlines policy areas where Parties should cooperate to increase SMEs access to digital trade opportunities and foster digital inclusion. These policy areas reflect domains where developing economies may face severe challenges in adopting digital tools and platforms.
- Subparagraph (d) promotes targeted programme development to increase the participation of all groups in the digital economy. Similar language appears in the DEPA, which emphasizes inclusive policy environments for marginalized communities, including women, rural populations, and persons with disabilities.[86]
- Subparagraph (e) higlights the importance of data-driven policymaking, encouraging the use of disaggregated data and statistical indicators to measure participation.
- Subparagraph (f) provides flexibility by allowing future areas of cooperation, echoing formulations in modern digital trade agreements like the EU-New Zealand FTA, the EU-Mexico Global Agreement, and the DEPA, which include open-ended cooperation clauses.[87]

(7) Paragraph 4 brings special attention to Small and Medium-Sized Enterprises (SMEs), recognizing their role in economic dynamism and job creation. Other digital trade agreements equally recognize the pivotal role played by SMEs in developing a thriving digital trade environment, which acknowledge the need to support SME digital integration without imposing any binding obligations.[88] The AfCFTA Digital Trade Protocol reflects a diverging trend, as it imposes binding obligations on parties with respect to the promotion of SMEs participation to digital trade.[89]

- Subparagraph (a) supports closer SME-to-SME cooperation, potentially through matchmaking platforms, digital clusters, or incubators—mechanisms widely promoted in OECD SME strategies and APEC SME digital initiatives.

[85] Australia-Singapore DEA, Article 36(2)(a); AfCFTA Digital Trade Protocol, Article 31(a).
[86] DEPA, Module 11, Article 1(3)(d).
[87] EU-New Zealand FTA, Chapter 12, Article 14(1)(f); EU-Mexico Global Agreement, Chapter 16, Article 11(1(f); DEPA; Module 11(3)(f).
[88] DEPA, Module 10, Article 1(2); Australia-Singapore DEA, Article 36(2).
[89] AfCFTA Digital Trade Protocol, Articles 30 to 33.

• Subparagraph (b) focuses on increased participation in digital trade platforms, echoing commitments in DEPA and the WTO's Work Programme on E-Commerce, which recognize digital marketplaces as gateways for SME internationalization.
• Subparagraph (c) advocates for best practice sharing in digital skills, financing access, and procurement participation, echoing the language used in the . These areas are commonly cited as key enablers of SME success.

(8) In conclusion, this provision represents a progressive and cooperative approach to embed inclusion in the digital economy. By addressing both structural and operational aspects of digital marginalization, from access infrastructure to programmatic outreach and SME enablement, it reflects the evolving role of trade agreements as tools for broader economic and social policy alignment. While largely aspirational and framed as "best efforts" cooperation, these commitments provide a valuable platform for policy coordination, knowledge transfer, and potentially the design of capacity-building programs that address persistent inclusion gaps across the Parties' economies.

COOPERATION

Context and Scope

(1) Cooperation provisions in digital trade agreements reflect an understanding among Parties that realizing the benefits of the digital economy requires active dialogue, joint initiatives, and capacity-building to bridge regulatory, infrastructural, and technological gaps. These provisions are particularly important in light of the rapidly evolving nature of digital technologies, where consistent regulation, trust frameworks, and interoperability mechanisms have not yet fully converged globally. As such, cooperation chapters often serve as a platform for alignment and policy experimentation, particularly in areas where domestic regulation is still developing or varies significantly across jurisdictions. Cooperation provisions are typically broad in scope, covering topics such as personal data protection, cybersecurity, digital identity, e-invoicing, artificial intelligence, and digital inclusion. They may encourage the exchange of regulatory experiences, the development of pilots or sandboxes, and support for SMEs participation in the digital economy.

(2) The flexibility and non-binding nature of cooperation provisions make more attractive, as they avoid hard commitments while encouraging proactive engagement. At the same time, their open-ended nature can lead to ambiguity or inconsistent implementation unless followed by concrete institutional mechanisms or technical assistance frameworks. Nonetheless, such provisions often lay the groundwork for future alignment in regulatory areas where binding rules are currently premature or politically sensitive. In this sense, they serve as a diplomatic tool for convergence and trust-building in the digital economy.

Article 18 – Cooperation

1. The Parties recognize the importance of strengthening cooperation to support the development of a trusted, secure, and open digital economy. The Parties shall cooperate to advance the objectives of this Agreement through dialogue, information exchange, and jointly agreed activities.

2. The parties shall endeavor to cooperate on matters related to this Agreement, including:

a. policy and regulatory exchanges on digital trade, personal data protection, cybersecurity, and trust frameworks;

b. pilots and regulatory sandboxes, including on digital identity, e-invoicing, and cross-border payments;

c. interoperability work on standards, conformity assessment, and mutual recognition where appropriate;

d. SME support, including matchmaking platforms and access to finance tools;

e. initiatives that promote participation of women, youth, persons with disabilities, and rural communities in the digital economy;

f. participation and joint proposals in relevant regional and multilateral fora.

3. The Parties shall encourage participation, as appropriate, by private sector, academia, technical bodies, and civil society in cooperation activities.

Commentary

(3) This provision establishes a cooperation framework among the Parties aimed at advancing the objectives of the Agreement and supporting the development of a trusted, secure, and inclusive digital economy. It emphasizes the importance of collaborative approaches to managing cross-border digital policy challenges and facilitating mutual capacity building. The provision reflects a non-binding model of cooperation common in digital trade agreements, whereby the Parties commit to dialogue, information exchange, and the pursuit of mutually agreed activities. Similar cooperative clauses are found in the EU-JAPAN EPA, the CPTPP and the USMCA, all of which highlight the critical role of international collaboration in ensuring the coherence and interoperability of digital regulatory environments.[90] Cooperation provisions in electronic commerce or digital trade chapters are common practice, although they differ in scope and bindingness of cooperation obligations.

(4) Paragraph 1 sets out a shared commitment to strengthen cooperation among the Parties to foster a secure, open, and trustworthy digital economy. The phrase "shall cooperate" signals a binding obligation in form, though it is tempered by the flexible formulation "through dialogue, information exchange, and jointly agreed activities," which allows each Party to determine the scope and depth of its engagement. The inclusion of the overarching objective of advancing the goals of the Agreement reinforces the cooperative spirit and aligns with international digital cooperation clauses, which also adopt flexible language to promote ongoing collaboration without prescribing specific outcomes.

[90] EU-Japan EPA, Chapter 8, Article 80; CPTPP, Chapter 14, Articles 15 and 16; USMCA, Chapter 19, Article 14. See also: EU-Chile Framework Agreement, Chapter 26, Article 14; EU-New Zealand FTA, Chapter 12, Article 14; EU-UK TCA, Article 211; EU-Mexico Global Agreement, Chapter 16, Article 11; EU-Singapore FTA, Chapter 8, Article 61; EU-Vietnam FTA, Chapter 8, Article 52; EU-Canada CETA, Chapter 16, Article 6; GCC-Singapore FTA, Chapter 8, Article 4; AfCFTA Digital Trade Protocol, Article 43; RCEP, Chapter 12, Article 4; Australia-Singapore DEA, Article 33.

(5) Paragraph 2 broadens the scope of potential cooperation by listing thematic areas where Parties are encouraged to work together. The use of "shall endeavor to cooperate" clearly identifies the provision as non-binding. Subparagraph 2(a) highlights cooperation in key regulatory domains such as digital trade policy, data protection, cybersecurity, and trust frameworks. This mirrors similar cooperation priorities in the CPTPP, which promotes regulatory dialogue and knowledge sharing across Parties.[91]

(6) Subparagraph 2(b) refers to the development and use of regulatory sandboxes and pilot programs in emerging digital areas, such as digital identity, e-invoicing, and cross-border payments. These tools allow regulators to experiment with new technologies and policies in a controlled environment. Subparagraph 2(c) supports cooperation on interoperability in standards, conformity assessment, and mutual recognition. This clause reflects the importance of reducing technical barriers to digital trade and facilitating cross-border integration.

(7) Subparagraph 2(d) emphasizes support for SMEs, including the provision of matchmaking platforms and access to finance tools. The EU-New Zealand FTA and the AfCFTA Digital Trade Protocol present similar cooperation mechanisms with respect to MSMEs.[92] Subparagraph 2(e) reflects a broader social inclusion agenda by promoting initiatives that support the participation of women, youth, persons with disabilities, and rural communities. This language is consistent with provisions on cooperation towards digital in the DEPA, which explicitly reference vulnerable or underrepresented groups.[93]

(8) Subparagraph 2(f) encourages joint participation in regional and multilateral forums, recognizing the importance of shaping global digital trade norms through coordinated engagement. This aspect of cooperation is aligned with digital diplomacy provisions in several digital agreements, which calls for joint positions in international standard-setting bodies and digital governance dialogues.[94]

[91] CPTPP, Chapter 14, Article 15(b).
[92] EU-New Zealand FTA, Chapter 12, Article 14(1)(d); AfCFTA Digital Trade Protocol, Article 43(n).
[93] DEPA, Module 11, Article 1(3).
[94] EU-JAPAN EPA, Chapter 8, Article 80(1); EU-New Zealand FTA, Chapter 12, Article 14(3); EU-Mexico Global Agreement, Chapter 16, Article 11(2); CETA, Chapter 16, Article 6(3); CPTPP, Chapter 14, Article 15(d); RCEP, Chapter 14, Article 4(1)(e); Australia-Singapore DEA, Article 33(e); USMCA, Chapter 19, Article 14(1)(c).

(9) Paragraph 3 encourages the participation of non-governmental stakeholders—namely, the private sector, academia, civil society, and technical bodies—in cooperation activities. While not binding, this provision reflects the multistakeholder nature of digital governance and the importance of leveraging expertise beyond government institutions.

(10) In sum, this provision establishes a broad yet flexible cooperation framework, structured around shared digital economy priorities. While most obligations are non-binding, the language used encourages practical engagement and reflects widely accepted international practices. The emphasis on pilot programs, standards interoperability, SME support, and digital inclusion highlight the multidimensional nature of digital trade cooperation. The provision's design supports both regulatory alignment and institutional capacity-building, enabling the Parties to progressively implement the Agreement while remaining responsive to technological change and policy innovation.

DISPUTE SETTLEMENT

Context and Scope

(1) Dispute settlement provisions in digital trade agreements establish a mechanism for resolving disagreements between Parties concerning the interpretation, application, or implementation of the agreement's provisions. The scope of dispute settlement provisions in digital trade agreements typically covers state-to-state disputes and is limited to matters addressed within the agreement. Common features include consultation procedures, timelines for engaging in good faith negotiations, and in some cases, recourse to mediation, good offices, or even adjudication by a panel or tribunal.

(2) The main advantage of having dispute settlement provisions in digital trade agreements lies in the predictability and trust they provide. They reinforce treaty parties' expectation that commitments will be upheld and provide recourse in the event of inconsistent implementation or application. On the other hand, overly rigid or legalistic mechanisms may discourage participation or strain diplomatic relations, especially when differences arise from legitimate regulatory concerns rather than bad faith behavior. Therefore, striking a balance between enforceability and flexibility is key, especially in areas involving public policy exceptions, cybersecurity, or data protection, where national sovereignty is particularly sensitive.

Article 19 – Dispute Settlement

1. The Parties shall at all times endeavor to agree on the interpretation and application of this Agreement, and shall make every attempt through cooperation and consultations to arrive at a mutually satisfactory resolution of any matter that might affect its operation or application.

2. This Article shall apply to any dispute between the Parties concerning the interpretation, application, or a Party's failure to carry out its obligations under this Agreement.

3. Cooperation and Consultations:

a. a Party may request consultations with another Party with respect to any matter covered by this Agreement.

b. The requesting Party shall submit a written request to the other Party, specifying the measure at issue and the legal basis for its complaint.

c. The requested Party shall respond to the request within thirty (30) days of its receipt and shall enter into consultations in good faith within sixty (60) days of the date of the request.

d. The Parties shall make every effort to resolve the dispute through these consultations, including through the exchange of information and best practices.

4. Use of Good Offices:

a. If the Parties fail to resolve the dispute through consultations within sixty (60) days of the date of the request, either Party may request the good offices of a mutually agreed-upon party.

b. The purpose of good offices is to assist the Parties in resuming direct negotiations or to find a mutually acceptable method of pacific settlement.

c. The good offices process is voluntary and shall be undertaken only with the consent of both disputing Parties.

d. The proceedings and any information shared during the good offices shall be strictly confidential and without prejudice to the rights of either Party in any future proceedings.

5. If the matter has not been resolved within 90 days of receipt of the request for consultations (or such other period as the Parties may agree), the Parties may submit the dispute to arbitration in writing. The forum, procedural rules, place (seat) of arbitration, language, and the method of appointment of arbitrators shall be agreed by the Parties in writing for the purposes of that dispute.

6. An arbitral award rendered pursuant to paragraph 19.5 shall be final and binding on the Parties to the arbitration. The award shall set out the tribunal's findings of fact, its determinations on the issues in dispute, and the reasons for its determinations. Unless the Parties agree otherwise, each Party shall bear its own costs, and the costs of the tribunal shall be shared equally.

Commentary

(3) This provision establishes a tieredframework for dispute avoidance and resolution between the Parties, emphasizing cooperation, consultations, the use of good offices, and where the Parties so agree, allows for recourse to ad hoc arbitration. It reflects a preference for diplomatic and non-adversarial means to manage potential disagreements regarding the interpretation, application, or implementation of the Agreement. The provision outlines both procedural and substantive obligations, some of which are binding, while others are framed in non-binding or voluntary terms, such as the use of good offices.

(4) Paragraph 1 establishes a general and ongoing obligation for the Parties to agree on the interpretation and application of the Agreement and to use cooperation and consultation to resolve any issue affecting its operation. The language "shall at all times endeavor" introduces a binding procedural obligation but leaves substantive flexibility through its soft law formulation. This clause highlights the primacy of amicable, negotiated outcomes and mirrors similar provisions found in the DEPA and the CPTPP, which frame dispute avoidance as a continuous effort rather than a formal step triggered only upon a disagreement.[95] The obligation to "make every attempt" further signals a high standard of effort required, though not enforceable through adjudicative means.

(5) Paragraph 2 clarifies the scope of the Article by stating its applicability to all disputes concerning the interpretation, application, or failure to carry out obligations under the Agreement. This clause is binding and procedural in nature, identifying the types of issues that may give rise to a dispute and ensuring that both Parties understand the reach of the consultation and cooperation framework. The inclusion of "a Party's failure to carry out its obligations" broadens the scope beyond interpretative disagreements, encompassing issues of compliance. This formulation is in line with comparable clauses in the USMCA and the CPTPP, where a similar breadth is provided to capture both implementation and interpretation issues.[96]

(6) Paragraph 3 outlines the procedures for consultations. Subparagraph 3(a) provides that a Party may request consultations with another Party on any matter covered by the Agreement. The permissive "may" indicates a right, rather than an obligation, to initiate consultations. Subparagraph 3(b) introduces a more binding formulation, requiring the requesting Party to submit a written request that specifies both the measure at issue and the legal basis of the complaint. This procedural requirement ensures clarity and facilitates structured engagement. The formulation mirrors the language in the CPTPP and the EU–Japan EPA, which also require such detail in consultation requests.[97]

---

[95] CPTPP, Chapter 28, Article 18; DEPA, Module 14, Article 2(1); See also: Jordan-Singapore FTA, Chapter 7, Article 2(1); US-Oman FTA, Chapter 20, Article 1; US-Bahrain FTA, Chapter 19, Article 1; US-Jordan FTA, Article 16(1); US-Morocco FTA, Chapter 20, Article 2; USMCA, Chapter 31, Article 1.
[97] CPTPP, Chapter 28; article 3; USMCA, Chapter 31, Article 2. See also: EU-Chile framework Agreement, Chapter 38, Article 2; GCC-Singapore, Chapter 9, Article 1(2); Jordan-Canada FTA, Chapter 14, Article 2(1); US-Oman FTA, Chapter 20, Article 2; US-Bahrain FTA, Chapter 19, Article 2; DEPA; Module 14, Article 3; RCEP, Chapter 19, Article 3(1).

