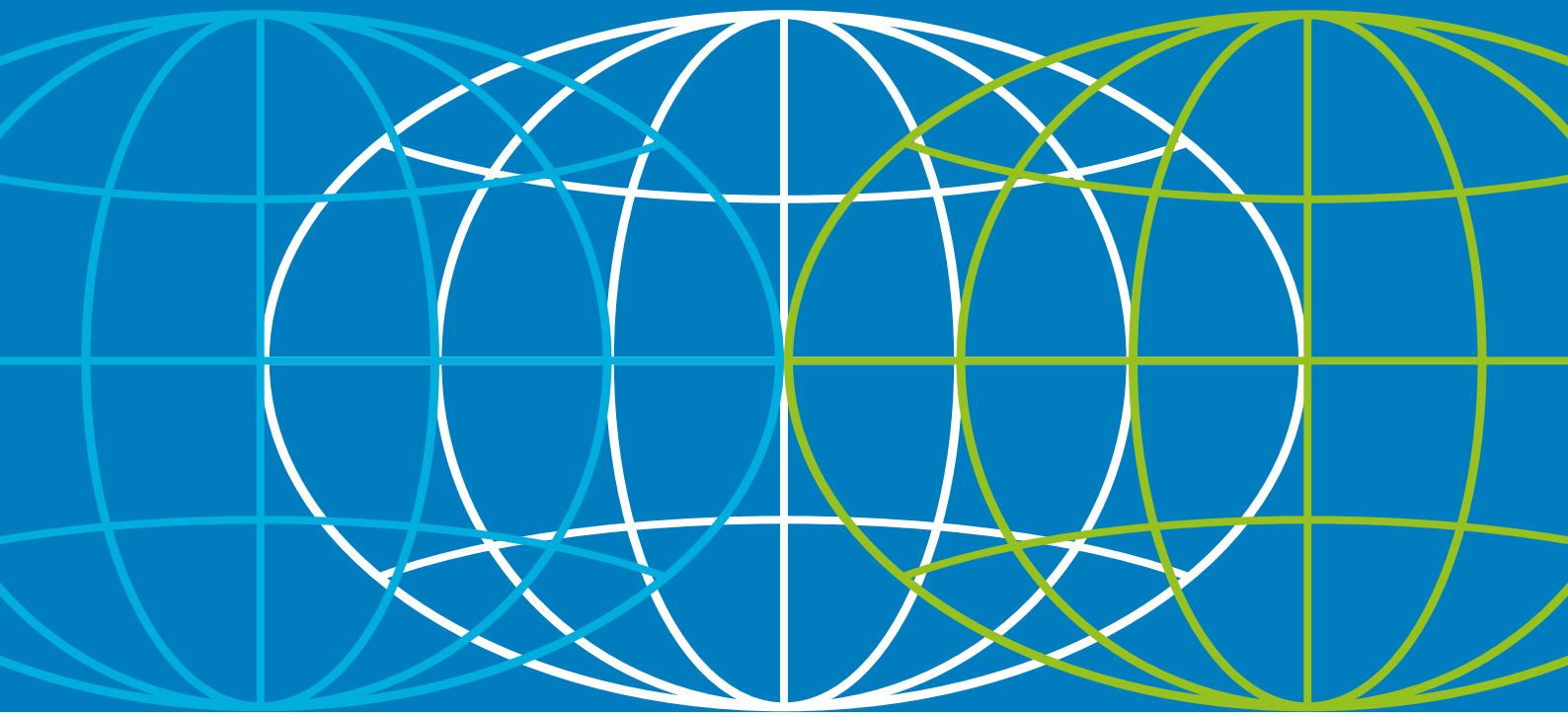
Asia-Pacific
Economic Cooperation



APEC Digital Trade Provisions Handbook

APEC COMMITTEE ON TRADE AND INVESTMENT

FEBRUARY 2026

Acknowledgements

APEC Project: CTI 01 2025S

Produced by

Danny Burrows (TradeWorthy Inc.)
info@trade-worthy.com

Joshua Meltzer (Policyware LLP)
info@policyware.org

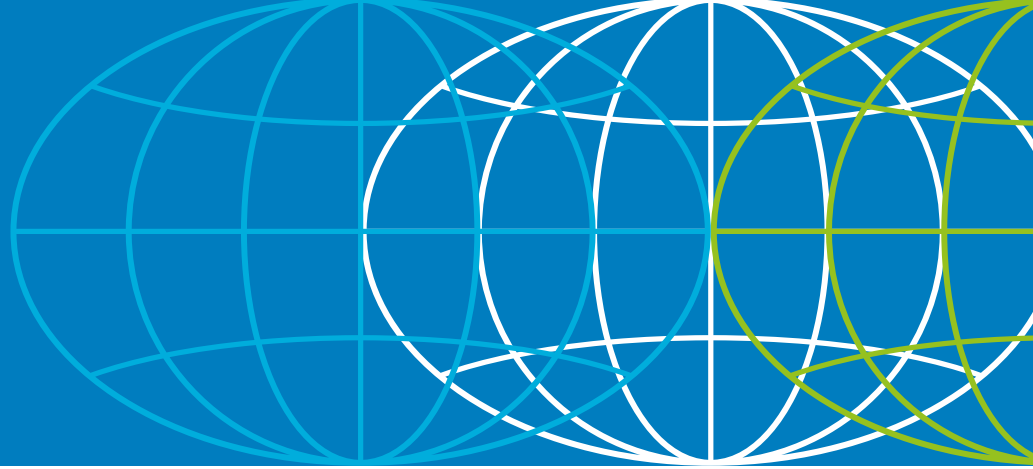
For

Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Email: info@apec.org
Website: www.apec.org
© 2026 APEC Secretariat
APEC#226-CT-03.1

This Handbook was funded by the
Australian Government through the
Department of Foreign Affairs and Trade (DFAT)

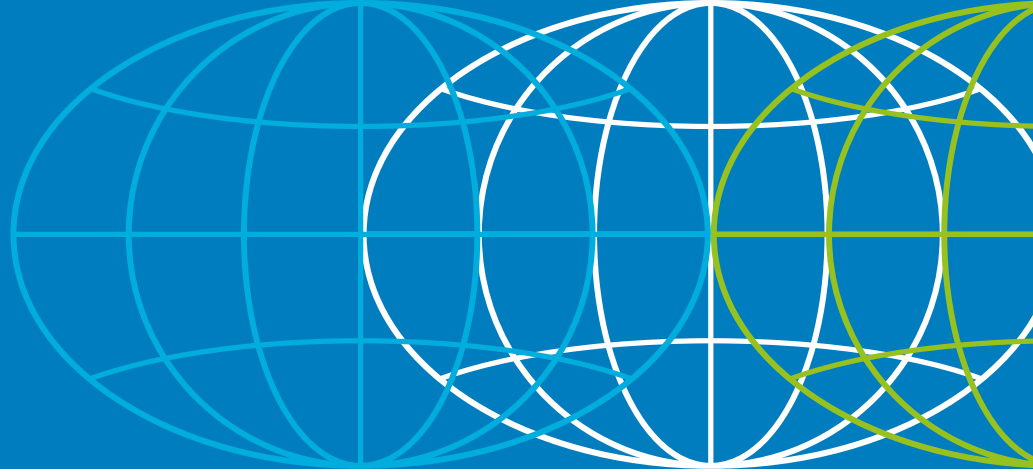
Table of Contents

Glossary of Terms



Acronym	Meaning
AANZFTA	ASEAN-Australia-New Zealand Free Trade Area
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DEPA	Digital Economy Partnership Agreement
DFTP	Digital Free Trade Portal
ECA	WTO Joint Statement Initiative on E-Commerce Agreement
ECIPE	European Centre for International Political Economy
FTA	Free Trade Agreement
GDPR	General Data Protection Regulation (EU)
ICT	Information and Communication Technology
IMF	International Monetary Fund
JSI	Joint Statement Initiative
MFN	Most-Favoured Nation
MSMEs	Micro, Small and Medium Enterprises
OECD	Organisation for Economic Co-operation and Development
PDF	Portable Document Format
PPD	Public-Private Dialogue
RCEP	Regional Comprehensive Economic Partnership
RTA	Regional Trade Agreement
SME	Small and Medium Enterprise
TFA	Trade Facilitation Agreement
UNCTAD	United Nations Conference on Trade and Development
VAT	Value Added Tax
WTO	World Trade Organization

Chapter 1
International Regulation of Digital Trade



1.1 What is digital trade?

Digital trade refers to all cross-border transactions that are either digitally ordered (e.g., cross-border e-commerce), digitally facilitated (e.g., by online platforms), or digitally delivered, though definitions differ.[1] This encompasses a wide range of activities, including e-commerce transactions, digital services delivered over the internet, and the cross-border flows of information including transmission of digital content such as software, video, music, and data (depending on the preferred definition).

1.2 Why does digital trade matter?

Digital trade matters because it powers modern commerce and creates new economic opportunities across borders. It reduces transaction costs, simplifies business processes, and enables firms—especially small and medium-sized enterprises (SMEs)—to participate in global value chains. By using digital platforms, cloud services, and data analytics, businesses can serve domestic and international customers, manage logistics, and receive payments with unprecedented efficiency.

At the economy level, digital trade supports economic growth (see 1.3 below) and productivity. Implementation of key provisions such as cross-border data flows, prohibition of data localisation, and recognition of electronic contracts help to reduce trade frictions

1 OECD definition refers to all cross-border transactions that are either digitally ordered (e.g., cross-border e-commerce), digitally facilitated (e.g., by online platforms), or digitally delivered. US International Trade Commission refers to, "The delivery of products and services over the internet by firms in any industry sector, and of associated products such as smartphones and internet-connected sensors... it excludes the value of sales of physical goods ordered online, as well as physical goods that have a digital counterpart (such as books, movies, music, and software sold on CDs or DVDs)."

(for example, using electronic trade documentation), and improve competitiveness.

For individual companies, especially those in developing economies, digital trade enables participation in global commerce without the need for physical infrastructure or intermediaries. Digital tools also enhance productivity—automating everything from invoicing to customs paperwork—and increase resilience by allowing remote operations and online service delivery. Lastly digital trade supports enhanced inclusivity, by lowering entry barriers for Indigenous and women entrepreneurs, rural SMEs, and new startups.

1.3 What is the digital trade opportunity for APEC economies?

For APEC economies, digital trade offers a powerful opportunity to strengthen economic growth, diversify exports, and increase participation in global markets. The region's strong digital uptake, dynamic start-up ecosystems, and extensive cross-border commercial links make APEC uniquely placed to benefit from rules-based digital integration.

Recent modelling by APEC shows that the benefits of adopting high-standard digital trade rules are significant. According to a 2023 APEC study[2], full adoption of provisions like cross-border data flow guarantees, prohibitions on data localisation, and recognition of digital signatures could boost real GDP across APEC economies by up to **USD 1.46 trillion** over 10 years. Exports could rise by **USD 785 billion,** with services trade accounting for the largest share of the gain. The study further estimates that employment across the region could grow by **around 6.65 million jobs**—particularly in digitally-intensive services and trade-related occupations.

These benefits are particularly compelling for developing APEC economies. Digital trade reduces traditional barriers – like limited logistics infrastructure – by allowing companies to engage in remote service delivery, digital marketing, and online sales. Smaller firms, including Indigenous, women- and youth-led enterprises, can reach international customers through cost-effective online communication and sales platforms, provided supportive legal and policy frameworks are in place.

The strategic value of digital trade also lies in its ability to deepen regional integration. Digital provisions – such as those related to privacy, cybersecurity, and e-invoicing

2 The Economic Impact of Adopting digital Trade Rules: Evidence from APEC Member Economies, CTI report, April 2023.

– can improve alignment of regulation across different markets. This, in turn, reduces the compliance burden for companies that want to grow across international borders.

1.4 How Do Economies Cooperate on Digital Trade Regulation?

As digital trade becomes an increasingly central part of the global economy, economies are cooperating to build common rules that enable secure, predictable, and inclusive digital transactions. One of the primary ways this cooperation takes place is through trade agreements—either as part of broader Free Trade Agreements (FTAs) or as stand-alone Digital Economy Agreements (DEAs). These digital trade commitments seek to reduce regulatory fragmentation, promote interoperability, and ensure trust and certainty for digital transactions.

Digital trade provisions can serve both **domestic and cross-border** purposes. Domestic-facing commitments include provisions that enhance consumer protection online, ensure data privacy, or promote the legal recognition of electronic contracts and signatures. These rules provide clarity and assurance for businesses and users within an economy's own borders and consumers transacting with that economy across international borders, but are also designed to align with international standards, such as on electronic transactions and signatures. Similarly, provisions primarily focused on cross-border treatment of digital goods and services seek to align practices internationally and create a predictable and aligned regulatory regime for business. These provisions include rules on **cross-border data transfers, non-discrimination of digital products,** and provisions **on customs duties for electronic transmissions.**

Digital trade provisions play a critical role in dismantling the high and divergent barriers identified by the OECD's Digital Services Trade Restrictiveness Index. The Digital STRI finds that **restrictions on digital trade have grown by 25 percent between 2014 and 2023** and remain highly uneven across economies, driven in particular by measures on cross-border data flows and levies on digital services, among others. Digital trade provisions can support reduction in digital trade barriers through clear and binding commitments, and by aligning domestic policies with international standards that reduce uncertainty for businesses operating in the digital sector across international borders.

Digital trade provisions in trade agreements can also be distinguished by their legal force. **Hard provisions**

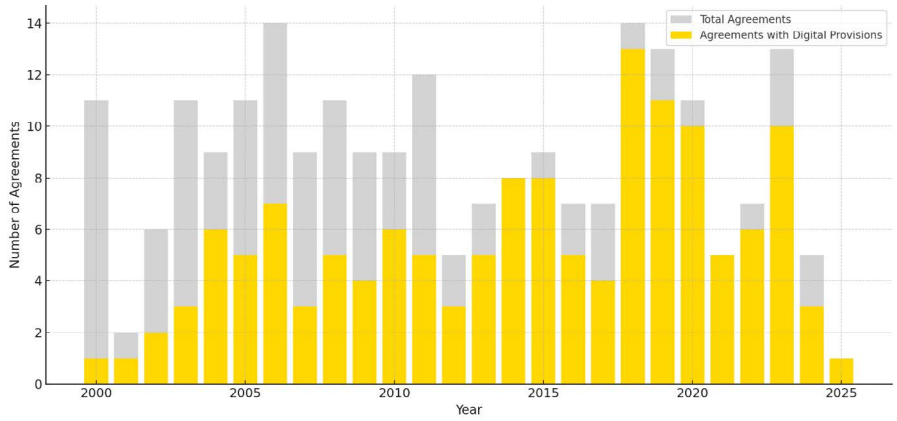
are binding commitments, typically also enforceable under the agreement's dispute settlement mechanism. Examples include obligations not to require data localisation or to allow cross-border data flows, often with specific conditions or exceptions. **Soft (sometimes known as 'hortatory') provisions,** by contrast, are more flexible and are usually framed in terms of cooperation, best endeavours, or shared principles. These might include commitments to exchange best practices on cybersecurity, or to promote interoperability in e-invoicing systems.

1.5 Evolution of Digital Trade Provisions among APEC Economies

Over the past two decades, digital trade has moved from a peripheral issue to a central feature of trade agreements involving APEC economies. This shift is clearly illustrated by two key trends: the **wider adoption** of digital trade provisions across agreements and the **increasing depth and complexity** of those commitments.

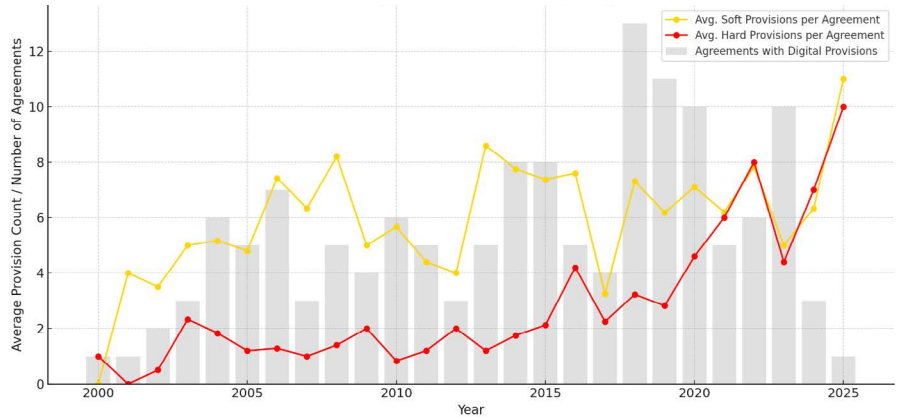
The first graph below shows a steady rise in the number of agreements (involving at least one APEC member) that include one or more provisions on digital trade —rising from a handful in the early 2000s to over a dozen by the late 2010s. Before 2015, around half of all agreements contained one or more digital trade provisions, though this percentage is now closer to 90%.

Proportion of Trade Agreements with Digital Provisions by Year (APEC)



The graph below reveals another important dimension of this evolution: **depth.** Newer agreements are not only more likely to contain digital trade provisions—they also contain more of them. On average, each agreement now covers a broader array of digital issues, such as data protection, e-payments, e-invoicing, and AI governance. The steady rise in hard commitments indicates a maturing digital rulebook that is more precise, enforceable, and aligned with commercial realities.

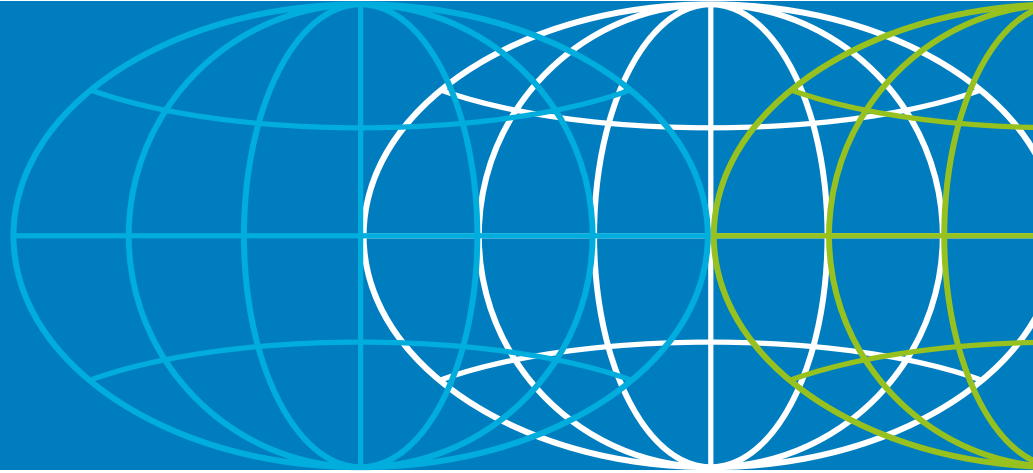
Average Number of Digital Trade Provisions per Agreement (APEC)



Both **soft provisions** (which support cooperation or best efforts) and **hard provisions** (which are binding and enforceable) have expanded significantly. This suggests growing confidence in embedding digital rules in legally binding instruments, while also maintaining space for experimentation and collaboration.

Together, these trends underscore how APEC economies are not just adopting digital trade rules—they are helping to shape a more sophisticated and coherent framework for governing the digital economy across the region. This evolution reflects the growing economic significance of digital trade and the need for predictable, interoperable, and forward-looking regulatory environments.