(7) Subparagraph 3(c) introduces explicit timeframes, requiring the requested Party to respond within thirty (30) days of receipt and to enter into consultations in good faith within sixty (60) days. These timelines introduce a binding procedural obligation and aim to avoid unnecessary delays, thus supporting the timely resolution of disputes. The obligation to consult "in good faith" aligns with general principles of international dispute settlement and appears in similar terms in the WTO Dispute Settlement Understanding (DSU).[98] Subparagraph 3(d) encourages the Parties to use consultations to exchange information and best practices to resolve the dispute. While this clause is non-binding in nature, it reinforces the provision's overall emphasis on cooperative mechanisms.

(8) Paragraph 4 introduces the use of good offices as a voluntary mechanism in the event that consultations do not yield a resolution within sixty (60) days. Subparagraph 4(a) permits either Party to request the good offices of a mutually agreed-upon third party. The discretionary "may" and the requirement for mutual agreement preserve the voluntary nature of the mechanism. Subparagraph 4(b) explains the purpose of good offices, namely to assist the Parties in resuming direct negotiations or finding alternative, mutually acceptable methods of pacific settlement.

(9) Subparagraph 4(c) emphasizes that good offices proceedings are undertaken only with the consent of both Parties, further confirming the voluntary and non-binding nature of this mechanism. Subparagraph 4(d) provides that the proceedings and any information exchanged during good offices shall be confidential and without prejudice to future proceedings. This clause safeguards the integrity of diplomatic efforts and is common in international dispute settlement processes, appearing in several agreements.[99]

(10) Paragraph 5 adds an optional adjudicative layer for dispute settlement by allowing the Parties, if a matter remains unresolved after 90 days from the consultation request (or any other period they agree), to submit the dispute to arbitration. The use of "may" confirms that arbitration is not automatic; it is available only where both Parties consent. Rather than prescribing a permanent forum or fixed rules, the paragraph requires the Parties to agree in writing on the forum, procedural rules, seat, language and method of appointment of arbitrators for each dispute. This design preserves a high degree of Party autonomy and flexibility while ensuring that, once agreed, arbitration proceeds on a clearly defined procedural basis. It also means that the effectiveness of this layer ultimately depends on continued cooperation, even at the stage of potential adjudication.

[98] DSU, Article 4(3)

[99] See example: USMCA, Chapter 31, Article 5(7); DEPA; Module 14, Article 4(2); GCC-Singapore FTA, Chapter 9, Article 3(3); RCEP, Chapter 19, Article 7(3).

[98] CPTPP, Chapter 28, Article 5(1); EU-Japan EPA, Chapter 21, Article 5(2). See also: GCC-Singapore FTA, Chapter 9, Article 2(2); RCEP, Chapter 19, Article 6(1) and (2); USMCA, Chapter 31, Article 4(1) and (2).

(11) Paragraph 6 governs the legal effect and minimum content of an arbitral award rendered pursuant to paragraph 5. By stipulating that an award is "final and binding" on the Parties, the provision reflects core principles of state-to-state arbitration and provides certainty once the Parties have chosen this route. The requirement for the award to set out findings of fact, determinations on the issues in dispute, and reasons enhances transparency and procedural fairness and is consistent with recognised arbitral practice. The default rule on costs, each Party bears its own costs and the costs of the tribunal are shared equally, unless the Parties agree otherwise, further maintains the neutral character of the mechanism and avoids deterring recourse to arbitration through uncertainty on cost allocation.

(12) Taken together, these paragraphs articulate a flexible but structured sequence of tools for managing disputes. The Article prioritises cooperative means, consultations and good offices, yet recognises that in some cases the Parties may wish to obtain a binding, reasoned decision through arbitration. Importantly, the Agreement does not establish a standing or compulsory adjudicative body: recourse to arbitration is optional and contingent on mutual consent and agreement on procedures. This combination of soft-law instruments with the possibility of ad hoc, binding resolution is particularly suited to the evolving nature of digital trade.

TRANSPARENCY

Context and Scope

(1) Transparency provisions in digital trade agreements are central to ensuring predictability, trust, and accountability in the regulatory environment that governs digital commerce. They refer primarily to the publication and accessibility of laws, regulations, administrative rulings, and procedures that affect digital transactions, services, and products. They also often include mechanisms for prior notice and public consultation, allowing stakeholders to be informed of, and contribute to, the rulemaking process. These provisions are particularly important in fast-moving digital sectors, where regulatory changes can have significant impacts on cross-border business operations.

(2) The scope of transparency commitments varies across digital trade agreements but generally includes three key components: the obligation to publish or otherwise make publicly available laws and regulations of general application; when possible, the publication of draft regulations in advance of their adoption; and the provision of reasonable opportunities for interested persons to submit comments. By promoting openness in the regulatory process, transparency provisions aim to reduce uncertainty and non-tariff barriers that may arise from opaque or inconsistent rulemaking. They benefit businesses, especially SMEs, that need to understand the legal environment to ensure compliance and plan their operations. For governments, these provisions foster better policy outcomes by facilitating stakeholder input and enhancing regulatory legitimacy.

Article 20 – Transparency

1. Each Party shall promptly publish, or otherwise make publicly available, its laws, regulations, procedures, and administrative rulings of general application relating to matters covered by this Agreement, in a manner that enables interested persons and other Parties to become acquainted with them.

2. When possible, a Party shall:

- **a. publish in advance proposed measures of general application; and**
- **b. provide a reasonable opportunity for interested persons to comment.**

Commentary

(3) This provision establishes transparency obligations in relation to the publication and accessibility of domestic legal and regulatory instruments relevant to the implementation and operation of the Agreement. It aims to ensure that Parties and stakeholders have timely access to applicable rules, and where feasible, are able to participate in regulatory processes. Transparency is a foundational principle in trade governance, and provisions of this nature are common across both WTO disciplines and digital trade agreements. The obligation to publish laws and provide avenues for comment supports legal certainty and accountability, which are particularly important in rapidly evolving digital markets. This structure combines binding and non-binding commitments, providing a baseline for transparency, while allowing for flexibility in domestic regulatory practices.

(4) Paragraph 1 sets out a binding obligation on each Party to "promptly publish or otherwise make publicly available" relevant legal and regulatory instruments. The scope of this obligation covers laws, regulations, procedures, and administrative rulings of general application that relate to matters falling within the scope of the MDEA. The language "shall" indicates a mandatory commitment, and the inclusion of "in a manner that enables interested persons and other Parties to become acquainted with them" emphasizes the accessibility and usability of the information. This mirrors the language adopted in the CPTPP and the DEPA, which contain similarly worded binding transparency requirements.[100] The obligation also echoes Article X of the GATT and Article III of the GATS, which enshrine the principle of transparency in the multilateral trade framework.[101] By mandating public availability, the provision seeks to reduce informational asymmetries and promote predictability in digital trade environments.

(5) Paragraph 2 introduces a softer, non-binding commitment. The use of "when possible" and "shall" implies that this obligation is binding to the extent of the feasibility within each Party's domestic legal and administrative context. Subparagraph 2(a) encourages the advance publication of proposed measures of general application. This practice is considered a best practice in regulatory governance, allowing stakeholders to anticipate changes and prepare accordingly. It is reflected in numerous trade agreements, including the CPTPP, and the USMCA, both of which encourage prior publication and public notice.[102]

[100] CPTPP, Chapter 26, Article 2(1); DEPA, Module 13, Article 2(1). See also: EU-Japan EPA, Chapter 17, Article 3(a); EU-New Zealand FTA, Chapter 23, Article 3(1); EU-UK TCA, Article 335(1); EU-Singapore FTA, Chapter 13, Article 3(1)(a); EU-Vietnam FTA, Chapter 14, Article 3(1)(a); Jordan-Canada FTA, Chapter 14, Article 1(1); US-Morocco FTA, Chapter 18, Article 1(1); AfCFTA Digital Trade Protocol, Article 38(1); Australia-Singapore DEA, Article 14(2); RCEP, Chapter 12, Article 12(1); USMCA, Chapter 29, Article 2(1).

[101] GATT, Article X(1); GATS, Article III(1) and (2).

[102] CPTPP, Chapter 26, Article 2(2)(a); USMCA, Chapter 29, Article 2(2)(a); See also: EU-Singapore FTA, Chapter 13, Article 3(2)(a); EU-Vietnam FTA, Chapter 14, Article 3(2)(a); Jordan-Canada FTA, Chapter 12, Article 1(2)(a); US-Morocco FTA, Chapter 18, Article 1(2)(a); Australia-Singapore DEA, Article 14(4)(a); DEPA, Module 13, Article 2(2)(a);

(6) Subparagraph 2(b) complements the previous clause by recommending that Parties provide a reasonable opportunity for interested persons to submit comments on proposed measures. This reflects a participatory model of rulemaking that is increasingly prevalent in modern trade and digital agreements. Provisions encouraging public consultation can be found in the DEPA, the EU-Singapore Digital Partnership, and the Australia-Singapore DEA.[103] While not binding, these clauses reinforce the broader objective of inclusive and transparent regulatory development, particularly where regulatory changes may have cross-border effects or impact digital trade flows.

(7) Taken together, this provision reflects a layered approach to transparency, combining a firm obligation to publish applicable rules with encouragement to incorporate participatory elements in the legislative or regulatory process. The binding nature of paragraph 1 ensures a minimum level of legal transparency, while paragraph 2 incentivizes regulatory openness and stakeholder engagement. This structure supports not only compliance with the Agreement but also broader principles of good governance and trust in digital trade systems. It aligns with international best practices without constraining the institutional autonomy of Parties, making it a practical and adaptable transparency standard for a digital trade context.

[103] DEPA; Module 13, Article 2(2)(b); EU-Singapore FTA, Chapter 113, Article 3(2)(b); Australia-Singapore DEA, Article 14(4)(b). See also: EU-Vietnam FTA, Chapter 14, Article 3(2)(b); Jordan-Canada FTA, Chapter 12, Article 1(2)(b); US-Morocco FTA, Chapter 18, Article 1(2)(b); CPTPP, Chapter 26, Article 2(2)(b).

TECHNICAL ASSISTANCE AND CAPACITY BUILDING

Context and Scope

(1) Technical assistance and capacity building (TACB) provisions in digital trade agreements serve as vital tools to ensure inclusive participation in the digital economy, particularly for developing and least-developed countries. These provisions are grounded in the recognition that disparities in digital infrastructure, regulatory capabilities, and human capital can prevent some economies from fully benefitting from digital trade opportunities. As such, TACB commitments are designed to narrow digital divides by supporting the development and implementation of legal frameworks, digital infrastructure, and institutional capabilities necessary to comply with and take advantage of digital trade disciplines.

(2) The scope of TACB provisions typically includes a wide range of cooperative activities such as: training and upskilling of government officials in areas like data governance, cybersecurity, and electronic commerce regulation; support for building secure and interoperable digital public infrastructure (e.g., digital ID systems or e-payment platforms); capacity-building for small and medium-sized enterprises (SMEs); and assistance with the development of inclusive policies targeting women, youth, and underrepresented communities. TACB provisions help operationalize the principles of inclusivity and shared benefit that underpin many digital economy frameworks. By strengthening the regulatory and institutional readiness of participating countries, these provisions help ensure that commitments made under digital trade agreements are not just formal obligations but deliver meaningful, widespread benefits across all economies involved.

Article 21 – Technical Assistance and Capacity Building

1. The Parties recognize that technical assistance and capacity building support effective implementation of this Agreement and help narrow digital divides.

2. Subject to the availability of resources and on mutually agreed terms, cooperation may include:

- **a. training for officials and regulators on digital trade, data governance, cybersecurity, and competition in digital markets;**
- **b. support for interoperable digital public infrastructure and secure networks;**

c. SME digitalization programs, including e-payments, digital IDs, and logistics solutions;

d. initiatives that advance digital skills and literacy for under-represented groups;

e. joint research, pilots, and testbeds with the private sector and technical bodies.

3. The Parties shall coordinate assistance and may mobilize a DCO MDEA Implementation Facility under the discipline of the Digital Space Accelerators (DSA) to match priority needs with funding and expertise.

Commentary

(3) This provision addresses the importance of technical assistance and capacity building in the effective implementation of the Agreement, especially for narrowing digital divides between and within Parties. It reflects a recognition that commitments in digital trade are only meaningful if Parties—particularly those with less developed digital infrastructure or regulatory frameworks—have the resources and institutional capacity to comply. The provision combines a non-binding recognition of shared goals with more structured, albeit still discretionary, avenues for cooperation. It draws from a growing body of digital economy agreements that embed implementation support mechanisms, such as the CPTPP and the AfCFTA Protocol on Digital Trade, which both emphasize capacity building as a key component of equitable digital integration.[104]

(4) Paragraph 1 opens with a policy-level acknowledgment of the role of technical assistance and capacity building in the success of the Agreement and in bridging digital divides. The use of "recognize" signifies a non-binding expression of shared understanding rather than a firm legal obligation. This clause sets the normative foundation for the cooperation measures outlined in the following paragraphs. Similar language appears in the CPTPP and the DEPA, both of which recognize the role of cooperation in supporting digital trade readiness and inclusivity.[105]

(5) Paragraph 2 outlines the potential areas of cooperation that may be pursued by the Parties, subject to the availability of resources and mutual agreement. This caveat frames the entire paragraph as non-binding and conditional, allowing Parties to tailor engagement based on capacities and interests. Subparagraph 2(a) identifies training for officials and regulators in key domains of digital trade—data governance, cybersecurity, and digital market competition. This reflects a common practice in recent agreements, such as in the CPTPP, where regulatory knowledge exchange and institutional strengthening are explicitly encouraged to promote convergence and preparedness.[106]

[104] CPTPP, Chapter 21, Article 1(1) and 2; AfCFTA Digital Trade Protocol, Article 42(1) and 43.
[105] CPTPP, Chapter 21, Article 1(1); RCEP, Chapter 13, Article 6; WTO TFA, Article 21(1).
[106] CPTPP, Chapter 21, Article 2.

A core feature of TACB provisions is their flexibility and non-binding nature. Most agreements phrase these commitments using terms such as "shall endeavor" or "subject to the availability of resources," which allows Parties to commit to cooperation without guaranteeing specific outcomes or financial contributions. This open-endedness can be both a strength, because it allows adaptation to national priorities, and a limitation if not followed up with concrete action or supported by mechanisms such as dedicated funding facilities, joint coordinating bodies, or public-private partnerships.

(6) Subparagraph 2(b) focuses on support for interoperable digital public infrastructure and secure networks. While not a binding commitment, this element signals an alignment with international discourse on the importance of secure and connected digital ecosystems (7) Subparagraph 2(c) targets digitalization programs for SMEs, including solutions such as e-payments, digital identity systems, and logistics platforms. The inclusion of SMEs mirrors common language in other FTAs and digital agreements, which recognize that smaller firms often lack the capacity to access digital trade opportunities without targeted support. This subparagraph highlight the intersection between trade facilitation and digital inclusion.

(8) Subparagraph 2(d) further expands the scope of cooperation to the promotion of digital skills and literacy, especially among underrepresented groups. This clause integrates a social inclusion dimension, reflecting global calls for gender-responsive and inclusive digital policy.

(9) Subparagraph 2(e) points to joint initiatives involving research, pilots, and testbeds in collaboration with private sector and technical bodies. This is particularly significant for innovation policy and public-private partnership frameworks, enabling experimental approaches to emerging technologies and regulatory sandboxes. Provisions of this nature can be found in DEPA's Annex on Emerging Technologies and in bilateral agreements such as the Australia-Singapore DEA, which promote testbeds and collaborative technology development.[107]

(10) Paragraph 3 introduces a semi-institutional mechanism to coordinate support efforts. The Parties commit to coordinating assistance and may mobilize a "DCO MDEA Implementation Facility" governed by the Digital Space Accelerators (DSA). While the "shall coordinate" language suggests a binding obligation to engage in coordination, the actual activation of the facility is discretionary ("may mobilize"). This hybrid approach allows for both structured dialogue and flexibility in operationalizing assistance. Although the mechanism is tailored to the DCO/MDEA context, it draws inspiration from institutional innovations in other agreements, such as DEPA's Joint Committee, which is similarly designed to align funding with priority needs.[108]

[107] DEPA, Module 8, Article 4; Australia-Singapore DEA, Article 16.
[108] DEPA, Module 12, Article 2 and 5.