Chapter 2
Using this Handbook on Digital Trade Provisions



2.1 Purpose and Structure of the Handbook

This handbook has been developed as a practical guide for trade negotiators, policymakers, and regulatory agencies across APEC economies to better understand and navigate digital trade provisions in international agreements. It supports informed policy decisions, promotes regulatory coherence, and enhances regional capacity for engaging in digital trade negotiations.

The handbook is organised by specific provisions that appear frequently in digital trade or e-commerce chapters of trade agreements. Each section addresses a single topic—such as electronic invoicing, data protection, or cybersecurity—outlining what the provision is, how it typically works, and why it matters. Case examples and data visualisations help illustrate how different APEC economies have adopted and developed these provisions over time. In some cases, the handbook also highlights international frameworks or best practice approaches that can guide future negotiations or reforms.

2.2 Core Digital Trade Provisions Covered

The handbook focuses on a set of commonly used digital trade and related provisions. The provisions are arranged into themes, as follows:

A. Trade Facilitation: provisions that support the freer flow of digital trade and alignment of standards across economies

B. Building Trust: provisions that support consumer confidence in digital trade

C. Data Flows: provisions that govern the flow of data that underpins digital trade

D. Emerging Issues: provisions on rapidly advancing elements of the digital economy

E. General & Security Exceptions and Scope: traditional trade provisions that provide policy flexibility for exceptional purposes.

These provisions are numbered for easy reference, along with a short description of its main function as follows:

A. **Trade Facilitation**	**Description**
A1: Paperless trading	Promotes the use of digital documentation for trade processes
A2: E-invoicing	Supports standardised digital billing systems across borders
A3: Electronic authentication and signatures	Facilitates legal recognition of electronic signatures and digital verification
A4: Digital ID	Facilitates interoperability and secure use of digital identity
A5: Customs duties on electronic transmissions	Permanently or temporarily prohibits tariffs on digital content such as software, media, or data
A6: Non-discrimination between digital products	Ensures equal treatment of digital products and services from foreign providers
A7: Access to and use of internet services and applications	Principles on Access to and Use of the Internet for e-commerce/digital trade
A8: Electronic payments	Encourages interoperability and efficiency of digital financial transactions

B. **Building Trust**	
B1: Protection of online personal information	Ensures secure and accountable handling of personal data online
B2: Cybersecurity	Encourages cooperation on addressing digital threats and crimes, and strengthening systems
B3: Consumer protection	Safeguards digital consumers through fair practices and dispute mechanisms
B4: Unsolicited commercial messages	Regulates unsolicited digital marketing and bulk communications (Spam)
C. **Data Flows**	
C1: Cross-border transfers of information	Regulates the international movement of data for business operations
C2: Data localisation	Regulates requirements to store or process data only within an economy
C3: Access to source code	Regulates mandatory transfer of proprietary software source code
D. **Emerging Issues**	
D1: Artificial Intelligence	Cooperation and responsible use of AI technologies
D2: Cryptography	Regulates requirements for handling of cryptographic features e.g. algorithms
D3: Review Clause	A commitment to review the inclusion of new/further commitments on digital trade
E. **General & Security Exceptions and Scope**	
E1:	Exceptions provisions provide economies with scope to adopt measures contrary to binding commitments.In addition, some agreements limit the scope of digital trade provisions or exclude certain industry sectors

Each of these provisions is analysed using examples from agreements which include at least one APEC economy, and complemented by data on their legal form—whether they are binding obligations (hard provisions) or best-endeavour commitments (soft provisions), as explained below.

For each provision, the handbook provides:

(i) a simple **explanation** of the issue

(ii) the **economic benefits** arising in relation to the issue

(iii) the **main barriers** arising in relation to that issue, and

(iv) how **trade agreements** deal with the issue.

For each provision, the handbook includes a sample provision with analysis. These are typically drawn from agreements that apply to multiple APEC economies.

The Handbook also provides a **Policy Checklist** to assist negotiators in selection and drafting of digital trade provisions. The Policy Checklist is designed as a practical decision-making tool, enabling users to **work systematically through key policy questions.** Each question represents a common issue that arises in digital trade negotiations, while the accompanying considerations outline relevant factors, precedent approaches in other agreements, and possible policy trade-offs.

The Policy Checklist's structured format allows negotiators to tailor provisions to their own economy's regulatory context while remaining informed by international practice. By making explicit the rationale behind each provision type, the Policy Checklist helps negotiators assess options more confidently and consistently.

2.3 Data Sources

This handbook provides original analysis of existing provisions in agreements involving APEC economies, and draws on a number of sources for quantitative analysis. These include the **TAPED (Trade Agreement Provisions on E-commerce and Data)** dataset[3], which systematically codes digital trade provisions across hundreds of trade agreements. For this handbook, provisions from agreements involving at least one APEC economy were extracted and analysed across time (based on the year they were signed). Each commitment is coded as:

- **1** – Soft commitment (best endeavours, policy cooperation, aspirational)
- **2** – Hard commitment (binding and enforceable obligations)

This coding allows the handbook to track trends in the number and depth of digital trade commitments by APEC economies over the past two decades.

For the purposes of creating graphs throughout this Handbook, the TAPED dataset was filtered for agreements involving at least one APEC economy and at least one digital trade provision from the list provided in Chapter 2.

The handbook also incorporates insights from the **APEC CTI study on the Economic Impact of Adopting Digital Trade Rules (2023), referred to herein as the "APEC Impact Study".** That study used economic modelling to quantify the benefits of digital trade reforms. For example, implementing a package of digital trade provisions based on APEC best practices was projected to increase GDP in some APEC economies by up to 3.7%, with the greatest benefits accruing to smaller and more digitally active economies. These findings help make the case for prioritising ambitious and cooperative digital trade commitments.

3 Mira Burri, María Vásquez Callo-Müller and Kholofelo Kugler, TAPED: Trade Agreements Provisions on Electronic Commerce and Data, available at: https://unilu.ch/taped, accessed in July 2025.

Section A:
Trade Facilitation

A1: Paperless Trading

What is paperless trading?

Paperless trading refers to the use of electronic forms instead of paper forms that are needed for international trade, and the acceptance of electronic forms as equivalent to paper forms.

What are the economic benefits from paperless trading?

Analysis of the economic benefits of trade commitments on paperless trade found that digitally delivered trade flows increased by 17% in the two years after such a commitment.

Commitments on paperless trading in trade agreements reduce costs and speed up cross-border commerce by replacing physical paperwork with electronic documentation. The ability to submit documents electronically allows customs and other government agencies to process more quickly than the documentation needed to enable trade, leading to shorter clearance times and fewer delays. By enabling online submission of trade documents, paperless trading lowers barriers for firms in remote or developing areas to participate in international trade. Paperless trading also enhances supply chain resilience by facilitating real-time information sharing. A 2023 APEC study found that nearly all economies have implemented digital solutions for customs documentation, and a growing number are expanding into digitally-enabled business-to-government and business-to-business trade processes.[4]

4 APEC (2023), Final Report on the Implementation of the APEC Paperless Trading Individual Action Plan, Committee on Trade and Investment, CTI 225, https://www.apec.org/docs/default-source/Publications/2023/12/Final-Report-on-the-Implementation-of-the-APEC-Paperless-Trading-Individual-Action-Plan/225_cti_paperless-trade.pdf

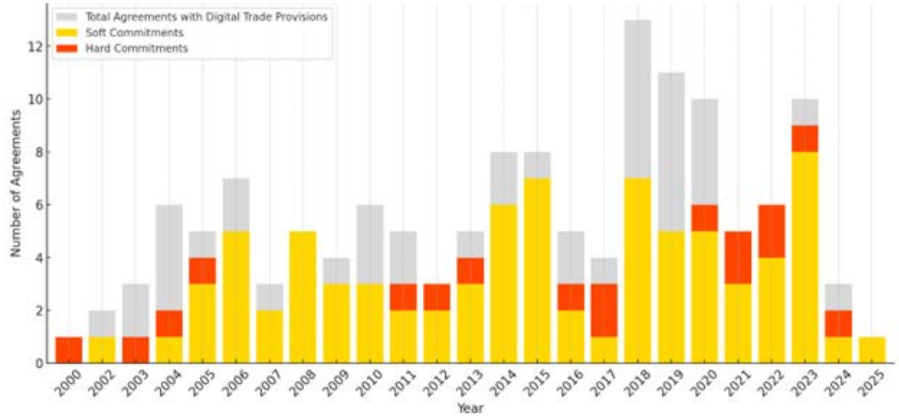
What are the main barriers to paperless trading?

There are various barriers to economies accepting paperless trading across borders. For one, there is still a domestic legal/regulatory barrier to accepting electronic documents as equivalent to paper documents. Poor ICT infrastructure can also limit the ability of businesses and governments to adopt paperless systems.

APEC economies also often have different rules on recognizing electronic documents and signatures. There is also a lack of mutual recognition among APEC economies that allows an electronic document in one economy to be accepted as valid in another APEC economy. Achieving interoperability requires coordination on standards and procedures across borders. Relatedly, there are technical challenges, such as where customs systems use incompatible data formats or standards. This includes ensuring having in place systems and the capacity to deal with data breaches, fraud, cybersecurity risks.

Paperless trading in trade agreements

Paperless Trading Commitments vs. Total Digital Trade Agreements by Year



Core provisions as seen in CPTPP, RCEP and the WTO Agreement on Electronic Commerce (ECA) are to make documents issued by customs authorities available in electronic format and to have these electronic documents treated as equivalent to paper documents. Other commitments include agreement to cooperation in international fora to enhance acceptance of digital documents.

Sample Paperless Trading Provision

This sample Paperless Trading provision is taken from the **WTO Agreement on Electronic Commerce.**

WTO JSI Article 8: Paperless Trading

8.2 With a view to creating a paperless border environment for trade in goods, the Parties recognize the importance of eliminating paper forms and documents required for importation, exportation, or transit of goods. To this end, each Party is encouraged to eliminate paper forms and documents, as appropriate, and transition towards using forms and documents in data-based formats.

8.3 Each Party shall make any form issued or controlled by its customs authority for importation, exportation, or transit of goods through its territory available to the public in electronic format.

8.4 Each Party shall endeavour to make any form issued or controlled by any government agency other than its customs authority for importation, exportation, or transit of goods through its territory available to the public in electronic format.

8.6 Each Party shall endeavour to make instructions for the submission in electronic format of the forms referred to in paragraphs 3 and 4 available through the Internet.

8.7 Each Party shall accept any form issued or controlled by its customs authority and, as appropriate, supporting documentation, required by its customs authority for importation, exportation, or transit of goods through its territory submitted in electronic format as the legal equivalent of the paper version of those documents.

Overall goal and commitment to transition towards paperless docs

Binding commitment applied to customs authorities

More hortatory commitment for other government agencies

Binding commitment to accept, but limited to its own customs authorities

WTO JSI Article 8

8.8 Each Party shall endeavour to accept any form issued or controlled by any government agency other than its customs authority and, as appropriate, supporting documentation, required by any government agency other than its customs authority for importation, exportation, or transit of goods through its territory submitted in electronic format as the legal equivalent of the paper version of those documents.

8.9 No Party shall be required to apply paragraphs 7 or 8 if:

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

(b) doing so would reduce the effectiveness of the customs or other trade procedures required for importation, exportation, or transit of goods through its territory.

8.11 The Parties shall endeavour to cooperate, as appropriate, in international fora to promote the use of electronic forms and documents required for importation, exportation, or transit of goods.

8.12 Recognizing that the use of an international standard for utilization of electronic forms and documents required for importation, exportation, or transit of goods can facilitate trade, each Party shall endeavour to take into account, as appropriate, standards of, or methods agreed by, relevant international organizations.

Hortatory commitment to accept electronic forms as equivalent from all other government agencies

Limits to the commitment

Hortatory commitment to cooperate

Hortatory commitment to "take into account" standards – supports interoperability and harmonization

Policy Checklist: Paperless Trading

Question	Consideration
Should a provision on paperless trading be included?	This is a threshold question. The database shows that Paperless Trading provisions have appeared since 2000 (the first year of data collected) and are now broadly included as seen in the WTO ECA, CPTPP, RCEP and DEPA.
Should it include commitments on making trade administration documents available in electronic form	This core provision could either be binding (e.g. in the WTO ECA or qualified (e.g. shall work towards) as used in CPTPP. It is somewhat common for this core provision to be binding.
Should it include a commitment to accept trade administration documents in electronic form as legally equivalent to the paper version?	This core provision could either be binding (e.g. shall) or qualified (e.g. endeavour to). It is somewhat common for this core provision to be binding.
Instead of a commitment on trade administration documents broadly, the WTO ECA distinguishes between document issues by customs authorities and those issues by other government agencies makes binding commitments to documents issued by other government agencies for import or export	Various FTAs apply a binding commitment to all trade administration documents. Under the WTO ECA, when it comes to customs authorities the commitment is binding, whereas for other agencies that issue documents related to trade, the commitment is hortatory.

Should it include a commitment to cooperate to promote paperless trading in international forum, as in the WTO ECA.	The WTO ECA includes this as a hortatory commitment
Whether to include a commitment to take into account international standards.	The WTO ECA and DEPA includes this as a hortatory commitment
How does this relate to previous commitments on Paperless Trading?	If your economy has previously committed to a position on paperless trading, ensure that the provisions are consistent unless a change in policy is desired

A2: E-invoicing

What is e-invoicing?

An e-invoice enables the digital exchange of standardised information between suppliers and buyers software using common standards and digital infrastructure such as the secure Peppol framework - an open international framework and set of standards to enable cross-border e-invoicing. A report by the APEC Committee on International Trade recommended Peppol standards for enabling e-invoicing interoperability [5], and some APEC economies such as Australia; New Zealand; and Singapore are already using Peppol to enable e-invoicing. E-invoicing enables a more efficient, accurate and secure way to send and receive invoices. E-Invoicing is therefore more than a digital invoice. It is also a way of providing standardized information that allows for automated business transactions between organizations. According to the Digital Economic Partnership Agreement (DEPA), electronic invoicing or e-invoicing "means the automated creation, exchange and processing of requests for payments between suppliers and buyers using a structured digital format".[6]

5 APEC Committee on Trade and Investment, "Interoperability of Electronic Invoicing systems in the APEC Region" Feb 2025
6 DEPA Article 2.1

What are the economic benefits from e-invoicing?

An interoperable e-invoicing system amongst APEC economies would produce a range of economic benefits. According to one estimate, there is an approximately USD 14 productivity benefit per e-invoice.[7] These benefits grow as adoption of e-invoicing grows. Specific benefits from e-invoicing are:

- Improved flow of information between customs and tax administrators that also fights tax fraud.
- More reliable and secure: e-invoicing exchanges such as through the secure Peppol network that reduces the risk of fakes, scams or ransomware attacks.
- E-invoicing reduces the risk of lost invoicing and provides greater control over who can view the invoice.
- Improved accuracy and data quality as e-invoices reduced errors arising from paper-based invoices and manual entry of data.
- Reduced payment times (estimated 5-7 days faster than traditional invoicing) that improves cash-flow for business.
- More environmentally friendly as it dispenses with the need for using paper and the resources used to manage invoices.

What are the main barriers to e-invoicing?

There are various barriers to using e-invoicing for international trade. The key ones are different approaches among APEC economies to the validity and approval of e-invoices, as well as a lack of common standards governing the format of the e-invoices, standards for identifications, as well as agreement on issues such as how long e-invoices need to be stored and in what medium. There are also different levels of uptake of e-invoicing among APEC economies, with some economies such as Australia; Japan; and Singapore already achieving widespread adoption, while other APEC economies lag.[8] APEC has also developed 2023 Principles for the Interoperability of Electronic Invoicing Systems in the APEC Region. The Principles provide a comprehensive framework to address interoperability challenges of e-invoicing systems.

7 Deloitte Access Economics 2016. The Economic Impact of E-Invoicing
8 APEC Committee on Trade and Investment, "Interoperability of Electronic Invoicing systems in the APEC Region" Feb 2025

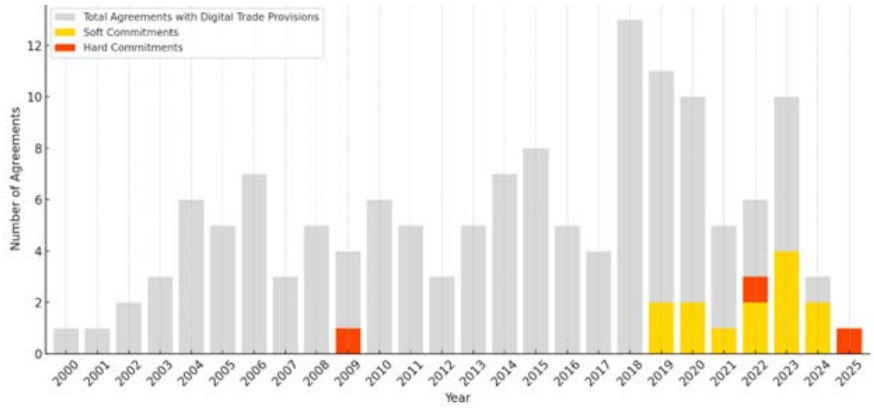
APEC 2023: principles for the interoperability of electronic Invoicing Systems in the APEC Region

APEC economies are encouraged to:

- Accord electronic invoices the same legal effect as paper invoices issued for the sale of goods or services;
- Base measures related to electronic invoicing on applicable international, open standards, guidelines or recommendations;
- Implement policies, infrastructure and processes that facilitate the development and use of electronic invoicing that allow buyers and sellers to exchange documents in a secure manner;
- Promote the use of common, open standards and protocols, including data language and syntax, to enable interoperability among different electronic invoicing systems and related documents;
- Build confidence in, and understanding of, each other's electronic invoicing policies, infrastructure and processes through the sharing of best practices; and
- Support initiatives which facilitate, and build capacity for, the development and adoption of interoperable electronic invoicing systems.