(11) This provision reflects an advanced model of cooperation and implementation support, combining flexible instruments with a vision for inclusive digital transformation. While most of the obligations are non-binding and subject to mutual agreement and resource availability, the provision contributes meaningfully to the implementation architecture of the Agreement. It positions technical assistance not merely as a peripheral activity, but as a core enabler of digital trade outcomes—particularly for SMEs and underrepresented populations. The inclusion of a coordination facility also signals a commitment to structured engagement, allowing for donor-recipient matching and long-term policy planning. Overall, this provision demonstrates how modern digital trade agreements are evolving beyond rule-making to include delivery mechanisms aimed at bridging capacity gaps and achieving shared digital prosperity.

STRATEGIC GUIDE TO DIGITAL ECONOMY AGREEMENTS

DIGITAL ECONOMY TAXATION AND CUSTOMS DUTIES

International Trends

Digital trade agreements often cover customs duties on electronic transmissions, rather than the taxation of the digital economy or other customs duties. The provisions follow two models. One model prohibits such customs duties, although different specifications thereon have emerged in international commitments worldwide. The other model recognises electronic transmissions as the provision of services which cannot be subject to customs duties.

The first model contains a core commitment that no party "shall" impose customs duties on electronic transmissions, including content transmitted electronically, from one party to the other. The following specifications have been added in certain agreements:

- Taxation: The commitment does not prevent parties from imposing internal taxes, fees or other charges on content transmitted electronically.
- Definitions: "Electronic transmission" are transmissions made using any electromagnetic means and including the content of the transmission. "Customs duties" include import and export duties.
- Prejudice: The commitment is without prejudice to parties' position on whether deliveries by electronic means should be categorised as trade in services or goods

In addition, several agreements have connected this commitment to other international fora. Certain provisions require parties to cooperate in relevant international fora to promote the adoption of commitments by non-parties not to impose customs duties on electronic transmissions. Other provisions are more specific and highlight international negotiations under the World Trade Organization.[109] Specifically, these provisions note that parties may adjust their customs regimes to outcomes in the WTO Ministerial Decisions on customs duties on electronic transmissions within the framework of the Work Programme on Electronic Commerce. *Example: China-New Zealand Free Trade Agreement Upgrade - Article 4.*

In the second model, parties agree that electronic transmissions shall be considered as the provision of services. Then, the provisions state that such transmissions cannot be subject to customs duties. *Example: United Kingdom-Georgia Strategic Partnership and Cooperation Agreement - Article 121.*

[109] Specifically, the WTO Ministerial Decision of 13 December 2017 in relation to the Work Programme on Electronic Commerce (WT/MIN(17)/65).

DCO Members Approaches

The DCO Member States are involved in several agreements that follow the first model, namely the:

- African Continental Free Trade Agreement Digital Trade Protocol
- Canada-Jordan Free Trade Agreement
- EU-Canada Comprehensive Economic and Trade Agreement
- EU-Chile Advanced Framework Agreement
- EU-Japan Economic Partnership Agreement
- EU-New Zealand Free Trade Agreement
- EU-Mexico Trade Agreement
- EU-Singapore Free Trade Agreement
- EU-Vietnam Free Trade Agreement
- GCC-Singapore Free Trade Agreement
- Singapore-Jordan Free Trade Agreement
- United States-Bahrain Free Trade Agreement
- United States-Jordan Free Trade Agreement
- United States-Oman Free Trade Agreement
- United States-Morocco Free Trade Agreement
- WTO Agreement on Electronic Commerce

The second model, on the other hand, is used in the EU-United Kingdom Trade and Cooperation Agreement.

Conclusion

Digital trade agreements generally require parties not to impose customs duties on electronic transmissions. The provisions all follow the same model, prohibiting such customs duties, although different specifications, for example regarding definitions and relevant international fora, are enshrined in international commitments worldwide.

At the international level, the DCO Member States are involved in several agreements covering customs duties, relying on one model with one exception. By participating in the DCO, Member States can exchange insights, leading to more robust conversations and revealing opportunities for coordinated efforts.

Digital Trade Agreements with Commitments on Digital Economy Taxation and Custom Duties

DCO Members:

The DCO Member States are involved in the following agreements with provisions on digital economy taxation and customs duties:

- African Continental Free Trade Agreement Digital Trade Protocol - Article 6 - Customs Duties
- Canada-Jordan Free Trade Agreement - Article 3-1 - Customs Duties on Products Delivered by Electronic Means
- EU-Canada Comprehensive Economic and Trade Agreement (CETA) - Chapter 16, Article 16.3 - Customs Duties on Electronic Deliveries
- EU-Chile Advanced Framework Agreement - Chapter 19, Article 19.6 - Customs Duties on Electronic Transmissions
- EU-Japan Economic Partnership Agreement - Chapter 8 Section F, Article 8.72 - Customs Duties
- EU-Mexico Trade Agreement - Chapter 16, Article 3 - Customs Duties on Electronic Transmissions
- EU-New Zealand Free Trade Agreement - Chapter 12, Article 12.6 - Customs Duties on Electronic Transmissions
- EU-Singapore Free Trade Agreement - Chapter 8, Article 8.58 - Customs Duties
- EU-United Kingdom Trade and Cooperation Agreement - Title III, Article 203 - Customs Duties on Electronic Transmissions
- EU-Vietnam Free Trade Agreement - Article 8.51 - Customs Duties
- GCC-Singapore Free Trade Agreement - Article 7.4 - Digital Products
- Singapore-Jordan Free Trade Agreement - Chapter 5, Article 5.1 - Electronic Transmissions
- United States-Bahrain Free Trade Agreement - Article 13.3 - Customs Duties
- United States-Jordan Free Trade Agreement - Article 7 - Electronic Commerce
- United States-Morocco Free Trade Agreement - Article 14.3 - Digital Products
- United States-Oman Free Trade Agreement - Chapter 14, Article 14.3 - Digital Products
- WTO Agreement on Electronic Commerce - Article 11 - Customs Duties on Electronic Transmissions

Non-DCO Members:

The following agreements also contain provisions on digital economy taxation and customs duties:

- Australia-China Free Trade Agreement - Chapter 12, Article 12.3 - Customs Duties
- Australia-Chile Free Trade Agreement - Article 16.4 - Customs Duties
- Australia-Hong Kong Free Trade Agreement - Chapter 11, Article 11.6 - Customs Duties
- Australia-Indonesia Comprehensive Economic Partnership Agreement - Chapter 13, Article 13.3 - Customs Duties
- Australia-Singapore Digital Economy Agreement - Article 5 - Customs Duties
- Australia-Singapore Free Trade Agreement - Chapter 14, Article 4 - Customs Duties
- Australia-Thailand Free Trade Agreement - Chapter 11, Article 1102 - Customs Duties
- Australia-United Kingdom Free Trade Agreement - Chapter 14, Article 14.3 - Customs Duties
- Canada-Colombia Free Trade Agreement - Chapter 15, Article 1503 - Customs Duties
- Canada-Honduras Free Trade Agreement - Chapter 16, Article 16.3 - Customs Duties on Digital Products Transmitted Electronically
- Canada-Panama Free Trade Agreement - Article 15.04 - Customs Duties on Digital Products Delivered Electronically
- Canada-Peru Free Trade Agreement - Chapter 15, Article 1503 - Customs Duties
- China-Cambodia Free Trade Agreement - Chapter 10, Article 10.3 - Customs Duties
- China-Korea Free Trade Agreement - Chapter 13, Article 13.3 - Customs Duties
- China-Mauritius Free Trade Agreement - Chapter 11, Article 11.3 - Customs Duties
- China-New Zealand Free Trade Agreement Upgrade - Chapter 19, Article 4 - Customs Duties
- China-Singapore Free Trade Agreement Upgrade - Chapter 15, Article 5 - Customs Duties
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership - Chapter 14, Article 14.3 - Customs Duties
- Digital Economy Partnership Agreement - Article 1 - Customs Duties
- Dominican Republic-Central America-United States Free Trade Agreement Free Trade Agreement - Article 14.3 - Digital Products
- European Free Trade Association-Moldova Free Trade Agreement - Chapter 5, Article 5.5 - Customs Duties
- Iceland-Liechtenstein-Norway-United Kingdom Free Trade Agreement - Chapter 4, Article 4.4 - Customs Duties
- India-United Arab Emirates Comprehensive Economic Partnership Agreement - Chapter 9, Article 9.15 - Customs Duties
- Japan-Switzerland Free Trade Agreement - Chapter 8, Article 76 - Customs Duties
- Korea-Australia Free Trade Agreement - Chapter 15, Article 15.3 - Customs Duties

- Korea-Canada Free Trade Agreement - Chapter 13, Article 13.3 - Customs Duties
- Korea-Colombia Free Trade Agreement - Article 12.2 - Customs Duties
- Korea-Israel Free Trade Agreement - Chapter 13, Article 13.3 - Customs Duties
- Korea-Peru Free Trade Agreement - Chapter 14, Article 14.4 - Customs Duties
- Korea-Singapore Digital Partnership Agreement - Article 14.5 - Customs Duties
- Korea-Singapore Free Trade Agreement - Chapter 14, Article 14.4 - Digital Products
- Korea-Vietnam Free Trade Agreement - Chapter 10, Article 10.2 - Customs Duties
- Peru-Australia Free Trade Agreement - Chapter 13, Article 13.3 - Customs Duties
- Regional Comprehensive Economic Partnership - Chapter 12, Article 12.11 - Customs Duties
- Singapore-Costa Rica Free Trade Agreement - Article 12.4 - Digital Products
- Singapore-New Zealand Closer Economic Partnership Upgrade - Chapter 9, Article 9.3 - Customs Duties
- Singapore-Panama Free Trade Agreement - Chapter 13, Article 13.3 - Digital Products
- Singapore-Sri Lanka Free Trade Agreement - Chapter 9, Article 9.3 - Customs Duties
- Singapore-Taiwan Economic Partnership Agreement - Chapter 11, Article 11.3 - Customs Duties and Internal Taxes
- Singapore-Turkey Free Trade Agreement - Chapter 9, Article 9.3 - Customs Duties
- United Kingdom-Japan Comprehensive Economic Partnership Agreement - Chapter 8, Section F, Article 8.72 - Customs Duties
- United Kingdom-Korea Free Trade Agreement - Chapter 7, Article 7.48 - Objective and Principles
- United Kingdom-New Zealand Free Trade Agreement - Chapter 15, Article 15.4 - Customs Duties
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-B - Customs Duties
- United Kingdom-Singapore Digital Economy Agreement - Article 8.59 - Customs Duties
- United States-Mexico-Canada Agreement - Chapter 19, Article 19.3 - Customs Duties
- United States-Chile Free Trade Agreement - Article 15.3 - Customs Duties on Digital Products
- United States-Colombia Free Trade Agreement - Chapter 15, Article 15.3 - Digital Products
- United States-Japan Digital Trade Agreement - Article 7 - Customs Duties
- United States-Korea Free Trade Agreement - Article 15.3 - Digital Products
- United States-Panama Trade Promotion Agreement - Chapter 14, Article 14.3 - Digital Products
- United States-Peru Trade Promotion Agreement - Article 15.3 - Digital Products

ELECTRONIC TRANSACTIONS AND ELECTRONIC AUTHENTICATION AND SIGNATURES

International Trends

Provisions on electronic transactions are common in digital trade agreements. We distinguish provisions on electronic transactions frameworks in general and provisions on electronic authentication and signatures.[110]

Provisions on electronic transactions frameworks follow three models, multiple of which can be found in the same agreement: non-binding provisions, mixed provisions, and dedicated provisions on the conclusion of electronic contracts.

- In non-binding provisions, parties endeavor to adopt or maintain domestic rules governing electronic transactions, sometimes referencing international frameworks such as UNCITRAL Model Laws. *Example: Korea-Vietnam Free Trade Agreement*
- In the mixed model, parties bindingly commit to ("shall") adopting or maintaining such a framework, again following international models. In addition, parties endeavour to avoid unnecessary regulatory burdens on electronic transactions and to facilitate input in the development of their frameworks. Rarely, agreements turn this endeavour into a commitment. In addition, some contain delaying language ("as soon as practicable") and references to applicable guidelines, agreements and model laws related to electronic commerce. *Example: Australia-Singapore Free Trade Agreement*
- Dedicated articles on electronic contracts commit parties not to deny the legal effect, validity, or enforceability of an electronic contract solely on the basis that it has been made by electronic means. Some provisions include exceptions, for instance regarding contracts concerning real estate or governed by family law, or when a party's laws and regulations provide otherwise. Some provisions further specify that the electronic transaction framework shall not create obstacles for the use of electronic contracts. Finally, certain provisions commit parties not to require prior authorization for the provision of a service by electronic means, with exceptions for telecommunications services, among others. Singular agreements use endeavour language regarding this absence of prior authorization. *Example: EU-Mexico Trade Agreement*

110 Note that this analysis focuses on dedicated provisions, disregarding general provisions on cooperation that touch upon electronic transactions as a regulatory issue in digital trade or provisions on digital identities.

Provisions on electronic authentication follow three models: non-binding provisions, prohibitive binding provisions, and prescriptive binding provisions.

- Non-binding provisions are relatively rare. In certain non-binding provisions, parties commit to work towards mutual recognition of electronic authentication methods and to collaborate and share best practices. In others, parties commit to establishing cooperation mechanisms between national accreditation and digital certification authorities and to work towards the mutual recognition of digital certificates. Finally, some non-binding provisions use "endeavour" language to the typical formulation for a prohibitive binding provision (see below). *Example: China-Eurasian Economic Union Free Trade Agreement*
- Prohibitive binding provisions prohibit parties from adopting or maintaining legislation for electronic authentication that a) prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods, or b) prevent parties from establishing that their electronic transaction complies with any legal requirements on authentication before authorities, or c) limit the recognition of authentication technology, methods, and implementation models. Notably, certain provisions include exceptions, for circumstances otherwise provided for under parties' laws, or for particular categories of transactions. In turn, some provisions limit these exceptions, by requiring them to serve a legitimate governmental objective and to be substantially related to achieving said objective. Furthermore, certain provisions add an encouragement for the use of interoperable electronic authentication and mutual recognition of electronic signatures, as well as an extension of the commitment to electronic seals, electronic time stamps, or electronic registered delivery services. *Example: United States-Peru Trade Promotion Agreement*
- Prescriptive binding provisions contain the same core commitments as the prohibitive binding provisions, albeit with an inverted formulation: They require parties to adopt frameworks that permit, rather than prohibiting frameworks that prohibit, the abovementioned use cases for electronic authentication. Another type of prescriptive binding provision focuses on electronic signatures. It requires parties to take steps to facilitate understanding of respective electronic signatures frameworks and to examine mutual recognition. *Examples: China-New Zealand Free Trade Agreement Upgrade.*

DCO Members Approaches

Regarding electronic transactions, the DCO Member States are involved in several agreements with dedicated provisions:

- The EU-Chile Advanced Framework Agreement, the EU-Japan Economic Partnership Agreement, the EU-Mexico Trade Agreement, the EU-New Zealand Free Trade Agreement, and the EU-United Kingdom Trade and Cooperation Agreement use the model of dedicated articles on electronic contracts. They each dedicate an article to the conclusion of contracts by electronic means and to the absence of prior authorization.
- The WTO Agreement on Electronic Commerce contains a dedicated provision on electronic contracts, as outlined above, and a provision that follows the non-binding model (consistently using "endeavour" language to cover the content typical to a mixed provision).
- The African Continental Free Trade Agreement Digital Trade Protocol contains a dedicated provision on electronic contracts and a special provision that follows the mixed model but uses binding language throughout.
- Regarding electronic authentication, the DCO Member States are involved in several agreements with dedicated provisions:
- The EU-Chile Advanced Framework Agreement, the EU-New Zealand Free Trade Agreement, the EU-Mexico Trade Agreement, and the EU-United Kingdom Trade and Cooperation Agreement use the prohibitive binding model.
- The EU-Singapore Free Trade Agreement follows the prescriptive binding model, dedicating a provision to electronic signatures.
- The WTO Agreement on Electronic Commerce follows the prohibitive binding model, as outlined above, with additional detail concerning definitions.
- The African Continental Free Trade Agreement Digital Trade Protocol contains dedicated articles on electronic trust services and electronic authentication, both following the prohibitive binding model. Notably, these provisions do not provide any exceptions.