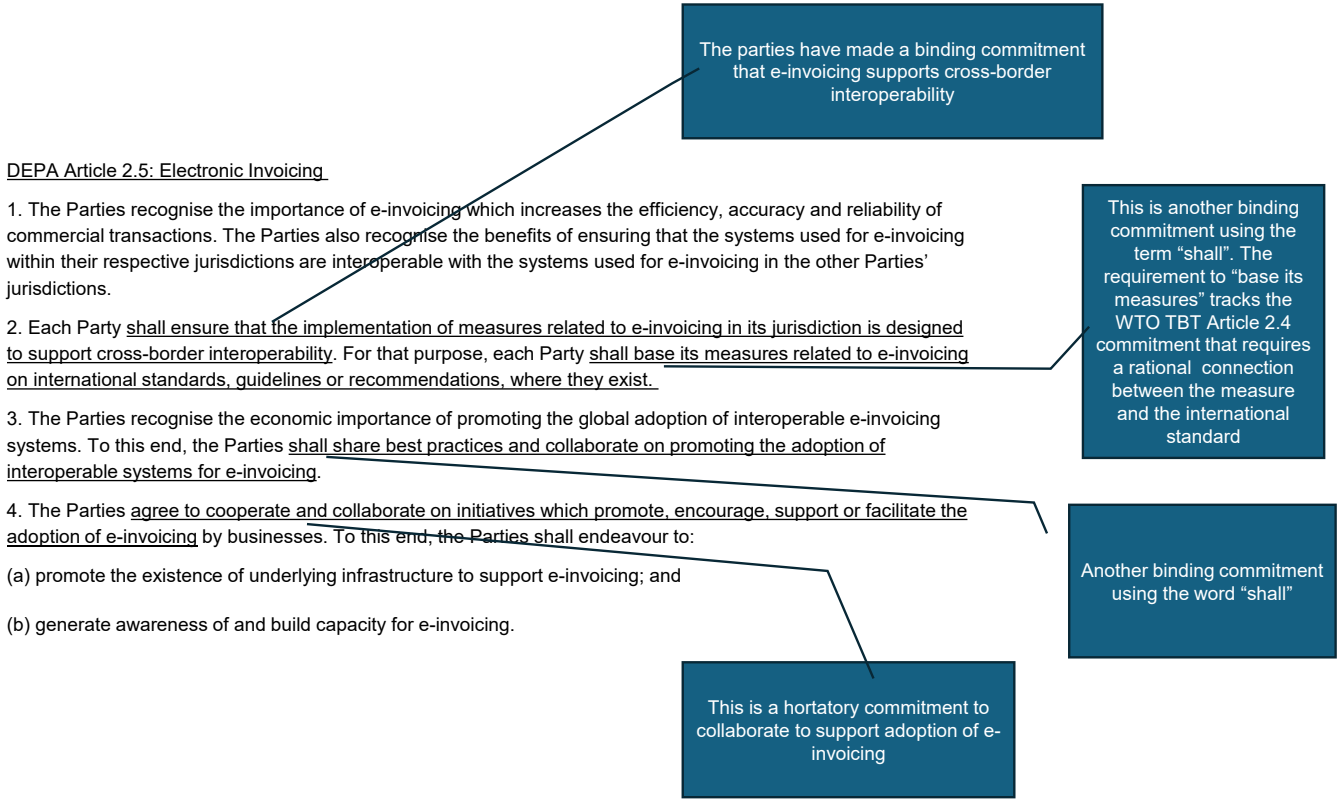
E-invoicing in trade agreements

E-Invoicing Commitments vs. Total Digital Trade Agreements by Year



Sample E-Invoicing Provision

This sample provision is taken from the **DEPA** text. Key commitments here are to implement e-invoicing to enable interoperability which allows for recognition for e-invoices across borders. The commitment to base e-invoicing measures on international standards is also important as it provides a basis for aligning domestic e-invoices standards and laws.



Policy Checklist: Electronic Invoicing

Question	Consideration
Should a provision on e-invoicing be included?	This is a threshold question. At least 16 provisions have appeared since 2009 and are now a common inclusion.
Should it include commitments to implement e-invoicing measures that support cross-border interoperability?	This core provision could either be binding (e.g. shall) as in DEPA or, qualified (e.g. endeavour to) as in WTO ECA. It is somewhat common for this core provision to be binding.
Should it include a commitment to "take into account" relevant international standards" or instead to commit to "base its measures relating to e-invoicing on international standards"?	The commitment to base the measure on international standards as in DEPA tracks the WTO TBT Article 2.4 commitment that WTO Members use international standards as "a basis for their technical regulations" and requires more a fit between the measure and the standard than the commitment to "take into account" international standards.
Should it include a commitment to share best practices on e-invoicing or to cooperate/ collaborate on supporting/facilitating adoption of e-commerce?	There are various commitments to cooperation that can be included, with these typically being hortatory in nature.
Should it include a commitment that e-invoices have legal effect and be admissible as evidence in legal proceedings?	This commitment is in the WTO ECA and gives added incentive and certainty for businesses using e-invoices.
How does this relate to previous commitments on electronic invoicing?	If your economy has previously committed to a position on e-invoicing, ensure that the provisions are consistent unless a change in policy is desired.

A3: Electronic authentication and signatures

What is electronic authentication and signatures?

Electronic Signature: is a digital equivalent of a handwritten signature. It signals intent, including acceptance as to the content of an electronic record. The WTO ECA defines an electronic signature as "data in electronic form that is in, affixed to, or logically associated with an electronic data message and that may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message".[9]

Electronic Authentication: refers to techniques to verify that a digital signature is valid, authentic, and created by the claimed signer. Authentication often relies on passwords, answers to security questions, or biometric information. The WTO ECA defines electronic authentication as the process or act of verifying the identity of a party to an electronic communication or transaction, or ensuring the integrity of an electronic communication."

What are the economic benefits from electronic authentication and signatures?

The APEC study on the economic impact of digital trade rules found that adopting trade commitments on e-signatures and e-authentication increased digital ordered trade by almost 19% and digitally delivered trade by over 21% in the year of adoption.[10] These economic gains resulted from reductions in operating costs and the need for complex paperwork and reducing time to process transactions.[11]

What are the main barriers to electronic authentication and signatures?

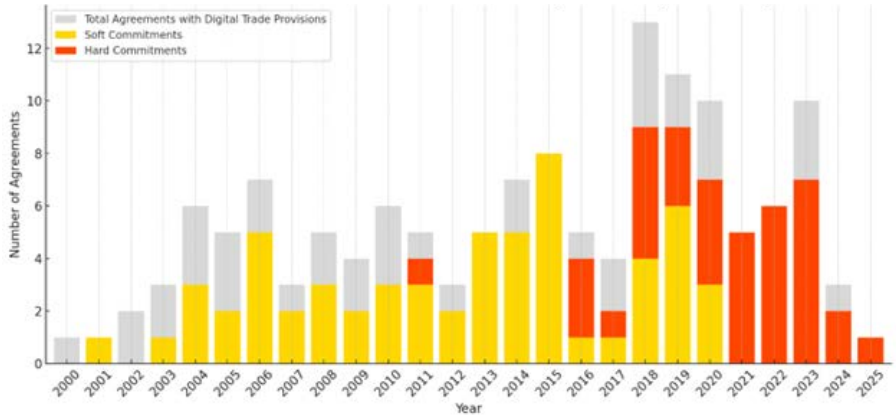
Digital signatures and authentication supports e-commerce where completing the transaction requires verification of a person's identity as part of an e-commerce transaction. Indeed, the WTO/OECD Aid for Trade rates e-signatures as a top challenge facing enterprises and consumers when accessing and using internet services.[12]

9 WTO ECA Article 5.1
10 Economic Impact of Adopting digital Trade Rules: Evidence from APEC Member Economies, CTI report, April 2023
11 Economic Impact of Adopting digital Trade Rules: Evidence from APEC Member Economies, CTI report, April 2023
12 OECD/WTO, Promoting Trade, Inclusiveness and Connectivity for Sustainable Development, 2017

The key challenges to recognizing electronic signatures across borders and to accepting electronic authentication methods amongst APEC economies are the lack of common standards and approaches. While most APEC economies recognize e-signatures as valid domestically, differences in laws and regulations among APEC economies can make it unclear whether an e-signature in one economy meets the other economies own domestic standards. Relatedly, different laws governing authentication of e-signatures as well as technologies for authentication create barriers to developing an APEC-wide approach to electronic authentication.

Electronic authentication and signatures in trade agreements

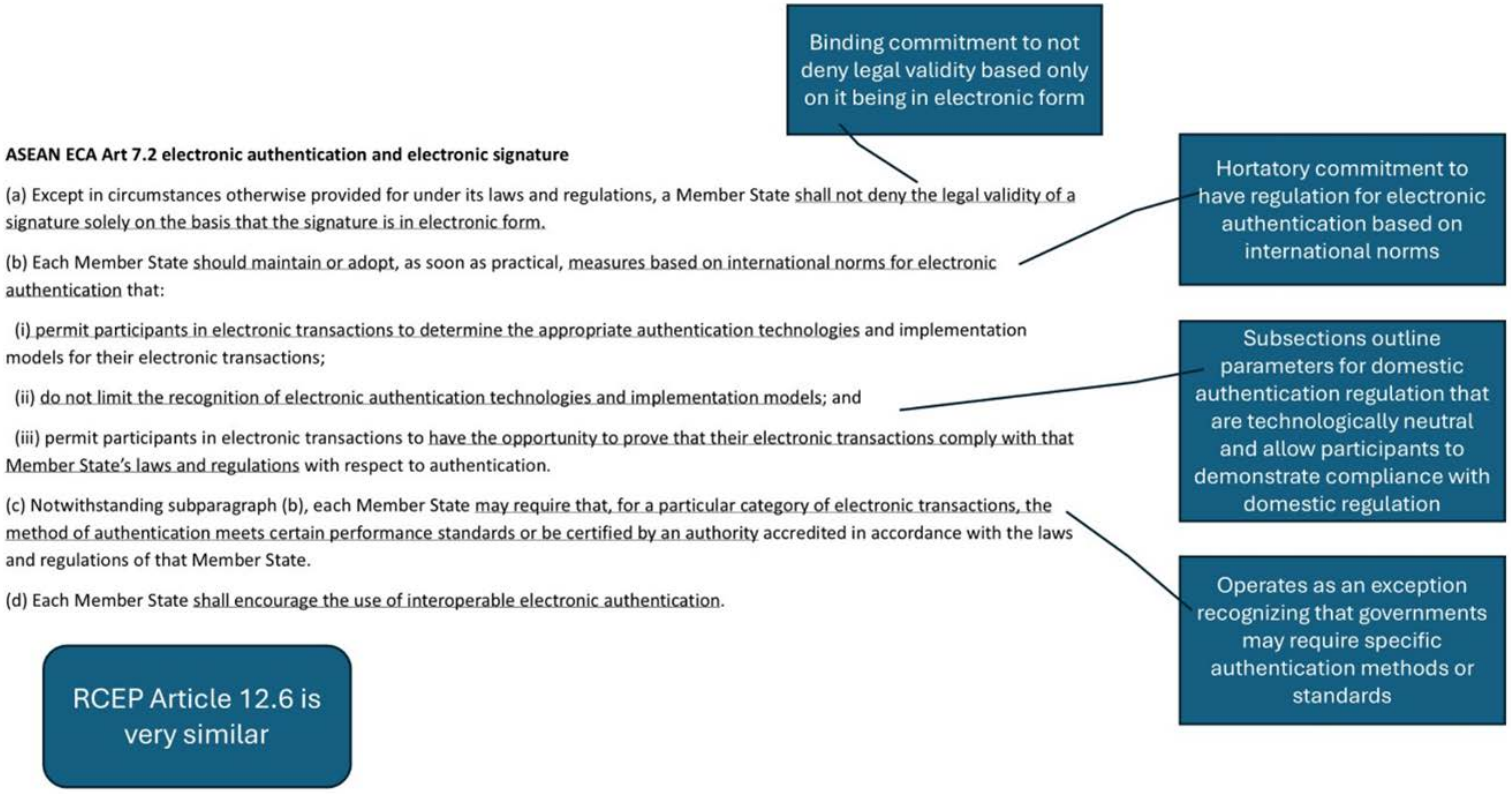
Electronic Authentication Commitments vs. Total Digital Trade Agreements by Year



The key commitment here is to ensure that electronic signatures have legal validity and are recognised as such across borders. This includes the ability to use and have recognized the technologies used to authenticate electronic signatures.