Conclusion

Regarding electronic transactions, the DCO Member States are involved in several agreements with dedicated provisions:

- The EU-Chile Advanced Framework Agreement, the EU-Japan Economic Partnership Agreement, the EU-Mexico Trade Agreement, the EU-New Zealand Free Trade Agreement, and the EU-United Kingdom Trade and Cooperation Agreement use the model of dedicated articles on electronic contracts. They each dedicate an article to the conclusion of contracts by electronic means and to the absence of prior authorization.
- The WTO Agreement on Electronic Commerce contains a dedicated provision on electronic contracts, as outlined above, and a provision that follows the non-binding model (consistently using "endeavour" language to cover the content typical to a mixed provision).
- The African Continental Free Trade Agreement Digital Trade Protocol contains a dedicated provision on electronic contracts and a special provision that follows the mixed model but uses binding language throughout.

Regarding electronic authentication, the DCO Member States are involved in several agreements with dedicated provisions:

- The EU-Chile Advanced Framework Agreement, the EU-New Zealand Free Trade Agreement, the EU-Mexico Trade Agreement, and the EU-United Kingdom Trade and Cooperation Agreement use the prohibitive binding model.
- The EU-Singapore Free Trade Agreement follows the prescriptive binding model, dedicating a provision to electronic signatures.
- The WTO Agreement on Electronic Commerce follows the prohibitive binding model, as outlined above, with additional detail concerning definitions.
- The African Continental Free Trade Agreement Digital Trade Protocol contains dedicated articles on electronic trust services and electronic authentication, both following the prohibitive binding model. Notably, these provisions do not provide any exceptions.

Digital Trade Agreements with Commitments on Electronic Transactions and Signatures

DCO Members:

The DCO Member States are involved in the following agreements with provisions on electronic transactions and contracts in general:

- African Continental Free Trade Agreement Digital Trade Protocol - Article 16 - Domestic Electronic Transactions Framework - and Article 12 - Electronic Contracts
- EU-Chile Advanced Framework Agreement - Chapter 19 - Article 19.7 - No Prior Authorization - and Article 19.8 - Conclusion of Contracts by Electronic Means
- EU-Mexico Free Trade Agreement - Chapter 16 - Article 4 - Principle of no prior authorization - and Article 5 - Electronic Contracts
- EU-New Zealand Free Trade Agreement - Chapter 12 - Article 12.7 - No Prior Authorization - and Article 12.8 - Conclusion of Contracts by Electronic Means
- EU-United Kingdom Trade and Cooperation Agreement - Title III - Article 204 - No Prior Authorization - and Article 205 - Conclusion of Contracts by Electronic Means
- EU-Japan Economic Partnership Agreement - Chapter 8 Section F Article 8.75 - Principle of no prior authorization - and Article 8.76 Conclusion of Contracts by Electronic Means
- WTO Agreement on Electronic Commerce - Article 4 - Electronic Transactions Framework - and Article 6 - Electronic Contracts

The DCO Member States are involved in the following agreements with provisions on electronic authentication and signatures:

- African Continental Free Trade Agreement Digital Trade Protocol - Article 8 - Electronic Trust Services - and Article 9 - Electronic Authentication
- EU-Chile Advanced Framework Agreement - Article 19.9 - Electronic Trust Services and Electronic Authentication
- EU-Mexico Trade Agreement - Chapter 16, Article 6 - Electronic Trust and Authentication Services
- EU-New Zealand Free Trade Agreement - Article 12.9 - Electronic Authentication
- EU-Singapore Free Trade Agreement - Chapter 8, Article 8.60 - Electronic Signatures
- EU-United Kingdom Trade and Cooperation Agreement - Title III, Article 206 - Electronic Authentication and Electronic Trust Services
- WTO Agreement on Electronic Commerce - Article 5 - Electronic Authentication and Electronic Signatures

Non-DCO Members:

The following agreements also contain provisions on electronic transactions and contracts in general:

- ASEAN-Australia-New Zealand Free Trade Area - Chapter 10, Article 4 - Domestic Regulatory Frameworks
- ASEAN Agreement on Electronic Commerce - Article 12 - Domestic Regulatory Framework
- Australia-Hong Kong Free Trade Agreement - Chapter 11 - Article 11.4 - Electronic Transactions Framework
- Australia-Indonesia Comprehensive Economic Partnership Agreement - Chapter 13 - Article 13.9 - Domestic Regulatory Frameworks
- Australia-Singapore Digital Economy Agreement - Article 8 - Domestic Electronic Transactions Framework
- Australia-United Kingdom Free Trade Agreement - Chapter 14 - Article 14.4 - Domestic Electronic Transactions Framework
- Australia-United Kingdom Free Trade Agreement - Chapter 14 - Article 14.5 - Conclusion of Contracts by Electronic Means
- China-New Zealand Free Trade Agreement Upgrade - Chapter 19 - Article 6 - Domestic Regulatory Frameworks
- China-Singapore Free Trade Agreement Upgrade - Chapter 15 - Article 3 - Domestic Regulatory Frameworks
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership - Chapter 14 - Article 14.5 - Domestic Electronic Transactions Framework
- Digital Economy Partnership Agreement - Domestic Electronic Transactions Framework
- Iceland-Liechtenstein-Norway-United Kingdom Free Trade Agreement - Chapter 4 - Article 4.5 - Electronic Contracts
- India-United Arab Emirates Comprehensive Economic Partnership Agreement - Chapter 9 - Article 9.5 - Domestic Electronic Transactions Framework
- Korea-Singapore Digital Partnership Agreement - Article 14.7 - Domestic Electronic Transactions Framework
- Regional Comprehensive Economic Partnership - Chapter 12 - Article 12.10 - Domestic Regulatory Framework
- Singapore-Eurasian Economic Union Free Trade Agreement - Chapter 9 - Article 9.4 - Domestic Regulatory Framework
- Singapore-Sri Lanka Free Trade Agreement - Chapter 9 - Article 9.5 - Domestic Electronic Transactions Framework
- Singapore-Turkey Free Trade Agreement - Chapter 9 - Article 9.5 - Domestic Electronic Transactions Framework

- United Kingdom-Japan Comprehensive Economic Partnership Agreement - Chapter 8 Section F Article 8.75 - Principle of no prior authorization
- United Kingdom-New Zealand Free Trade Agreement - Chapter 15 - Article 15.5 - Conclusion of Contracts by Electronic Means
- United Kingdom-New Zealand Free Trade Agreement - Chapter 15 - Article 15.6 - Domestic Electronic Transactions Framework
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-C - Domestic Electronic Transactions Framework
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-D - Conclusion of Contracts by Electronic Means
- United Kingdom-Singapore Digital Economy Agreement - Article 8.60 - Domestic Electronic Transactions Framework and Electronic Contracts
- United States-Mexico-Canada Agreement - Chapter 19 - Article 19.5 - Domestic Electronic Transactions Framework
- United States-Japan Digital Trade Agreement - Article 9 - Domestic Electronic Transactions Framework

The following agreements also contain provisions on electronic authentication and signatures:

- ASEAN Agreement on Electronic Commerce - Article 7 - Facilitating Cross-Border E-Commerce (2. Electronic Authentication and Electronic Signatures)
- ASEAN-Australia-New Zealand Free Trade Area - Chapter 10, Article 5 - Electronic Authentication and Digital Certificates
- Australia-Chile Free Trade Agreement - Chapter 16, Article 16.6 - Electronic Authentication
- Australia-China Free Trade Agreement - Chapter 12, Article 12.6 - Electronic Authentication and Digital Certificates
- Australia-Hong Kong Free Trade Agreement - Chapter 11, Article 11.3 - Electronic Signatures and Electronic Authentication
- Australia-Indonesia Comprehensive Economic Partnership Agreement - Chapter 13, Article 13.5 - Electronic Authentication and Electronic Signatures
- Australia-Singapore Digital Economy Agreement - Article 9 - Electronic Authentication and Electronic Signatures
- Australia-Singapore Free Trade Agreement - Chapter 14, Article 7 - Electronic Authentication and Electronic Signatures
- Australia-Thailand Free Trade Agreement - Chapter 11, Article 1104 - Electronic Authentication and Digital Certificates
- Australia-United Kingdom Free Trade Agreement - Article 14.6 - Electronic Authentication and Electronic Trust Services
- China-Cambodia Free Trade Agreement - Chapter 10, Article 10.4 - Electronic

Authentication and Electronic Signatures

- China-Eurasian Economic Union Free Trade Agreement - Chapter 11, Article 11.3 - Electronic Authentication
- China-Korea Free Trade Agreement - Chapter 13, Article 13.4 - Electronic Authentication and Electronic Signatures
- China-Mauritius Free Trade Agreement - Article 11.5 - Electronic Authentication and Digital Certificates
- China-New Zealand Free Trade Agreement Upgrade - Article 7 - Electronic Authentication, Signature, and Digital Certificates
- China-Singapore Free Trade Agreement Upgrade - Chapter 15, Article 4 - Electronic Authentication and Electronic Signatures
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership - Article 14.6 - Electronic Authentication and Electronic Signatures
- European Free Trade Association-Moldova Free Trade Agreement - Article 5.6 - Electronic Authentication, Trust Services, and Contracts by Electronic Means
- Iceland-Liechtenstein-Norway-United Kingdom Free Trade Agreement - Article 4.6 - Electronic Authentication and Electronic Trust Services
- India-United Arab Emirates Comprehensive Economic Partnership Agreement - Chapter 9, Article 9.6 - Authentication
- Japan-Switzerland Free Trade Agreement - Chapter 8, Article 78 - Electronic Signatures and Certification Services
- Korea-Australia Free Trade Agreement - Chapter 15, Article 15.5 - Electronic Authentication and Electronic Signatures
- Korea-Israel Free Trade Agreement - Chapter 13, Article 13.5 - Electronic Authentication and Electronic Signatures
- Korea-Peru Free Trade Agreement - Chapter 14, Article 14.8 - Electronic Authentication and Digital Certificates
- Korea-Singapore Digital Partnership Agreement - Article 14.8 - Electronic Authentication and Electronic Signatures
- Korea-Vietnam Free Trade Agreement - Chapter 10, Article 10.3 - Electronic Authentication, Electronic Signatures, and Digital Certificates
- Peru-Australia Free Trade Agreement - Chapter 13, Article 13.6 - Electronic Authentication and Electronic Signatures
- Regional Comprehensive Economic Partnership - Article 12.6 - Electronic Authentication and Electronic Signature
- Singapore and the Separate Customs Territory of Taiwan on Economic Partnership - Chapter 11, Article 11.5 - Authentication and Electronic Signatures
- Singapore-Eurasian Economic Union Free Trade Agreement - Chapter 9, Article 9.5 - Electronic Signatures
- Singapore-New Zealand Closer Economic Partnership Upgrade - Chapter 9, Article 9.5 - Electronic Authentication and Electronic Signatures

- Singapore-Sri Lanka Free Trade Agreement - Chapter 9, Article 9.6 - Electronic Authentication and Electronic Signatures
- Singapore-Turkey Free Trade Agreement - Chapter 9, Article 9.6 - Electronic Authentication and Electronic Signatures
- United Kingdom-Japan Comprehensive Economic Partnership Agreement - Chapter 8, Article 8.77 - Electronic Authentication and Electronic Signatures
- United Kingdom-New Zealand Free Trade Agreement - Article 15.7 - Electronic Authentication
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-E - Electronic Authentication and Electronic Trust Services
- United Kingdom-Singapore Digital Economy Agreement - Article 8.61 - Electronic Authentication
- United States-Mexico-Canada Agreement - Article 19.6 - Electronic Authentication and Electronic Signatures
- United States-Colombia Free Trade Agreement - Article 15.6 - Authentication
- United States-Japan Digital Trade Agreement - Article 10 - Electronic Authentication and Electronic Signatures
- United States-Korea Free Trade Agreement - Chapter 15, Article 15.4 - Electronic Authentication and Electronic Signatures
- United States-Peru Trade Promotion Agreement - Chapter 15, Article 15.6 - Authentication

ELECTRONIC PAYMENTS

International Trends

Electronic payments provisions in digital trade agreements are rare and not to be conflated with electronic invoicing provisions. We distinguish between three models: non-binding provisions, binding provisions, and detailed binding provisions.

Non-binding provisions establish basic principles in which Member States "recognise" the importance of safe, secure, and efficient e-payment systems. The provisions explicitly acknowledge varying levels of readiness in terms of capacity, infrastructure, and regulation. They state that Member States "shall encourage" the use of such systems in accordance with domestic laws and regulations, without specifying implementation requirements. *Example: ASEAN Agreement on Electronic Commerce.*

Binding provisions establish commitments to support the development of efficient, safe, and secure cross-border electronic payments through three core objectives: fostering internationally accepted standards, promoting interoperability, and encouraging innovation and competition. The provisions then require parties to apply several, but not always all, of the following mechanisms:

- make regulations publicly available; and/or
- endeavour to finalize approvals in a timely manner; and/or
- prevent discrimination between financial and non-financial institutions regarding infrastructure access; and/or
- adopt international standards for electronic payment messaging and data exchange; and/or
- facilitate the use of open platforms and architectures through Application Programming Interfaces; and/or
- facilitate innovation and competition and the introduction of new financial and electronic payment products; and/or
- promote the interoperability of digital electronic payment infrastructures; and/or
- enable cross-border authentication mechanisms and electronic know-your-customer verifications. *Example: Australia-Singapore Digital Economy Agreement.*

Detailed binding provisions build on these commitments and additionally provide precise definitions and binding language. They define "electronic payment" and "self-regulatory organization" before establishing specific obligations. In addition to the requirements outlined above, these provisions require that parties grant national treatment for access to payment systems operated by public entities, subject to commitments under the General Agreement on Trade in Services. Furthermore, the provisions preserve regulatory autonomy through explicit statements that nothing prevents parties from maintaining licensing requirements. *Example: WTO Agreement on Electronic Commerce.*

DCO Members Approaches

The DCO Member States are involved in two trade agreements that cover electronic payments.

1. The African Continental Free Trade Agreement Digital Trade Protocol follows the second model (binding provision) with certain idiosyncrasies. First, it states that Parties shall support the development of affordable, real-time, safe, secure, inclusive, responsible and universally accessible cross-border digital payment and settlement systems. Second, it requires parties to develop an Annex on Cross-Border Digital Payments.

2. The WTO Agreement on Electronic Commerce follows the third model (detailed binding provision), as outlined above.

Conclusion

Electronic payments provisions in digital trade agreements are rare and establish various requirements for parties to foster internationally accepted standards, promote interoperability, and encourage innovation and competition. The three models range from non-binding provisions establishing basic principles, binding provisions establishing commitments, and detailed binding provisions expanding on these commitments and providing precise definitions.

At the international level, the DCO Member States are involved in two agreements covering electronic payments, relying on different models. The DCO allows Member States to share their experiences, fostering productive discussions and potentially uncovering areas for collective action.