Sample Electronic Authentication Provision

This sample Electronic Authentication provision is taken from the **ASEAN Agreement on Electronic Commerce (AEC).**



Policy Checklist: Electronic Authentication

Question	Consideration
Should a provision on Electronic Authentication be included?	This is a threshold question. Around 100 provisions have appeared since 2001 and are now typically included in agreements that include digital trade provisions.
Should it include commitments not to deny the legal validity of an electronic signature?	This core provision is typically binding (e.g. shall) as in the WTO ECA, CPTPP and the ASEAN AEC.
Should it include commitments to not prohibit parties determining the appropriate electronic authentication method or electronic signature?	This core provision is typically binding (e.g. shall) as in the WTO ECA, and the CPTPP. The ASEAN ECA commitment is hortatory and is a commitment by parties to allow participants to determine which electronic authentication technology to use.
Should it include commitments to allow parties to an electronic transaction to establish that the transaction complies with legal requirements regarding authentication?	It is more common for this core provision to be binding.
Should it include a provision requiring a particular method of authentication to meet standards or be certified?	This provision is typically framed as a limited exception and is found broadly including in the WTO ECA, CPTPP and ASEAN AEC.
How does this relate to previous commitments on unsolicited commercial messages?	If your economy has previously committed to a position on electronic authentication, ensure that the provisions are consistent unless a change in policy is desired.

A4: Digital ID

What is Digital ID?

Digital Identity: broader conception of information used by a computer to identify an agent – usually a person but can be a legal entity. Passports, driver's licenses are examples of proof of a person's identity. A digital identity ensures that you know with whom you are interacting and thereby fosters trust throughout supply chains. It involves authentication ("Who are you?") and authorization ("What are you allowed to do?") processes.

What are the Economic Benefits from Digital Identity?

According to the World Bank there are over 1bn people without a digital identity. Having a digital identity is key to enabling economic inclusion broadly, including when it comes to participating in digital trade. There are various estimates of the economic benefits from digital ID. McKinsey estimated that extending digital ID in seven economies - Brazil; China; Ethiopia; India; Nigeria; the UK; and the US would by 2030 unlock economic value equivalent to 3-13 percent of GDP.[13]

Having a digital identity has a range of implications for digital trade. For one, having a digital identity allows parties to an e-commerce transaction to verify, reducing fraud and building trust, enabling digital trade.

A digital identity also supports regulatory compliance such as with Know Your Customer (KYC) and anti-money laundering (AML) checks for cross-border payments.[14]

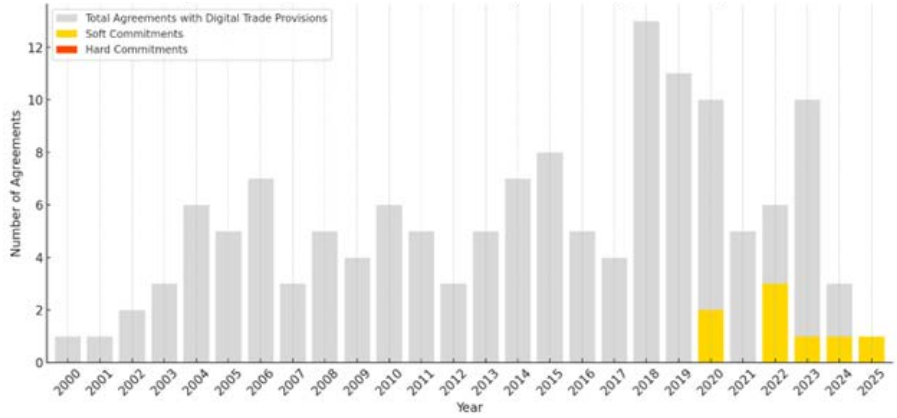
What are the Challenges and Barriers to Digital ID?

From a digital trade perspective, the challenges are both the lack of a digital ID, and where these exist, the lack of interoperability – the absence of common standards and approaches - that allow for recognition of digital IDs across borders. Digital identities leverage domestic systems and unless these systems are built on globally acceptable standards and practices are often unique and therefore not readily recognized or their systems and technologies translatable in other economies. There are an estimated forty different digital ID systems in use globally, including for example India's Digital ID Aadhaar for roughly 1.2bn people and which uses a unique 12 digit ID number issued by the India government to residents.

13 McKinsey Global Institute, "Digital Identification: A key to inclusive growth", April 2019
14 Data age 2025: The evolution of data to life-critical, Seagate, March 2017; World Bank (2018). The State of Identification Systems in Africa: Country Briefs

Digital ID in trade agreements

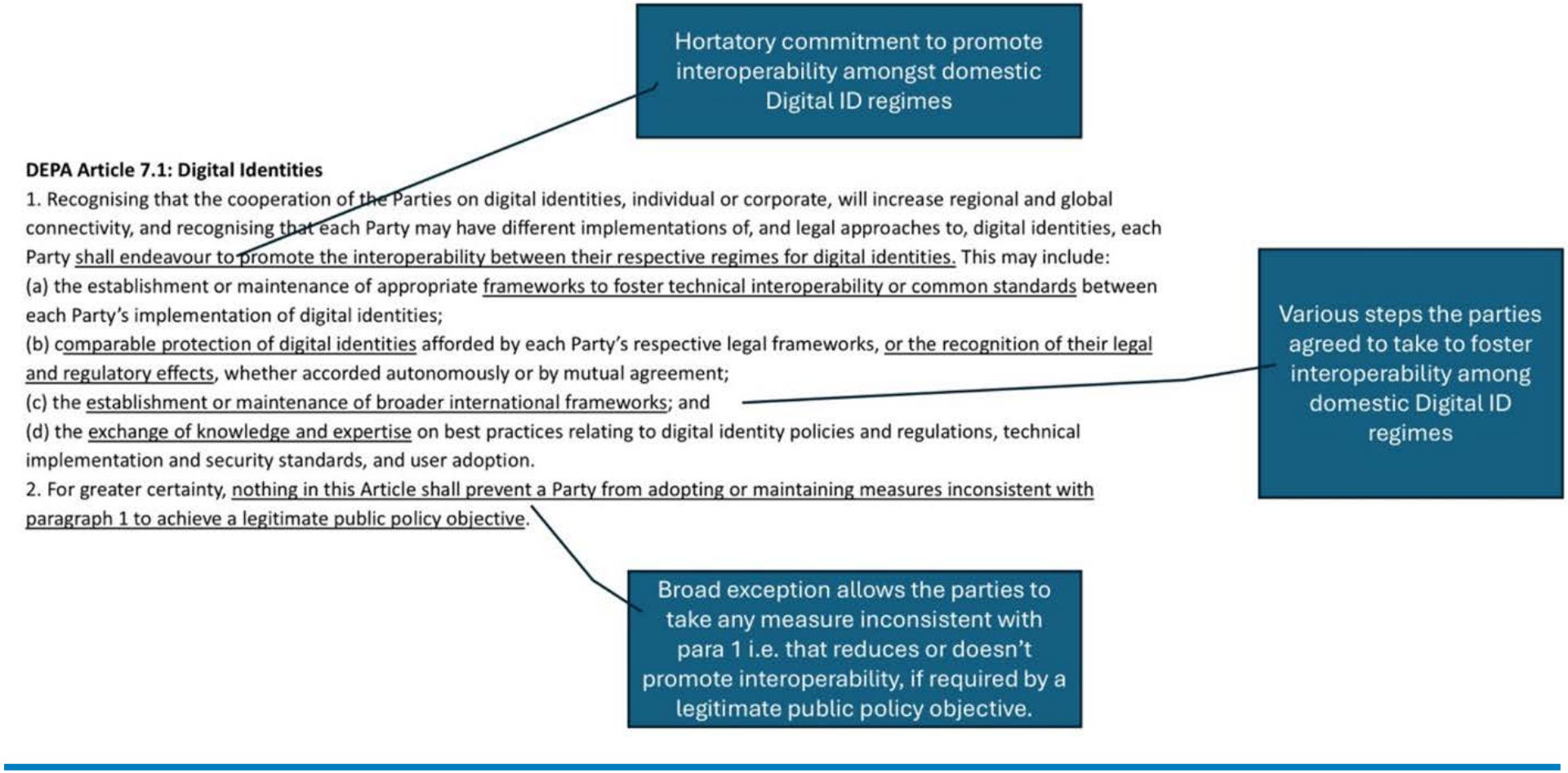
Digital Identity Commitments vs. Total Digital Trade Agreements by Year



Digital Identity commitments include the promotion of interoperability amongst domestic systems for digital identity that can include taking steps such as common standards and exchange of knowledge and expertise.

Sample Digital Identity Provision

This sample **Digital Identity** provision is taken from the **DEPA** text.



Policy Checklist: Digital Identity

Question	Consideration
Should a provision on Digital Identity be included?	This is a threshold question. Digital Identity provisions have appeared since 2020 and are now infrequently included.
Should it include commitments to promote the interoperability between domestic regimes for digital identities?	This provision serves as the key hortatory goal of Digital Identity provisions, such as in DEPA.
Should it include commitments to develop frameworks or standards that enable interoperability?	This core provision could either be binding (e.g. shall) or qualified (e.g. endeavour to) but is a practical step that APEC economies can take to enable interoperability.
Should it include commitments to cooperation in developing international frameworks on digital identity or to exchange knowledge and expertise?	These provisions are typically hortatory as in DEPA and useful in building momentum at the international level to developing common approaches and methods for recognizing digital identities across borders.
Should the provision be subject to a specific exception?	Some digital identity provisions such as DEPA include an exception for any measure adopted to achieve a legitimate public policy objective.
How does this relate to previous commitments on Digital Identity?	If your economy has previously committed to a position on Digital Identity, ensure that the provisions are consistent unless a change in policy is desired.

A5: Customs duties & electronic transmissions

What is the issue of customs duties on electronic transmissions?

Electronic transmissions refer to the transfer of data, including 'products' such as software, music, films, over the internet. As more goods and services are traded digitally, some economies are considering whether to apply customs duties (tariffs) to trade in these digital products.

Applying duties to electronic transmissions would increase costs for businesses and consumers, disrupt digital trade, and create legal uncertainty. It is also administratively complex and would require officials to assess the value and origin of data. In part due to this administrative complexity, few economies have in practice imposed such duties to date.

What are the economic benefits from commitments not to impose customs duties on electronic transmissions?

Key economic benefits of commitments not to impose customs duties on electronic transactions include:

- **Lower costs for businesses and consumers:** Companies can deliver products such as software, games, or design files without the added cost, helping to reduce prices and increase availability.
- **Encouragement of SMEs:** By eliminating border costs, SMEs can more easily enter global markets using online platforms.
- **Boost to the broader digital economy:** Duty-free digital trade promotes faster, more efficient business models and international value chains.

As a core part of a broader package of digital trade provisions, the commitment to not impose customs duties on electronic transmissions could boost real GDP by up to **2.1%** in some APEC economies and increase exports of digitally deliverable services (like software, music, and video content) by up to **4.4%.** These provisions are linked to lower transaction costs, reduced trade barriers, and improved access to global digital markets.[15]

Recent economic studies have also shown that r**emoving the WTO moratorium on customs duties for electronic transmissions could result in significant economic costs,** particularly for developing economies.

15 The Economic Impact of Adopting digital Trade Rules: Evidence from APEC Member Economies, CTI report, April 2023

One estimate finds that such a change could reduce global GDP by up to USD 10.6 billion annually, while offering only modest tariff revenue gains.[16]

What are the main challenges to commitments on customs duties in relation to electronic transmissions?

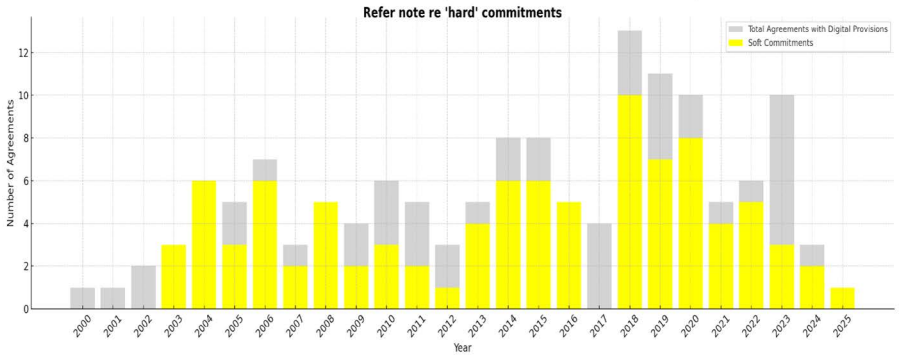
Key policy challenges expressed by some economies on the commitment to prohibiting customs duties include:

Revenue pressures: Especially for developing economies, there is concern that exempting digital imports from customs duties may shrink government tariff revenue, especially as more products (such as books) are delivered digitally (such as audiobooks).

- **Uncertainty around definitions:** there is sometimes disagreement over what qualifies as an "electronic transmission". Does it include any data? Streaming services? 3D printing files? This uncertainty creates legal ambiguity.
- **Administrative challenges:** imposing duties on electronic transmissions, even if desired, would be difficult to implement. The issue of origin and value – the key elements of tariffs on goods – are highly complicated with even single data requests by consumers relying on global data flows from data centres in multiple locations.

How is the issue of customs duties on electronic transmissions handled in trade agreements?

Commitments on Customs Duties (Moratorium on Electronic Transmissions)



<u>Note:</u> the TAPED Database does not technically classify any of the existing customs duties provisions as 'hard commitments' though this does not reflect the binding nature of many commitments, including Article 14.3 of the CPTPP explained below.

16 See, for example:
- ECIPE (2019), The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions, ECIPE Policy Brief No. 3/2019.
- IMF (2023), Fiscal Revenue Mobilization and Digitally Traded Products: Taxing at the Border or Behind It?, IMF Staff Discussion Note SDN/2023/005.
- OECD (2023), Electronic Transmissions and International Trade – Findings from Research and Practice.

The agreement not to impose customs duties on electronic transmissions has become a consistent feature of modern trade agreements, including those involving APEC economies.

WTO Members agreed in 1998 to not impose customs duties on electronic transmissions – a decision known as the WTO Moratorium on Customs Duties on Electronic Transmissions. This multilateral e-commerce Moratorium places a temporary prohibition on the imposition of customs duties on electronic transmissions. The Moratorium has been regularly renewed, with the next renewal due at the 14th Ministerial Conference in March 2026.

Some economies have agreed not to impose customs duties through permanent commitments in bilateral and regional trade agreements. In other agreements, some economies have agreed a temporary prohibition on customs duties on electronic transmissions, pending discussions at the WTO.

Some agreements, such as the **WTO ECA** and the **CPTPP**, make a clear and binding commitment that parties will not impose customs duties on electronic transmissions between economies. These provisions aim to lock in the current global practice.

Earlier agreements, particularly those concluded before the WTO ECA E-commerce, recognised that further developments may occur at the WTO, and could therefore reopen the commitment for discussion. However, the emergence of the WTO ECA (representing a consensus among dozens of WTO members) has further entrenched the commitment for no customs duties on electronic transmissions. The **inclusion of this provision in the ECA reflects an emerging international norm,** building upon a broad base of practice across APEC and other regional agreements such as the CPTPP, DEPA, and RCEP. To provide further clarity, many agreements (but not all) define **"electronic transmissions"** as including both the transmission and its content. This means that not only the act of transmission (e.g. downloading a file) but also the digital product itself (like a music track or a software program) is protected from customs duties.

Allowing Other Taxes and Fees

Importantly, most trade agreements clarify that the ban on customs duties **does not prevent governments from imposing internal taxes,** such as **value-added tax (VAT),** as long as those taxes are applied in a **non-discriminatory** way. In other words, treating foreign and domestic companies equally.

Sample Customs Duties Provision

This sample Customs Duties provision is taken from the **Comprehensive and Progressive Agreement for the Trans-Pacific Partnership** text.

Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)

Article 14.3: 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.

Coverage of prohibition includes electronic transmissions and the content of transmissions.

The imposition of FTA-consistent internal taxes, fees or other charges on content is permitted.

Policy Checklist: Customs Duties & Electronic Transmissions

Question	Consideration
Should a provision on Customs Duties & Electronic Transmissions be included?	This is a threshold question. Customs Duties provisions have appeared since 2003 and are now typically included in a third of all agreements.
Should it include commitments on not imposing customs duties on electronic transmissions?	This core provision is typically binding, but refer to developments in the WTO that may adjust the underlying commitment.
Should it include permission to charge other (non-duty) taxes and fees?	The flexibility to allow imposition of non-duty taxes and fees is common.
How does this relate to previous commitments on customs duties and electronic transmissions?	If your economy has previously committed to a position on customs duties on electronic transmissions, ensure that the provisions are consistent unless a change in policy is desired.

A6: Non-discrimination between digital products

What is non-discrimination between digital products?

The non-discrimination provision commits parties to not discriminate in favor of domestic digital products that are like imported digital products i.e. that compete in the market. The non-discrimination commitment is also a commitment not to provide more favourable treatment to the digital products from one party compared to a like digital product of another party.

What are the economic benefits from non-discrimination between digital products?

Commitments to non-discrimination are central to all WTO and free trade agreements. The key non-discrimination commitments are to national treatment (NT) – to treat like domestic products no less favorably than like imported products and the most-favored-nation (MFN) commitment – to accord the same treatment to all like imported products. These commitments aim to achieve equality of opportunities to compete, leading to more efficient markets. Applying a specific non-discrimination commitment to digital products also gives greater certainty to traders about the application of NT and MFN to digital products. The commitment also defines what is a digital product, which adds further certainty and avoids the question still relevant in the WTO context as to whether a digital product is a good or service.

Adopting a commitment to non-discrimination in trade agreements was found to lead to increases in digitally ordered trade of up to almost 20% following the first two years after adoption, and to increases in digitally deliverable trade values of over 29% over the next three years.[17] The non-discrimination commitment is also subject to the exceptions provisions in the applicable trade agreement or FTA. This aligns with how the NT and MFN commitments work when applied to goods and services in the WTO and FTA generally.