Digital Trade Agreements with Commitments Electronic Payments

DCO Members:

The DCO Member States are involved in two agreements with a provision on electronic payments:

- African Continental Free Trade Agreement Digital Trade Protocol - Article 15 - Digital Payments
- WTO Agreement on Electronic Commerce - Article 10 - Electronic Payments

Non-DCO Members:

The following agreements also contain provisions on electronic payments:

- ASEAN Agreement on Electronic Commerce - Article 9 - Electronic Payment
- Australia-Singapore Digital Economy Agreement - Article 11 - Electronic Payments
- Digital Economy Partnership Agreement - Article 8 - Electronic Payments
- European Free Trade Association-Moldova Free Trade Agreement - Article 5.12 - Electronic Payments and Invoicing
- India-United Arab Emirates Comprehensive Economic Partnership Agreement - Article 9.17 - Digital and Electronic Payments
- Korea-Singapore Digital Partnership Agreement - Article 14.11 - Electronic Payments
- United Kingdom-Singapore Digital Economy Agreement - Annex B

TRADE FACILITATION WITH DIGITAL MEANS

International Trends

Paperless trade provisions in digital trade agreements are widespread and differ greatly in terms of their bindingness and level of detail. We differentiate three models: endeavour provisions, simple binding provisions, and detailed binding provisions.

Endeavour provisions state that parties "shall endeavour" to make trade documents available electronically and accept electronic documents as legal equivalents of paper documents. Such provisions usually include basic cooperation commitments for promoting electronic document acceptance and references to international guidelines. Flexibility is maintained through language such as "where appropriate" and "endeavour" throughout the provision. Notably, one such provision states that parties “shall work” towards establishing a single window system. Example: Australia-Chile Free Trade Agreement.

The simple binding provisions build on the endeavour provisions but remove the "endeavour" qualification from requirements. Parties thus bindingly commit to make trade documents available electronically (in English) and accept electronic documents as legal equivalents of paper documents. Two carve-outs are foreseen for these commitments: The presence of a domestic or international legal requirement or the reduction of the effectiveness of the trade administration process. These provisions also maintain elements of cooperation and references to international guidelines from the endeavour provisions. *Example: United Kingdom-Singapore Digital Economy Agreement.*

Two types of detailed binding provisions have emerged.

- The first type focuses on integrated data exchange systems and single windows. They require ("shall") parties to establish Single Windows, create secure interfaces between systems, and include specific provisions for data protection and confidentiality. The model emphasizes system interoperability and introduces detailed cooperation mechanisms, including information sharing and pilot projects, and establishes specific requirements for system interoperability. Example: Korea-Singapore Digital Partnership Agreement.
- The other type focuses on the transition from paper to electronic documents, establishing "shall" requirements for customs authorities and “shall endeavour” requirements for other government agencies. Furthermore, it references international standards for electronic form. Example: WTO Agreement on Electronic Commerce.

DCO Members Approaches

The DCO Member States are involved in several agreements with provisions on paperless trade.

- The EU-Colombia, Peru, Ecuador Free Trade Agreement and the EU-New Zealand Free Trade Agreement follow the first model (endeavour provision), as outlined above.
- The African Continental Free Trade Agreement Digital Trade Protocol follows the second model (simple binding provision), as outlined above.
- The WTO Agreement on Electronic Commerce follows the third model (detailed binding provision) including "shall" requirements for customs authorities and "shall endeavour" requirements for other government agencies. The Agreement further contains a dedicated provision on single windows, focusing on data exchange and system Interoperability.

Conclusion

Paperless trade provisions in digital trade agreements range from endeavour provisions on basic trade facilitation to detailed binding provisions outlining requirements for single window systems. Throughout the different models, the emphasis lies on the availability of electronic trade administration documents, as well as advanced trade facilitation mechanisms.

At the international level, the DCO Member States are involved in several agreements covering paperless trade, using different models. Through the DCO, Member States can engage in experience-sharing, which can enhance dialogue and highlight areas where collaboration could be beneficial.

Digital Trade Agreements with Commitments on Paperless trade

DCO Members:

The DCO Member States are involved in the following agreements with provisions on paperless trade:

- African Continental Free Trade Agreement Digital Trade Protocol - Article 10 - Paperless Trading
- EU-Colombia, Peru, Ecuador Free Trade Agreement - Title IV, Chapter 6, Article 165 - Management of Paperless Trading
- EU-New Zealand Free Trade Agreement - Article 12.15 - Paperless Trade in Goods
- WTO Agreement on Electronic Commerce - Article 8 - Paperless Trading - and Article 9 - Single Windows Data Exchange and System Interoperability

Non-DCO Members:

The following agreements also contain provisions on paperless trade:

- ASEAN Agreement on Electronic Commerce - Article 7 - Facilitating Cross-Border E-Commerce (1. Paperless Trading)
- ASEAN-Australia-New Zealand Free Trade Area - Chapter 10, Article 8 - Paperless Trading
- Australia-Chile Free Trade Agreement - Chapter 16, Article 16.9 - Paperless Trading
- Australia-China Free Trade Agreement - Chapter 12, Article 12.9 - Paperless Trading
- Australia-Hong Kong Free Trade Agreement - Chapter 11, Article 11.10 - Paperless Trading
- Australia-Indonesia Comprehensive Economic Partnership Agreement - Chapter 13, Article 13.4 - Paperless Trading
- Australia-Singapore Digital Economy Agreement - Article 12 - Paperless Trading
- Australia-Singapore Free Trade Agreement - Chapter 14, Article 10 - Paperless Trading
- Australia-Thailand Free Trade Agreement - Chapter 11, Article 1107 - Paperless Trading
- Australia-United Kingdom Free Trade Agreement - Article 14.8 - Paperless Trading
- Canada-Colombia Free Trade Agreement - Chapter 15, Article 1505 - Paperless Trade Administration
- Canada-Peru Free Trade Agreement - Chapter 15, Article 1506 - Paperless Trade Administration
- China-Cambodia Free Trade Agreement - Chapter 10, Article 10.7 - Paperless Trade
- China-Korea Free Trade Agreement - Chapter 13, Article 13.6 - Paperless Trading
- China-Mauritius Free Trade Agreement - Chapter 11, Article 11.8 - Paperless Trading
- China-New Zealand Free Trade Agreement Upgrade - Chapter 19, Article 10 - Paperless Trading
- China-Singapore Free Trade Agreement Upgrade - Chapter 15, Article 9 - Paperless Trading
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership - Article 14.9 - Paperless Trading
- European Free Trade Association-Moldova Free Trade Agreement - Chapter 5, Article 5.7 - Paperless Trade Administration

- Iceland-Liechtenstein-Norway-United Kingdom Free Trade Agreement - Article 4.7 - Paperless Trading
- India-United Arab Emirates Comprehensive Economic Partnership Agreement - Chapter 9, Article 9.4 - Paperless Trading
- Japan-Switzerland Free Trade Agreement - Chapter 8, Article 79 - Paperless Trade Administration
- Korea-Australia Free Trade Agreement - Chapter 15, Article 15.7 - Paperless Trading
- Korea-Canada Free Trade Agreement - Chapter 13, Article 13.5 - Paperless Trade Administration
- Korea-Colombia Free Trade Agreement - Chapter 12, Article 12.4 - Paperless Trade Administration
- Korea-Israel Free Trade Agreement - Chapter 13, Article 13.8 - Paperless Trading
- Korea-Peru Free Trade Agreement - Chapter 14, Article 14.6 - Paperless Trading
- Korea-Singapore Digital Partnership Agreement - Article 14.12 - Paperless Trading
- Korea-Vietnam Free Trade Agreement - Chapter 10, Article 10.7 - Paperless Trading
- Peru-Australia Free Trade Agreement - Chapter 13, Article 13.9 - Paperless Trading
- Regional Comprehensive Economic Partnership - Article 12.5 - Paperless Trading
- Singapore-New Zealand Closer Economic Partnership Upgrade - Chapter 9, Article 9.8 - Paperless Trading
- Singapore-Sri Lanka Free Trade Agreement - Chapter 9, Article 9.8 - Paperless Trading
- Singapore-Taiwan Economic Partnership - Chapter 11, Article 11.6 - Paperless Trade Administration
- Singapore-Turkey Free Trade Agreement - Chapter 9, Article 9.8 - Paperless Trading
- United Kingdom-New Zealand Free Trade Agreement - Article 15.10 - Paperless Trading
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-G - Paperless Trading
- United Kingdom-Singapore Digital Economy Agreement - Article 8.61-B - Paperless Trading
- United States-Mexico-Canada Agreement - Article 19.9 - Paperless Trading
- United States-Colombia Free Trade Agreement - Chapter 15, Article 15.7 - Paperless Trade Administration
- United States-Korea Free Trade Agreement - Chapter 15, Article 15.6 - Paperless Trading
- United States-Peru Trade Promotion Agreement - Chapter 15, Article 15.7 - Paperless Trade Administration

DATA PROTECTION

International Trends

Data protection provisions are widespread in digital trade agreements, albeit with varying degrees of bindingness. We differentiate three models: non-binding provisions, mixed provisions with binding and non-binding elements, and binding provisions.

The non-binding model relies on "should" language to establish non-binding expectations on data protection. Such provisions typically encourage parties to adopt or maintain laws, regulations or administrative measures to protect the data of other parties' users, when they engage in electronic commerce. This basic data protection requirement is usually complemented by an encouragement to build regulatory cooperation mechanisms, including information exchange on domestic regimes. *Example: Canada-Peru Free Trade Agreement.*

The mixed model combines binding and non-binding elements. The provisions typically recognize the economic and social benefits of data protection in electronic commerce. A binding ("shall") requirement to adopt or maintain legal frameworks for protecting data presents the core obligation. The provisions often specify that such a framework can comprise comprehensive privacy laws, sector-specific regulations, or laws that enforce voluntary undertakings. Additional elements are drafted in binding or non-binding language, depending on the agreement. This includes the consideration of international principles, the development of compatibility mechanisms and the publication of information on specific compliance requirements and remedies for violations. Example: Comprehensive and Progressive Agreement for Trans-Pacific Partnership.

The binding model uses "shall" language throughout, covering all the elements of the mixed model with additional specifications. For instance, certain provisions specify the principles for data protection frameworks, including security, accountability, and transparency, among others. Furthermore, this model specifies mechanisms for compatibility and interoperability between different data protection regimes. Such mechanisms typically include regulatory recognition, trustmarks, and certification frameworks. Some agreements acknowledge specific international frameworks as valid mechanisms to facilitate cross-border information. Finally, the binding model places significant emphasis on cooperation, requiring information exchange in binding language. Example: Australia-Singapore Digital Economy Agreement.

DCO Members Approaches

The DCO Member States are involved in several agreements with dedicated provisions on data protection.

- The EU-Canada Comprehensive Economic and Trade Agreement, the EU-Colombia, Peru, Ecuador Free Trade Agreement and the EU-Chile Advanced Framework Agreement rely on the first model (non-binding provision), as outlined above. The EU-United Kingdom Trade and Cooperation Agreement follows the non-binding model, and additionally requires parties to inform each other about data protection measures.
- The EU-Japan Economic Partnership Agreement and the EU-New Zealand Free Trade Agreement follow the second model (mixed provision). The WTO Agreement on Electronic Commerce also follows this model, albeit providing additional detail and a dedicated exception provision.
- The African Continental Free Trade Agreement Digital Trade Protocol follows the third model (binding provision), as outlined above.

Conclusion

The progression across the bindingness of international commitments reflects different approaches to balancing flexibility with harmonization in data protection requirements. The core element across all models is establishing a data protection framework. In addition, from non-binding to mixed to binding models, additional commitments range from basic cooperation towards detailed pointers for regulatory design and alignment.

At the international level, the DCO Member States are involved in several agreements covering data transfers, using various models. Member States may use the DCO as a platform to share their experiences, fostering informed discussions and identifying potential opportunities for collaboration.

Digital Trade Agreements with Commitments on Data Protection

DCO Members:

The DCO Member States are involved in the following agreements with provisions on data protection:

- African Continental Free Trade Agreement Digital Trade Protocol - Article 21 - Protection of Personal Data
- EU-Canada Comprehensive Economic and Trade Agreement - Chapter 16 Article 16.4 - Trust and confidence in electronic commerce

- EU-Chile Advanced Framework Agreement - Chapter 19 Article 19.5 - Protection of personal data and privacy
- EU-Colombia, Peru, Ecuador Free Trade Agreement - Title IV Chapter 6 Article 164 - Protection of Personal Data
- EU-Japan Economic Partnership Agreement - Chapter 8 Section F, Article 8.82 - Protection of Personal Data
- EU-New Zealand Free Trade Agreement - Chapter 12 - Article 12.5 - Protection of personal data and privacy
- EU-United Kingdom Trade and Cooperation Agreement - Title III Article 202 - Protection of Personal Data and Privacy
- WTO Agreement on Electronic Commerce - Article 16 - Personal Data Protection - and Article 25 - Personal Data Protection Exception

Non-DCO Members:

The following agreements also contain provisions on data protection:

- ASEAN Agreement on Electronic Commerce - Article 7 - Facilitating Cross-Border E-Commerce (5. Online Personal Information Protection)
- ASEAN-Australia-New Zealand Free Trade Area - Chapter 10 Article 7 - Online Data Protection
- Australia-Chile Free Trade Agreement - Chapter 16 Article 16.8 - Online Personal Data Protection
- Australia-China Free Trade Agreement - Chapter 12 Article 12.8 - Online Data Protection
- Australia-Hong Kong Free Trade Agreement - Chapter 11 Article 11.9 - Protection of Personal Information
- Australia-Singapore Digital Economy Agreement - Article 17 - Personal Information Protection
- Australia-Singapore Free Trade Agreement - Chapter 14 Article 9 - Personal Information Protection
- Australia-Thailand Free Trade Agreement - Chapter 11 Article 1106 - Online Personal Data Protection
- Australia-United Kingdom Free Trade Agreement - Chapter 14 Article 14.12 - Personal Information Protection
- Canada-Colombia Free Trade Agreement - Chapter 15 Article 1506 - Protection of Personal Information
- Canada-Peru Free Trade Agreement - Chapter 15 Article 1507 - Protection of Personal Information
- China-Cambodia Free Trade Agreement - Chapter 10 Article 10.6 - Online Personal Information Protection
- China-Eurasian Economic Union Free Trade Agreement - Chapter 11 Article 11.6 -

Personal Information Protection

- China-Korea Free Trade Agreement - Chapter 13 Article 13.5 - Protection of Personal Information in Electronic Commerce
- China-Mauritius Free Trade Agreement - Chapter 11 Article 11.7 - Online Data Protection
- China-New Zealand Free Trade Agreement Upgrade - Chapter 19 Article 9 - Online Personal Information Protection
- China-Singapore Free Trade Agreement Upgrade - Chapter 15 Article 8 - Personal Information Protection
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership - Chapter 14 - Article 14.8 - Personal Information Protection
- Digital Economy Partnership Agreement - Personal Information Protection
- European Free Trade Association-Moldova Free Trade Agreement - Chapter 5 Article 5.13 - Protection of Personal Data and Privacy
- Iceland-Liechtenstein-Norway-United Kingdom Free Trade Agreement - Chapter 4 Article 4.12 - Protection of Personal Data and Privacy
- India-United Arab Emirates Comprehensive Economic Partnership Agreement - Chapter 9 Article 9.10 - Personal Data Protection
- Korea-Australia Free Trade Agreement - Chapter 15 Article 15.8 - Online Personal Data Protection
- Korea-Canada Free Trade Agreement - Chapter 13 Article 13.4 - Protection of Personal Information
- Korea-Colombia Free Trade Agreement - Chapter 12 Article 12.3 - Online Personal Data Protection
- Korea-Israel Free Trade Agreement - Chapter 13 Article 13.7 - Personal Data Protection
- Korea-Peru Free Trade Agreement - Chapter 14 Article 14.7 - Protection of Personal Information
- Korea-Singapore Digital Partnership Agreement - Article 14.17 - Personal Information Protection
- Korea-Vietnam Free Trade Agreement - Chapter 10 Article 10.6 - Personal Data Protection
- Peru-Australia Free Trade Agreement - Chapter 13 Article 13.8 - Personal Information Protection
- Regional Comprehensive Economic Partnership - Chapter 12 Article 12.8 - Online Personal Information Protection
- Singapore-Eurasian Economic Union Free Trade Agreement - Chapter 9 Article 9.7 - Personal Data Protection
- Singapore-New Zealand Closer Economic Partnership Upgrade - Chapter 9 Article 9.7 - Personal Information Protection
- Singapore-Sri Lanka Free Trade Agreement - Chapter 9 Article 9.7 - Personal Data Protection

- Singapore-Turkey Free Trade Agreement - Chapter 9 Article 9.7 - Personal Data Protection
- United Kingdom-Japan Comprehensive Economic Partnership Agreement - Chapter 8 Section F Article 8.80 - Personal Information Protection
- United Kingdom-New Zealand Free Trade Agreement - Chapter 15 Article 15.13 - Personal Information Protection
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-J - Personal Data Protection
- United Kingdom-Singapore Digital Economy Agreement - Article 8.61-E - Personal Information Protection
- United States-Mexico-Canada Agreement - Chapter 19 - Article 19.8 - Personal Information Protection
- United States-Japan Digital Trade Agreement - Article 15 - Personal Information Protection

CROSS-BORDER DATA TRANSFERS

International Trends

Data transfer provisions are common in digital trade agreements and generally follow two models: general prohibitions on data transfer restrictions and specific prohibitions on data transfer restrictions.

General prohibitions on data transfers restrictions typically recognize that parties have their own regulatory requirements for data protection and transfers. Parties then generally commit not to prohibit or restrict cross-border data transfers for business purposes. Provisions then provide exceptions, allowing parties to adopt measures that restrict data transfers to achieve legitimate public policy objectives. Objectives are generally not enumerated. The provisions further state that measures must not create arbitrary discrimination or disguised trade restrictions, and must not impose restrictions on transfers greater than required to achieve the objective. Example: Comprehensive and Progressive Agreement for Trans-Pacific Partnership.

Specific prohibitions on data transfer restrictions commit parties to ensure cross-border data transfers and prohibit specific measures that restrict data transfers. These measures include:

- requiring the use of local computing facilities and demanding the localization of data storage and processing, as well as making transfers contingent on infrastructure or data localization;[111]
- prohibiting outbound transfers in general or towards the other party; and
- requiring prior approval of transfers to the other party.

Specific prohibitions also contain exception mechanisms. One mechanism is similar to the general prohibition model, albeit with specifications on "legitimate public policy objectives." Objectives must be interpreted in an objective manner and include, among others, the protection of public security, public morals, life or health, as well as the maintenance of public order. Another mechanism allows data protection measures, including on data transfers, as long as they provide instruments for data transfers under conditions of general application. This refers to conditions that are objective and apply horizontally, across economic actors and scenarios. *Example: EU-New Zealand Free Trade Agreement.*

[111] Since these provisions touch upon the location of computing facilities, the corresponding chapter and Annex make reference thereto, without further discussing their content.

Beyond these two models, select digital trade agreements include other, less frequently used provisions on data transfers. Such provisions cover only specific sectors, for instance financial services, or establish non-binding commitments regarding data transfers.

DCO Members Approaches

The DCO Member States are involved in five agreements with dedicated provisions on data transfers.

The African Continental Free Trade Agreement Digital Trade Protocol follows the first model (general prohibition) albeit with certain idiosyncrasies. Namely, it creates an Annex on Cross-Border Data Transfers that sets out legitimate public policy objectives, how data may be used, and restrictions on sharing of data to third parties.

The EU-Chile Advanced Framework Agreement, the EU-New Zealand Free Trade Agreement, and the EU-United Kingdom Trade and Cooperation Agreement follow the second model (specific prohibition), as outlined above. The EU-Japan Economic Partnership Agreement, which was amended in 2024 via a data flows and personal data protection protocol, follows this model and provides additional detail.

Conclusion

Data transfer provisions in digital trade agreements aim to facilitate digital trade while protecting data. There are two models of international commitments. General prohibitions on data transfer restrictions, with exceptions, and specific prohibitions on data transfer restrictions, which prohibit enumerated measures and also provide exceptions. Specific prohibitions are more precisely formulated, especially with regards to the exception mechanisms. In addition, sector-specific and non-binding data transfer provisions exist but are rarely used.

At the international level, the DCO Member States are involved in several agreements covering data transfers, using both models. Member States can utilize DCO as a forum to exchange experiences. This can allow for a more informed dialogue and potentially uncover areas for future coordination.

Digital Trade Agreements with Commitments on Cross-Border Data Transfers

DCO Members:

The DCO Member States are involved in the following agreements with provisions on cross-border data transfers:

- African Continental Free Trade Agreement Digital Trade Protocol - Article 20 - Cross-Border Data Transfers
- EU-Chile Advanced Framework Agreement - Chapter 19 Article 19.4 - Cross-Border Data Flows: Prohibition of Data Localization
- EU-Japan Economic Partnership Agreement - Chapter 8 Section F 8.81 - Cross-border transfer of information by electronic means
- EU-New Zealand Free Trade Agreement - Chapter 12 Article 12.4 - Cross-Border Data Flows
- EU-United Kingdom Trade and Cooperation Agreement - Title III Article 201 - Cross-Border Data Flows

Non-DCO Members:

The following agreements also contain provisions on cross-border data transfers:

- ASEAN Agreement on Electronic Commerce - Article 7 - Facilitating Cross-Border E-Commerce (4. Cross-border Transfer of Information by Electronic Means)
- Australia-Hong Kong Free Trade Agreement - Chapter 11 Article 11.7 - Movement of Information
- Australia-Hong Kong Free Trade Agreement - Chapter 11 Article 11.15 - Movement of Information and Location of Computing Facilities for Financial Services
- Australia-Indonesia Comprehensive Economic Partnership Agreement - Chapter 13 Article 13.11 - Cross-Border Transfer of Information by Electronic Means
- Australia-Singapore Digital Economy Agreement - Article 23 - Cross-Border Transfer of Information by Electronic Means
- Australia-Singapore Free Trade Agreement - Chapter 14 Article 13 - Cross-Border Transfer of Information by Electronic Means
- Australia-United Kingdom Free Trade Agreement - Chapter 14 Article 14.10 - Cross-Border Transfer of Information by Electronic Means
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership - Chapter 14 Article 14.11 - Cross-Border Transfer of Information by Electronic Means
- Digital Economy Partnership Agreement - Cross-Border Transfer of Information by Electronic Means

- European Free Trade Association-Moldova Free Trade Agreement - Chapter 5 Article 5.11 - Cross-border Data Flows
- Iceland-Liechtenstein-Norway-United Kingdom Free Trade Agreement - Chapter 4 Article 4.11 - Cross-Border Data Flows
- India-United Arab Emirates Comprehensive Economic Partnership Agreement - Chapter 9 Article 9.11 - Cross-Border Flow of Information
- Korea-Singapore Digital Partnership Agreement - Article 14.14 - Cross-Border Transfer of Information by Electronic Means
- Peru-Australia Free Trade Agreement - Chapter 13 Article 13.11 - Cross-Border Transfer of Information by Electronic Means
- Regional Comprehensive Economic Partnership - Chapter 12 Article 12.15 - Cross-Border Transfer of Information by Electronic Means
- Singapore-Eurasian Economic Union Free Trade Agreement - Chapter 9 Article 9.8 - Cross-Border Transfer of Information in Electronic Commerce
- Singapore-New Zealand Closer Economic Partnership Upgrade - Chapter 9 Article 9.10 - Cross-Border Transfer of Information by Electronic Means
- Singapore-Sri Lanka Free Trade Agreement - Chapter 9 Article 9.9 - Cross-Border Transfer of Information by Electronic Means
- United Kingdom-Japan Comprehensive Economic Partnership Agreement - Chapter 8 Section F Article 8.84 - Cross-border Transfer of Information by Electronic Means
- United Kingdom-New Zealand Free Trade Agreement - Chapter 15 Article 15.14 - Cross-Border Transfer of Information by Electronic Means
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-K - Cross-Border Transfer of Information by Electronic Means
- United Kingdom-Singapore Digital Economy Agreement - Article 8.61-F - Cross-Border Transfer of Information by Electronic Means
- United States-Mexico-Canada Agreement - Chapter 19 Article 19.11 - Cross-Border Transfer of Information by Electronic Means
- United States-Japan Digital Trade Agreement - Article 11 - Cross-Border Transfer of Information by Electronic Means
- United States-Korea Free Trade Agreement - Chapter 15 Article 15.8 - Cross-Border Information Flows

LOCATION OF COMPUTING FACILITIES

International Trends

Data localization provisions are common in digital trade agreements and can be categorised into three models: strict data localization prohibitions, data localization prohibitions with exceptions, and sector-specific data localization provisions.

Strict prohibitions are relatively rare. Such provisions strictly prohibit the requirement for businesses to use or locate computing facilities within a party's territory as a condition for conducting business. These provisions are straightforward, establishing a strict prohibition on data localization requirements without allowing for exceptions. While they acknowledge that parties may have their own regulatory requirements concerning the use of computing facilities, for instance concerning the security and confidentiality of communications, no exceptions allow for national data localization mandates. *Example: United States-Mexico-Canada Agreement.*

Prohibitions with exceptions are the most common model of data localization provisions. These provisions generally prohibit mandatory data localization in the same manner as strict prohibitions. But they allow for exceptions, namely if localization requirements are necessary to achieve legitimate public policy objectives. These objectives are usually not enumerated. Furthermore, the provisions demand that data localization measures are not applied in a manner that constitutes arbitrary or unjustifiable discrimination and do not impose disguised trade restrictions. Finally, the data localization measures must not exceed what is necessary to achieve the objective. *Example: Comprehensive and Progressive Agreement for Trans-Pacific Partnership.*

Sector-specific data localization provisions mainly concern financial services. These provisions generally prohibit mandatory localization for financial services in a similar fashion to strict prohibitions. They tend to include exceptions, albeit through a different mechanism that emphasises regulatory access. Namely, data localization mandates are prohibited, provided that parties' financial regulatory authorities have access to data that is stored abroad, for regulatory and supervisory purposes. In addition, parties must provide financial service providers with the opportunity to remediate any lack of access, before demanding data localization. *Example: Korea-Singapore Digital Partnership Agreement.*

DCO Members Approaches

The DCO Member States are involved in one agreement with a dedicated provision on data localization. The African Continental Free Trade Agreement Digital Trade Protocol follows the second model, establishing a prohibition with exceptions.
Notably, certain EU agreements contain provisions dedicated to Cross-Border Data Transfers that also touch upon data localization. These provisions have been discussed in the chapter on Cross-Border Data Transfers. To ensure comprehensiveness and clarity, the present Annex on "Location of Computing Facilities" lists them again, separately.

Conclusion

Data localization provisions in digital trade agreements aim to facilitate digital trade while maintaining regulatory oversight. There are three models of international commitments. Strict prohibitions do not allow for data localization mandates. Prohibitions with exceptions leave room for data localization mandates, with significant restrictions. Sector-specific provisions emphasize regulatory access to data without localization, leaving limited room for data localization mandates.

At the international level, the DCO Member States are involved in one agreement covering data localization and establishing a prohibition with exceptions. This count excludes the EU provisions discussed in the chapter on Cross-Border Data Transfers. Member States can utilize DCO as a platform to share experiences and understand the rationale behind different approaches. This can foster a more informed discussion and potentially identify areas for future alignment.

Digital Trade Agreements with Commitments on Location of Computing Facilities

DCO Members:

The DCO Member States are involved in the following agreements with provisions on data localization:

- African Continental Free Trade Agreement Digital Trade Protocol - Article 22 - Location of Computing Facilities

The following agreements including DCO Member States also contain provisions that cover data localization, but are discussed in the chapter on Cross-Border Data Transfers:

- EU-Chile Advanced Framework Agreement - Chapter 19 Article 19.4 - Cross-Border Data Flows: Prohibition of Data Localization
- EU-Japan Economic Partnership Agreement - Chapter 8 Section F 8.81 - Cross-border transfer of information by electronic means
- EU-New Zealand Free Trade Agreement - Chapter 12 Article 12.4 - Cross-Border Data Flows
- EU-United Kingdom Trade and Cooperation Agreement - Title III Article 201 - Cross-Border Data Flows

Non-DCO Members:

The following agreements also contain provisions on data localization:

- ASEAN Agreement on Electronic Commerce - Article 7 - Facilitating Cross-Border E-Commerce (6. Location of Computing Facilities)
- Australia-Hong Kong Free Trade Agreement - Chapter 11 Article 11.8 - Location of Computing Facilities
- Australia-Hong Kong Free Trade Agreement - Chapter 11 Article 11.15 - Movement of Information and Location of Computing Facilities for Financial Services
- Australia-Indonesia Comprehensive Economic Partnership Agreement - Chapter 13 Article 13.12 - Location of Computing Facilities
- Australia-Singapore Digital Economy Agreement - Article 24 - Location of Computing Facilities
- Australia-Singapore Digital Economy Agreement - Article 25 - Location of Computing Facilities for Financial Services
- Australia-Singapore Free Trade Agreement - Chapter 14 Article 15 - Location of Computing Facilities
- Australia-United Kingdom Free Trade Agreement - Chapter 14 Article 14.11 - Location of Computing Facilities
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership - Chapter 14 Article 14.13 - Location of Computing Facilities
- Digital Economy Partnership Agreement - Article 15 - Location of Computing Facilities
- Korea-Singapore Digital Partnership Agreement - Article 14.15 - Location of Computing Facilities
- Korea-Singapore Digital Partnership Agreement - Article 14.16 - Location of Computing Facilities for Financial Services
- Peru-Australia Free Trade Agreement - Chapter 13 Article 13.12 - Location of Computing Facilities

- Regional Comprehensive Economic Partnership - Chapter 12 Article 12.14 - Location of Computing Facilities
- Singapore-New Zealand Closer Economic Partnership Upgrade - Chapter 9 Article 9.11 - Location of Computing Facilities
- Singapore-Sri Lanka Free Trade Agreement - Chapter 9 Article 9.10 - Location of Computing Facilities
- United Kingdom-Japan Comprehensive Economic Partnership Agreement - Chapter 8 Section F Article 8.85 - Location of Computing Facilities
- United Kingdom-New Zealand Free Trade Agreement - Chapter 15 Article 15.15 - Location of Computing Facilities
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-L - Location of Computing Facilities
- United Kingdom-Singapore Digital Economy Agreement - Article 8.61-G - Location of Computing Facilities
- United States-Mexico-Canada Agreement - Chapter 19 Article 19.12 - Location of Computing Facilities
- United States-Japan Digital Trade Agreement - Article 12 - Location of Computing Facilities - and Article 13 - Location of Financial Service Computing Facilities for Covered Financial Service Suppliers

The following agreements also contain provisions that cover data localization, but are discussed in the chapter on Cross-Border Data Transfers:

- Iceland-Liechtenstein-Norway-United Kingdom Free Trade Agreement - Chapter 4 Article 4.11 - Cross-Border Data Flows
- European Free Trade Association-Moldova Free Trade Agreement - Chapter 5 Article 5.11 - Cross-Border Data Flows

ONLINE CONSUMER PROTECTION AND UNSOLICITED COMMERCIAL ELECTRONIC COMMUNICATIONS

International Trends

Consumer protection provisions are widespread in digital trade agreements. Over time, four models have emerged: non-binding provisions, basic binding provisions, prescriptive binding provisions, and prohibitive binding provisions. Similarly, provisions dedicated to unsolicited commercial electronic messages ("spam") have various degrees of bindingness and precision, albeit with more overlap.

The non-binding model comprises provisions that merely recognize the importance of consumer protection in e-commerce and cross-border cooperation. Some provisions also state that parties should exchange information and experiences on online consumer protection. By using entirely non-binding language, parties acknowledge the importance of consumer protection without creating specific obligations. Example: Canada-Honduras Free Trade Agreement.

The basic binding model combines the recognition of consumer protection's importance with specific binding obligations. Provisions typically require parties to adopt consumer protection laws targeting fraudulent and deceptive practices in online commerce. The goal is to protect e-commerce consumers equivalently to traditional commerce consumers. Still, significant qualifying language ("to the extent possible"), provides parties with flexibility in implementation. Beyond this core requirement, basic binding models often contain non-binding elements concerning cooperation. Example: China-Singapore Free Trade Agreement Upgrade.

The prescriptive binding model maintains the equivalence principle and adds detailed provisions on business conduct. The emphasis lies on prescriptive regulation of business behaviour: Parties shall encourage businesses to do certain practices rather than prescribing what they cannot do, including:

- Providing accurate, clear, and accessible information about themselves and their offerings;
- Enabling consumers to identify products precisely before purchase;
- Allowing consumers to correct errors and modify orders;
- Requiring explicit consumer consent for purchases;
- Ensuring consumers can retain transaction records; and
- Providing secure payment mechanisms with security level information. *Example:*

Australia-Chile Free Trade Agreement.

The prohibitive binding model requires parties to prohibit certain business practices ("misleading and deceptive commercial activities"). Most agreements enumerate such practices, most commonly: making material misrepresentations affecting consumer decisions, failing to deliver products after charging consumers, and charging accounts without authorization. Some provisions expand these prohibited practices, for instance to advertising without intention to supply. Some specify the practices, for instance regarding which aspects of products cannot be misrepresented (quality, price, origin) or consumer redress mechanisms. Notably, certain provisions also add positive obligations, regarding fair and honest dealing with consumers, complete and transparent information provision, and product safety. Finally, institutional aspects such as cooperation and redress mechanisms are covered, by either binding or non-binding language. *Example: WTO Agreement on Electronic Commerce.*

Provisions regulating spam are less common but still frequent, with a notable overlap.

- Singular provisions use "shall endeavour" language, encouraging parties to adopt measures to regulate spam, promote cooperation, and adopt best practices. Example: India-United Arab Emirates Comprehensive Economic Partnership Agreement.
- Provisions requiring parties to act directly are more prevalent and share two core requirements. First, parties must ensure that spam suppliers facilitate the ability of recipients to prevent spam, ensuring straightforward and accessible ways to opt-out or unsubscribe. Second, parties must require the consent of recipients to be obtained before sending spam. Certain provisions add a third element regarding strategies to minimize spam and reduce their volume and impact on users. Binding provisions typically demand a robust recourse mechanism, ensuring that recipients have access to legal remedies. Certain agreements add further detail, for instance requiring spam messages to be clearly identifiable and disclose details on the supplier. Example: United States-Mexico-Canada Agreement.

DCO Members Approaches

Regarding online consumer protection, the DCO Member States are involved in several agreements with dedicated provisions:

- The United States-Oman Free Trade Agreement, the EU-Colombia, Peru, Ecuador Free Trade Agreement, and the EU-Japan Economic Partnership Agreement follow the first model (non-binding provision), as outlined above.
- The EU-Mexico Trade Agreement follows the second model (basic binding provision),

as outlined above.

- The EU-Chile Advanced Framework Agreement, the EU-United Kingdom Trade and Cooperation Agreement, the EU-New Zealand Free Trade Agreement, the WTO Agreement on Electronic Commerce, and the African Continental Free Trade Agreement Digital Trade Protocol follow the fourth model (prohibitive binding provision), as outlined above, albeit with varying degrees of detail.

Regarding spam, the DCO Member States are also involved in several agreements with dedicated provisions. The EU-Chile Advanced Framework Agreement, the EU-Japan Economic Partnership Agreement, the EU-Mexico Trade Agreement, the EU-New Zealand Free Trade Agreement, the EU-United Kingdom Trade and Cooperation Agreement, the WTO Agreement on Electronic Commerce, and the African Continental Free Trade Agreement Digital Trade Protocol all follow the second model, requiring parties to act directly.

Conclusion

Consumer protection provisions are common and diverge in terms of their bindingness, level of detail, and approach to business practices. Most commonly, provisions require parties' consumer protection frameworks to grant equivalent protection to online and offline consumers. Frequently, provisions enumerate prohibited practices, from misrepresentations, to failure of delivery, to unauthorized charging. Provisions on spam also have various degrees of bindingness, although most require suppliers parties to allow spam only if suppliers obtain recipients' consent and facilitate their ability to prevent reception.

At the international level, the DCO Member States are involved in several agreements covering online consumer protection and spam regulation, using different models.

Digital Trade Agreements with Commitments on Online Consumer Protection and Unsolicited Commercial Electronic Communications

DCO Members:

The DCO Member States are involved in the following agreements with provisions on consumer protection:

- African Continental Free Trade Agreement Digital Trade Protocol Article 27 - Online Consumer Protection
- EU-Chile Advanced Framework Agreement - Chapter 19 Article 19.10 - Online Consumer

Trust
- EU-Colombia, Peru, Ecuador Free Trade Agreement - Title IV Chapter 6 Article 166 - Consumer Protection
- EU-Japan Economic Partnership Agreement - Chapter 8 Section F Article 8.78 - Consumer Protection
- EU-Mexico Trade Agreement - Chapter 16 Article 7 - Online Consumer Protection
- EU-New Zealand Free Trade Agreement - Article 12.12 - Consumer Trust Online
- EU-United Kingdom Trade and Cooperation Agreement - Title III Article 208 - Online Consumer Trust
- United States-Oman Free Trade Agreement - Chapter 14 Article 14.4 - Consumer Protection
- WTO Agreement on Electronic Commerce - Article 14 - Online Consumer Protection

The DCO Member States are involved in the following agreements with provisions on spam:

- African Continental Free Trade Agreement Digital Trade Protocol - Article 28 - Unsolicited Commercial Electronic Communications
- EU-Chile Advanced Framework Agreement - Chapter 19.11 - Article 19.7 Unsolicited direct marketing communications
- EU-Japan Economic Partnership Agreement - Chapter 8 Section F Article 8.79 - Unsolicited commercial electronic messages
- EU-Mexico Trade Agreement - Chapter 16 Article 8 - Unsolicited Commercial Electronic Messages
- EU-New Zealand Free Trade Agreement - Chapter 12 Article 12.13 - Unsolicited direct marketing communications
- EU-United Kingdom Trade and Cooperation Agreement - Title III Article 209 - Unsolicited Direct Marketing Communications
- WTO Agreement on Electronic Commerce - Article 15 - Unsolicited Commercial Electronic Messages

Non-DCO Members:

The following agreements also contain provisions on consumer protection:

- ASEAN Agreement on Electronic Commerce - Article 7 - Facilitating Cross-Border E-Commerce (3. Online Consumer Protection)
- ASEAN-Australia-New Zealand Free Trade Area - Chapter 10 Article 6 - Online Consumer Protection
- Australia-Chile Free Trade Agreement - Chapter 16 Article 16.7 - Online Consumer Protection
- Australia-China Free Trade Agreement - Chapter 12 Article 12.7 - Online Consumer

Protection

- Australia-Hong Kong Free Trade Agreement - Chapter 11 Article 11.5 - Consumer Protection
- Australia-Indonesia Comprehensive Economic Partnership Agreement - Article 13.6 - Online Consumer Protection
- Australia-Singapore Digital Economy Agreement - Article 15 - Online Consumer Protection
- Australia-Singapore Free Trade Agreement - Chapter 14 Article 8 - Online Consumer Protection
- Australia-Thailand Free Trade Agreement - Chapter 11 Article 1105 - Online Consumer Protection
- Australia-United Kingdom Free Trade Agreement - Article 14.16 - Online Consumer Protection
- Canada-Colombia Free Trade Agreement - Chapter 15 Article 1504 - Consumer Protection
- Canada-Honduras Free Trade Agreement - Chapter 16 Article 16.4 - Consumer Protection
- Canada-Peru Free Trade Agreement - Chapter 15 Article 1505 - Consumer Protection
- China-Cambodia Free Trade Agreement - Chapter 10 Article 10.5 - Online Consumer Protection
- China-Eurasian Economic Union Free Trade Agreement - Article 11.5 - E-commerce Consumer Protection
- China-Mauritius Free Trade Agreement - Article 11.6 - Online Consumer Protection
- China-New Zealand Free Trade Agreement Upgrade - Article 8 - Online Consumer Protection
- China-Singapore Free Trade Agreement Upgrade - Article 7 - Online Consumer Protection
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership - Article 14.7 - Online Consumer Protection
- Digital Economy Partnership Agreement - Article 15 - Online Consumer Protection
- European Free Trade Association-Moldova Free Trade Agreement - Article 5.9 - Online Consumer Trust
- India-United Arab Emirates Comprehensive Economic Partnership Agreement - Article 9.8 - Online Consumer Protection
- Iceland-Liechtenstein-Norway-United Kingdom Free Trade Agreement - Article 4.8 - Online Consumer Protection
- Japan-Switzerland Free Trade Agreement - Chapter 8 Article 80 - Protection of Online Consumers
- Korea-Australia Free Trade Agreement - Chapter 15 Article 15.6 - Online Consumer Protection
- Korea-Canada Free Trade Agreement - Chapter 13 Article 13.6 - Consumer Protection

- Korea-Colombia Free Trade Agreement - Chapter 12 Article 12.5 - Consumer Protection
- Korea-Israel Free Trade Agreement - Chapter 13 Article 13.6 - Online Consumer Protection
- Korea-Peru Free Trade Agreement - Chapter 14 Article 14.5 - Consumer Protection
- Korea-Singapore Digital Partnership Agreement - Article 14.21 - Online Consumer Protection
- Korea-Vietnam Free Trade Agreement - Chapter 10 Article 10.5 - Online Consumer Protection
- Regional Comprehensive Economic Partnership - Article 12.7 - Online Consumer Protection
- Singapore-Eurasian Economic Union Free Trade Agreement - Article 9.9 - Consumer Protection
- Singapore-New Zealand Closer Economic Partnership Upgrade - Chapter 9 Article 9.6 - Online Consumer Protection
- Singapore-Peru Free Trade Agreement - Chapter 13 Article 13.2 - Protection from Fraudulent and Deceptive Commercial Practices
- Singapore-Sri Lanka Free Trade Agreement - Chapter 9 Article 9.11 - Online Consumer Protection
- United Kingdom-Japan Comprehensive Economic Partnership Agreement - Chapter 8 Section F Article 8.79 - Consumer Protection
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-R - Online Consumer Protection
- United Kingdom-Singapore Digital Economy Agreement - Article 8.61-M - Online Consumer Protection
- United States-Mexico-Canada Agreement - Article 19.7 - Online Consumer Protection
- United States-Colombia Free Trade Agreement - Article 15.5 - Consumer Protection
- United States-Japan Digital Trade Agreement - Article 14 - Online Consumer Protection
- United States-Korea Free Trade Agreement - Chapter 15 Article 15.5 - Online Consumer Protection
- United States-Peru Trade Promotion Agreement - Chapter 15 Article 15.5 - Consumer Protection

The following agreements also contain provisions on spam:

- Australia-Hong Kong Free Trade Agreement - Chapter 11 Article 11.11 - Unsolicited Commercial Electronic Messages
- Australia-Indonesia Comprehensive Economic Partnership Agreement - Chapter 13 Article 13.8 - Unsolicited Commercial Electronic Messages
- Australia-Singapore Digital Economy Agreement - Article 19 - Unsolicited Commercial Electronic Messages

- Australia-Singapore Free Trade Agreement - Chapter 14 Article 16 - Unsolicited Commercial Electronic Messages
- Australia-United Kingdom Free Trade Agreement - Chapter 14 Article 14.17 - Unsolicited Commercial Electronic Messages
- China-New Zealand Free Trade Agreement Upgrade - Chapter 19 Article 11 - Unsolicited Commercial Electronic Messages
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership - Chapter 14 Article 14.14 - Unsolicited Commercial Electronic Messages
- European Free Trade Association-Moldova Free Trade Agreement - Chapter 5 Article 5.10 - Unsolicited Commercial Electronic Messages
- Iceland-Liechtenstein-Norway-United Kingdom Free Trade Agreement - Chapter 4 Article 4.9 - Unsolicited Commercial Electronic Messages
- India-United Arab Emirates Comprehensive Economic Partnership Agreement - Chapter 9 Article 9.9 - Unsolicited Commercial Electronic Messages
- Korea-Australia Free Trade Agreement - Chapter 15 Article 15.9 - Unsolicited Commercial Electronic Messages
- Korea-Singapore Digital Partnership Agreement - Article 14.20 - Unsolicited Commercial Electronic Messages
- Peru-Australia Free Trade Agreement - Chapter 13 Article 13.13 - Unsolicited Commercial Electronic Messages
- Regional Comprehensive Economic Partnership - Chapter 12 Article 12.9 - Unsolicited Commercial Electronic Messages
- Singapore-Eurasian Economic Union Free Trade Agreement - Chapter 9 Article 9.10 - Unsolicited Commercial Electronic Messages
- Singapore-New Zealand Closer Economic Partnership Upgrade - Chapter 9 Article 9.12 - Unsolicited Commercial Electronic Messages
- United Kingdom-Japan Comprehensive Economic Partnership Agreement - Chapter 8 Section F Article 8.81 - Unsolicited Commercial Electronic Messages
- United Kingdom-New Zealand Free Trade Agreement - Chapter 15 Article 15.11 - Unsolicited Commercial Electronic Messages
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-S - Unsolicited Commercial Electronic Messages
- United Kingdom-Singapore Digital Economy Agreement - Article 8.61-N - Unsolicited Commercial Electronic Messages
- United States-Mexico-Canada Agreement - Chapter 19 Article 19.13 - Unsolicited Commercial Electronic Communications
- United States-Japan Digital Trade Agreement - Article 16 - Unsolicited Commercial Electronic Messages

CYBERSECURITY

International Trends

Cybersecurity provisions in digital trade agreements are frequent, but focus on cooperation rather than establish binding commitments.[113] We distinguish between three models: recognition provisions, provisions to endeavour and encourage, and provisions to act.

In recognition provisions, parties do not commit but enshrine their shared understanding of the importance of cybersecurity measures. In general terms, such provisions recognize one or several of the following elements: That cybersecurity underpins the digital economy, that secure digital trade helps achieve global prosperity, and that threats to cybersecurity undermine confidence in digital trade. Furthermore, such provisions recognize the importance of concrete measures on cybersecurity, namely several (but not always all) of the following:

- building the capabilities of national entities responsible for computer security incident response;
- using existing collaboration mechanisms to cooperate on identifying and mitigating intrusions affecting parties' electronic networks and addressing them swiftly;
- developing the workforce, including through mutual qualification recognition; and
- holding dialogues on cybersecurity, including information and experience sharing to build awareness and develop best practices. Example: India-United Arab Emirates Comprehensive Economic Partnership Agreement.

Other provisions contain "shall" language, albeit to "endeavour to" and "encourage" certain actions.

- In some provisions, parties commit to endeavour regarding certain of the concrete measures outlined in the paragraph above on recognition provisions. Specifically, the endeavours concern building capabilities, collaboration mechanisms, and dialogues. Example: Iceland-Liechtenstein-Norway-United Kingdom Free Trade Agreement.
- Other provisions acknowledge that risk-based approaches may be more effective than prescriptive approaches due to the evolving nature of cybersecurity threats. Thus, the parties "shall encourage" enterprises to use risk-based approaches, relying on open and transparent industry standards, to manage cybersecurity risks, address cybersecurity events, and improve cybersecurity resilience. *Example: United States-Mexico-Canada Agreement.*

[113] Cybersecurity is often mentioned in general provisions on "cooperation" that are not analysed in this chapter.

Finally, provisions to act build on the above and add direct to commitments to adopt or maintain measures to ensure cybersecurity and combat cybercrime, taking into account regional, continental, and international standards and guidelines. Furthermore, parties shall require enterprises in their jurisdictions to use best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity incidents. *Example: African Continental Free Trade Agreement Digital Trade Protocol.*

DCO Members Approaches

The DCO Member States are involved in two agreements with provisions on cybersecurity.

- The WTO Agreement on Electronic Commerce follows the first model. In addition to typical recognition formulations, it states that parties shall endeavour to use, and encourage enterprises within their jurisdictions to use, risk-based cybersecurity approaches that rely on risk management best practices and consensus-based, transparent, and open standards.
- The African Continental Free Trade Agreement Digital Trade Protocol follows the third model, as outlined above.

Conclusion

Cybersecurity provisions in digital trade agreements are mainly non-binding and focused on international collaboration, rather than national regulation. Parties recognize the importance of cybersecurity for flourishing digital trade and mechanisms to uphold cybersecurity. Rarely, parties commit to endeavours regarding mechanisms to uphold cybersecurity or to encouraging firms to improve their cybersecurity. A unique provision contains a commitment to act, namely to adopt cybersecurity frameworks and require firms to follow best practices.

At the international level, the DCO Member States are involved in two agreements covering cybersecurity, using different models. Using the DCO as a platform, Member States can share their expertise, enabling deeper dialogue and uncovering opportunities for mutual coordination.

Digital Trade Agreements with Commitments on Cybersecurity

DCO Members:

The DCO Member States are involved in the following agreements with provisions on cybersecurity:

- African Continental Free Trade Agreement Digital Trade Protocol - Article 25 - Cybersecurity
- WTO Agreement on Electronic Commerce - Article 17 - Cybersecurity

Non-DCO Members:

The following agreements also contain provisions on cybersecurity:

- ASEAN Agreement on Electronic Commerce - Article 8 - Cybersecurity
- Australia-Singapore Digital Economy Agreement - Article 34 - Cybersecurity
- Australia-Singapore Free Trade Agreement - Chapter 14, Article 18 - Cooperation on Cybersecurity Matters
- Australia-United Kingdom Free Trade Agreement - Chapter 14, Article 14.20 - Cybersecurity
- China-New Zealand Free Trade Agreement Upgrade - Chapter 19, Article 13 - Cyber Security
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership - Chapter 14, Article 14.16 - Cooperation on Cybersecurity Matters
- Digital Economy Partnership Agreement - Cybersecurity Cooperation - Article 1 - Cybersecurity Cooperation
- India-United Arab Emirates Comprehensive Economic Partnership Agreement - Chapter 9, Article 9.19 - Cyber Security
- Iceland-Liechtenstein-Norway-United Kingdom Free Trade Agreement - Chapter 4, Article 4.15 - Cybersecurity
- Korea-Singapore Digital Partnership Agreement - Article 14.22 - Cybersecurity Cooperation
- Peru-Australia Free Trade Agreement - Chapter 13, Article 13.15 - Cooperation on Cybersecurity Matters
- Regional Comprehensive Economic Partnership - Chapter 12, Article 12.13 - Cyber Security
- Singapore-New Zealand Closer Economic Partnership Upgrade - Chapter 9, Article 9.17 - Cooperation on Cybersecurity Matters

- United Kingdom-New Zealand Free Trade Agreement - Chapter 15, Article 15.18 - Cooperation on Cyber Security Matters
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-Q - Cyber Security
- United Kingdom-Singapore Digital Economy Agreement - Article 8.61-L - Cyber Security
- United States-Mexico-Canada Agreement - Chapter 19, Article 19.15 - Cybersecurity
- United States-Japan Digital Trade Agreement - Article 19 - Cybersecurity

ARTIFICIAL INTELLIGENCE

International Trends

Provisions on artificial intelligence are rare in digital trade agreements. The novelty of this issue reflects both the importance of artificial intelligence for digital trade and the will of governments to nurture its development and address the challenges it brings. The currently existing provisions can be grouped into three models, based on their detail and directness in the pursuit of cooperation: short endeavour provisions, long endeavour provisions, and endeavour and cooperate provisions.

The first model are short provisions in which parties commit to endeavour to collaborate. The provisions first recognize the growing importance of artificial intelligence and the economic and social importance to develop ethical and governance frameworks. In view of the cross-border nature of the digital economy, the provisions acknowledge the benefits of the international alignment of frameworks. Then, the provisions include "shall endeavour" language, urging that parties promote the adoption of artificial intelligence governance frameworks. In this process, parties are to take into consideration both internationally recognised principles and guidelines, including explainability, transparency, fairness and human-centred values. One provision additionally specifies that this is to occur through relevant regional, multilateral, and international fora. This provision further calls for the promotion of dialogue and experience sharing on regulations, policies and initiatives relating to artificial intelligence. *Example: Korea-Singapore Digital Partnership Agreement.*

The second model are long provisions in which parties commit to endeavour to cooperate. This model similarly acknowledges the relevance of artificial intelligence, as well as other emerging technologies, including distributed ledger technologies, digital twins, immersive technologies and the Internet of Things. The model then includes "shall endeavour" language in two regards. First, the development of governance frameworks that take into account the international principles and guidelines outlined above. In addition, the parties recognize the importance of principles of international bodies, risk-based regulation, and technological interoperability and neutrality. Second, the cooperation on matters related to artificial intelligence and emerging technologies with respect to digital trade. Specifically, such cooperation "may include" the exchange of information and best practices, the cooperation on issues related to artificial intelligence, the promotion of collaboration across research and industry, and the active participation in international fora on matters of trade and artificial intelligence. *Example: United Kingdom-Singapore Digital Economy Agreement.*

The third model builds on the previous endeavours but further adds "shall cooperate" language. Similarly to the other provisions, this model recognises the importance of artificial intelligence and its governance. Again, the parties "shall endeavour" to collaborate on such governance frameworks, taking into account international principles and principles. Furthermore, the parties "shall cooperate" by sharing research and industry practices, promoting the responsible use of artificial intelligence, and encouraging commercialization opportunities and collaboration between research and industry. This presents a more direct commitment to cooperation. *Example: Australia-Singapore Digital Economy Agreement.*

DCO Members Approaches

The DCO Member States are not involved in any agreements with provisions on artificial intelligence.

Conclusion

Provisions on artificial intelligence in digital trade agreements are rare and focused on cooperation, rather than national regulation. The provisions consistently recognize the importance of artificial intelligence, its governance, and international alignment thereon. The core of the provisions are commitments to endeavour to cooperate, mainly on developing governance frameworks guided by international principles. One model provides a direct commitment to cooperation, focused mainly on information sharing, the promotion of responsible artificial intelligence use, and cooperation between research and industry.

At the international level, the DCO Member States are not involved in any agreements covering artificial intelligence. The DCO offers Member States a forum to exchange experiences, paving the way for enriched discussions and the discovery of future collaboration areas.

Digital Trade Agreements with Commitments on Artificial Intelligence

DCO Members:

The DCO Member States are not involved in any agreements with provisions on artificial intelligence.

Non-DCO Members:

The following agreements contain provisions on artificial intelligence:

- Australia-Singapore Digital Economy Agreement - Article 31 - Artificial Intelligence
- Digital Economy Partnership Agreement - Article 8.2 - Artificial Intelligence

SOURCE CODE

International Trends

Source code provisions in digital trade agreements are fairly common, but not widespread. Aiming to protect intellectual property and trade secrets, these provisions share a core prohibition for mandatory source code sharing. Variations persist, however, regarding the scope of provisions and the exception mechanisms they provide.

The main commonality between source code provisions is that they prohibit parties from requiring the transfer or access to source code as a mandatory condition for market access. This includes software import, distribution, sale, or use. Although the core of these provisions is thus similar, differences emerge regarding the scope. Specifically, certain provisions:

- limit the prohibition to mass-market software, excluding software used for critical infrastructure. Example: Comprehensive and Progressive Agreement for Trans-Pacific Partnership.
- explicitly include algorithms expressed in source code within the scope of the prohibition. Others explicitly include source code of software contained in a product. Example: United States-Mexico-Canada Agreement.
- explicitly clarify that the prohibition does not apply to voluntary transfers of source code, such as those made on a commercial basis or under open-source licenses. Example: United Kingdom-Singapore Digital Economy Agreement.

Further differences emerge regarding exception mechanisms, since certain provisions:

- allow exceptions for regulatory bodies or judicial authorities to require access for specific purposes such as investigations or enforcement actions. Example: Australia-Singapore Digital Economy Agreement.
- provide exceptions for court orders concerning the enforcement of competition rules and intellectual property rights. Example: European Free Trade Association-Moldova Free Trade Agreement.
- provide exceptions for the protection of essential security interests. Specifically, this relates to the procurement of arms, ammunition or war materials, and procurement indispensable for national security or defence purposes. Example: Australia-Indonesia Comprehensive Economic Partnership Agreement.

DCO Members Approaches

The DCO Member States are involved in several agreements including provisions on source code, which all follow the model outlined above:

- EU-Chile Advanced Framework Agreement
- EU-New Zealand Free Trade Agreement
- EU-Mexico Trade Agreement
- EU-United Kingdom Trade and Cooperation Agreement
- EU-Japan Economic Partnership Agreement
- African Continental Free Trade Agreement Digital Trade Protocol

Conclusion

Source code provisions in digital trade agreements consistently prohibit parties from requiring the transfer or access to source code as a mandatory condition for market access. Although the core of these provisions is thus similar, differences emerge regarding the scope and exception mechanisms. The scope varies in terms of what types of software are covered, whether algorithms expressed in source code are protected, and if voluntary transfers are explicitly carved out. Exception mechanisms vary regarding the justifications and competent authorities that can nevertheless request access to source code, often to enforce laws and protect national security.

At the international level, the DCO Member States are involved in several agreements covering source code, using the same model. Member States can leverage the DCO as a hub for sharing experiences, promoting informed dialogue and identifying potential avenues for alignment.

Digital Trade Agreements with Commitments on Source Code

DCO Members:

The DCO Member States are involved in the following agreements with provisions on source code:

- African Continental Free Trade Agreement Digital Trade Protocol - Article 24 - Source Code
- EU-Chile Advanced Framework Agreement - Chapter 19, Article 19.12 - Prohibition of Mandatory Transfer of or Access to Source Code
- EU-Japan Economic Partnership Agreement - Chapter 8 Section F, Article 8.73 - Source Code
- EU-Mexico Trade Agreement - Chapter 16, Article 9 - Source Code
- EU-New Zealand Free Trade Agreement - Chapter 12, Article 12.11 - Transfer of or Access to Source Code
- EU-United Kingdom Trade and Cooperation Agreement - Title III, Article 207 - Transfer of or Access to Source Code

Non-DCO Members:

The following agreements also contain provisions on source code:

- Australia-Hong Kong Free Trade Agreement - Chapter 11, Article 11.12 - Treatment of Source Code
- Australia-Indonesia Comprehensive Economic Partnership Agreement - Chapter 13, Article 13.13 - Source Code
- Australia-Singapore Digital Economy Agreement - Article 28 - Source Code
- Australia-Singapore Free Trade Agreement - Chapter 14, Article 19 - Source Code
- Australia-United Kingdom Free Trade Agreement - Chapter 14, Article 14.18 - Source Code
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership - Chapter 14, Article 14.17 - Source Code
- European Free Trade Association-Moldova Free Trade Agreement - Chapter 5, Article 5.14 - Transfer of or Access to Source Code
- Iceland-Liechtenstein-Norway-United Kingdom Free Trade Agreement - Chapter 4, Article 4.10 - Source Code
- Korea-Singapore Digital Partnership Agreement - Chapter 14, Article 14.19 - Source Code
- Peru-Australia Free Trade Agreement - Chapter 13, Article 13.16 - Source Code
- Singapore-New Zealand Closer Economic Partnership Upgrade - Chapter 9, Article 9.13 - Source Code
- United Kingdom-Japan Comprehensive Economic Partnership Agreement - Chapter 8 Section F, Article 8.73 - Source Code
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-P - Source Code
- United Kingdom-Singapore Digital Economy Agreement - Article 8.61-K - Source Code
- United States-Mexico-Canada Agreement - Chapter 19, Article 19.16 - Source Code
- United States-Japan Digital Trade Agreement - Article 17 - Source Code

SMEs AND DIGITAL INCLUSION

International Trends

Digital inclusion provisions in trade agreements are relatively novel and rare. Existing provisions follow the same cooperative model, sharing several core components with slight variations in bindingness. Recently, a new binding model has emerged, although it is yet to enter into force.

Cooperative provisions first articulate the foundational principle through non-binding language, "recognising" or "acknowledging" the importance of digital inclusion so that all people and businesses can participate in, contribute to, and benefit from the digital economy. The provisions universally recognize that certain groups face greater barriers to participation, using non-binding language to emphasize the need for tailored approaches. However, they differ in how they specify these groups: Some explicitly reference indigenous peoples, persons with disabilities, rural populations, and low socio-economic groups, while others remain more general.

Cooperative provisions then establish cooperation as the primary mechanism for promoting digital inclusion. The basic commitment to cooperate typically uses binding language ("shall"), while the specific cooperative activities are not enumerated bindingly, but rather with "may include." Specifically, these activities consistently encompass:

- Sharing experiences and best practices;
- Identifying and addressing barriers to digital trade opportunities;
- Improving digital skills and access to online tools;
- Developing methods for data collection and analysis on digital inclusion; and
- Exchanging knowledge and experts.

In addition, some cooperative provisions cover specific areas such as labour protection and SME participation. On SMEs, one provision establishes a binding requirement to foster cooperation on digital trade between SMEs and the parties, encourage SMEs' participation in platforms linking them to international stakeholders, and share best practices in areas that help SMEs adapt to digital trade.

Furthermore, cooperative provisions vary regarding the implementation mechanisms, with some establishing binding obligations for cooperation through specific agencies and stakeholders. Certain provisions extend to the international dimension, requiring participation in international fora, such as the World Trade Organization. Typically, these provisions recognize the digital divide between countries while others focus on domestic inclusion. *Example: United Kingdom-New Zealand Free Trade Agreement.*

On the other hand, the binding model takes a more direct approach, establishing binding obligations without preliminary context-setting or aspirational statements. Unlike the cooperative provisions that mix binding and non-binding elements, the binding model formulates one core obligation ("shall") and then lists specific required activities. The core obligation is to promote and facilitate the inclusion and participation of women, youth, indigenous peoples, rural and local communities, persons with disabilities, and other underrepresented groups in digital trade. The activities partly overlap with those in the cooperative provisions (sharing best practices, increasing digital skills, and addressing barriers). In addition, they extend to infrastructure, for instance regarding the improvement of connectivity and provision of affordable internet. *Example: African Continental Free Trade Agreement Digital Trade Protocol - Article 30.*

DCO Members Approaches

The DCO Member States are involved in one trade agreement that covers SMEs and Digital Inclusion. The African Continental Free Trade Agreement Digital Trade Protocol follows the second model, as outlined above.

Conclusion

Existing provisions on digital inclusion follow a cooperative model that sets the aspirational goal of digital inclusion and establishes binding commitments to cooperate thereon. The specific cooperative activities largely overlap, from sharing best practices, to addressing barriers, to improving digital skills, to exchanging knowledge. Some cooperative provisions cover further activities, such as labour protection and SME participation. Furthermore, cooperative provisions vary regarding the concrete implementation mechanisms, with some specifying pertinent agencies and international fora.

Finally, a novel model is emerging, taking a more direct approach to establish binding obligations, but is yet to enter into force.

At the international level, the DCO Member States are involved in one agreement covering digital inclusion, relying on the binding model. Member States can utilize the DCO to exchange ideas and experiences, creating opportunities for more informed dialogue and identifying shared priorities for coordination.

Digital Trade Agreements with Commitments on SMEs and Digital Inclusion

DCO Members:

The DCO Member States are involved in one agreement with a provision on digital inclusion:

- African Continental Free Trade Agreement Digital Trade Protocol - Article 30 - Digital Inclusion

Non-DCO Members:
The following agreements also contain provisions on digital inclusion:

- Digital Economy Partnership Agreement - Module 11 - Digital Inclusion
- United Kingdom-Singapore Digital Economy Agreement - Article 8.61-P - Digital Inclusion
- United Kingdom-Ukraine Digital Trade Agreement - Article 132-T - Digital Inclusion
- United Kingdom-New Zealand Free Trade Agreement - Chapter 15, Article 15.20 - Digital Inclusion

Digital
Cooperation
Organization

@dcorg | www.dco.org