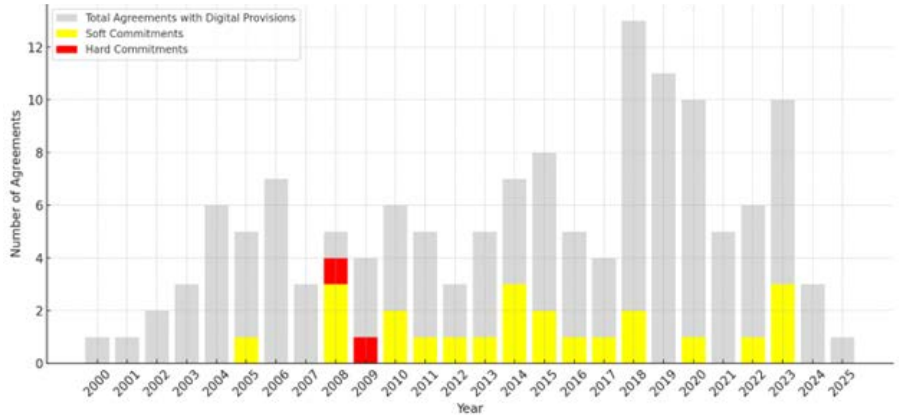
What are the main barriers to non-discrimination between digital products?

The key issue for any government will be the extent they are willing to abide by the non-discrimination norm and whether the exception provisions provide enough policy flexibility.

17 Economic Impact of Adopting digital Trade Rules: Evidence from APEC Member Economies, CTI report, April 2023

Non-discrimination between digital products in trade agreements

Commitments on Non-Discrimination (Tech Neutrality)



The typical no-discrimination commitment in digital trade agreements or chapters is to not accord less favourable treatment to digital products either created, produced or published in the territory of another Party or to digital products where the author, performer or developed is a person of another Party, than the treatment accorded to other like products - which includes domestic like products or like products from other Party's.

Sample Non-Discrimination Provision

This sample Non-Discrimination provision is taken from the **CPTPP** text.

CPTPP Article 14.4: Non-Discriminatory Treatment of Digital Products

1. No Party shall accord less favourable treatment to digital products created, produced, published, contracted for, commissioned or first made available on commercial terms in the territory of another Party, or to digital products of which the author, performer, producer, developer or owner is a person of another Party, than it accords to other like digital products.4

Footnote 4: For greater certainty, to the extent that a digital product of a non-Party is a "like digital product", it will qualify as an "other like digital product" for the purposes of this paragraph.

Article 14.1 digital product means a computer programme, text, video, image, sound recording or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically.3

Footnote 3: The definition of digital product should not be understood to reflect a Party's view on whether trade in digital products through electronic transmission should be categorised as trade in services or trade in goods.

Applies a NT and MFN commitment

Extends scope to treatment a Party to extends to like products from a non-Party.

Opportunity to define what is a digital product avoids the uncertainty in the WTO, which affects whether the NT/MFN commitments in GATT or GATS apply.

Australia-Singapore DEA has an identical provision

Policy Checklist: Non-Discrimination

Question	Consideration
Should a provision on Non-Discrimination be included?	This is a threshold question. 25 provisions have appeared since 2005 and are now intermittently included. Agreements that include the non-discrimination commitment include the CPTPP and Australia-Singapore DEA. There is no such commitment in the WTO ECA.
How to define what is a digital product?	This core provision is a key determinant of the scope of the commitment.
Should the commitment applied to treatment that a Party accords to non-Party's?	The CPTPP for example includes a binding commitment to non-discriminatory treatment also captures treatment accorded by a Party to non-Party's. This has the effect of making the non-discrimination commitment operate more like a multilateral MFN commitment and ensure that any better treatment accorded to like digital products from a non-Party is also extended to all Parties to the agreement.
How does this relate to previous commitments on non-discrimination?	If your economy has previously committed to a position on non-discrimination, ensure that the provisions are consistent unless a change in policy is desired.

A7: Access to and use of internet services and applications

What is access to and use of internet services and applications?

Trade agreements with this provision use the same text which includes three core principles that govern access of consumers to the internet. These are (i) the right to use services and application of choice, (ii) to choose which end-user devices to connect to the internet and (iii) to have access to network management practices of the internet access service supplier. These principles address the rights of consumers to access and use the internet, including connecting applications of choice, as well as getting access to information on network management practices. .

What are the economic benefits from access to and use of internet services and applications?

Principles on internet access and use—such as ensuring open, secure, reliable, and affordable connectivity—can enable digital trade, allow consumers to access and use services and applications of their choice. This in turn enhances personal freedom, competition, and innovation and allows consumers to choose digital services based on their own preferences, while fostering competition among digital service providers. This principle also promotes digital inclusion by ensuring consumers—regardless of location—can participate in the digital economy by enabling access to services such as online education, financial tools, and remote work platforms. By preventing arbitrary restrictions or gatekeeping of online services, the principle strengthens trust in digital markets and supports a fair, open, and consumer-centric digital trade environment.

Allowing consumers to connect the end-user devices of their choice (such as smartphones, tablets, computers, smart TVs, or IoT devices) to the Internet allows consumers to choose the devices that best meet their needs. This can stimulate competition among hardware manufacturers. This principle also fosters a more open and inclusive digital ecosystem by reducing barriers to participation in online commerce and services. When consumers can use any compatible device to access the Internet, they can more easily engage in cross-border e-commerce.

This third principle allows consumers to access information network management practices. This commitment enhances transparency around these practices, which can help prevent discriminatory or anti-competitive behavior

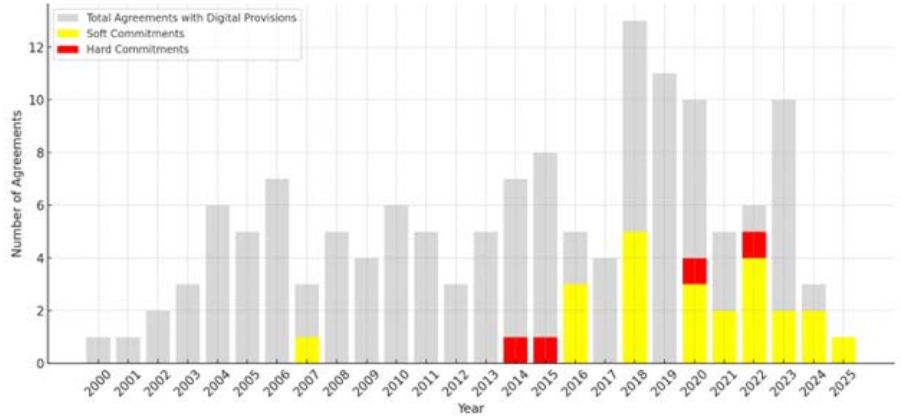
that could limit access to digital services. This openness also promotes competition among service providers, and ensures that digital trade operates in a more predictable environment.

What are the main barriers to access to and use of internet services and applications?

Different domestic laws and regulation on consumer rights and internet management practices may not align or be at odds with these principles.

Access to and use of internet services and applications in trade agreements

Commitments on Access to the Internet



Since 2016, commitments on Access to the Internet have gradually appeared in trade agreements involving APEC economies, with soft commitments far more common than hard ones. While the total number of digital trade agreements has varied year to year, the share including Internet access provisions has grown modestly over time. The data suggests that APEC economies increasingly acknowledge Internet access as a principle of digital trade, though binding commitments remain limited.

Sample Internet Access Provision

This sample Internet **Access** provision is taken from the CPTPP.

CPTPP Article 14.10: Principles on Access to and Use of the Internet for Electronic Commerce

Subject to applicable policies, laws and regulations, the Parties recognise the benefits of consumers in their territories having the ability to:

(a) access and use services and applications of a consumer's choice available on the Internet, subject to reasonable network management;7

(b) connect the end-user devices of a consumer's choice to the Internet, provided that such devices do not harm the network; and

(c) access information on the network management practices of a consumer's Internet access service supplier.

Footnote 7 The Parties recognise that an Internet access service supplier that offers its subscribers certain content on an exclusive basis would not be acting contrary to this principle.

Policy Checklist: Access to and use of internet services and applications

Question	Consideration
Should a provision on Access be included?	This is a threshold question. Some FTAs include these provisions such as USMCA, CPTPP, DEPA and the Australia-Singapore FTA, whereas other agreements such as RCEP and the Japan-EU Economic Partnership do not. These types of provisions have appeared intermittently since 2007.
Should it include all the three paragraphs in the provision?	All trade agreements with this commitment include all the principles of internet access and use in paragraphs (a)-(c). This includes CPTPP, DEPA, USMCA and the Singapore-Australia DEA.
Should it include as a footnote the text which clarifies that providing subscribers exclusive content would not be contrary to the principles of consumer choice?	This footnote ensures that business models built around providing exclusive content on a subscription basis are understood as not being inconsistent with the principle. All trade agreements with this commitment include the same footnote to this first principle.
How does this relate to previous commitments on Access?	If your economy has previously committed to a position on Access, ensure that the provisions are consistent unless a change in policy is desired.

A8: Electronic payments

What are Electronic payments?

Electronic payments are themselves a form of digital trade and also are a key enabler of other forms of digital trade.

What are the economic benefits from Electronic payments?

The total transaction value in cross-border payments was USD 194 trillion in 2024, and is expected to reach over USD 320 trillion by 2032, with the largest growth and use of electronic payments being for e-commerce transactions. Efficient cost-effective cross-border payments facilitate economic integration and trade. Currently, businesses often find it costly to receive payments from customers in another economy. For example, 60% of cross-border B2B payments require some sort of manual intervention taking 15-20 mins at least. These frictions increase the costs of remittances which hits the poorest and most vulnerable who rely on sending money back home. Enabling small businesses to have access to secure and remote transactions also helps include underserved populations in digital trade. Additionally, electronic payments can enhance transparency and reduce fraud.

What are the main barriers to Electronic payments?

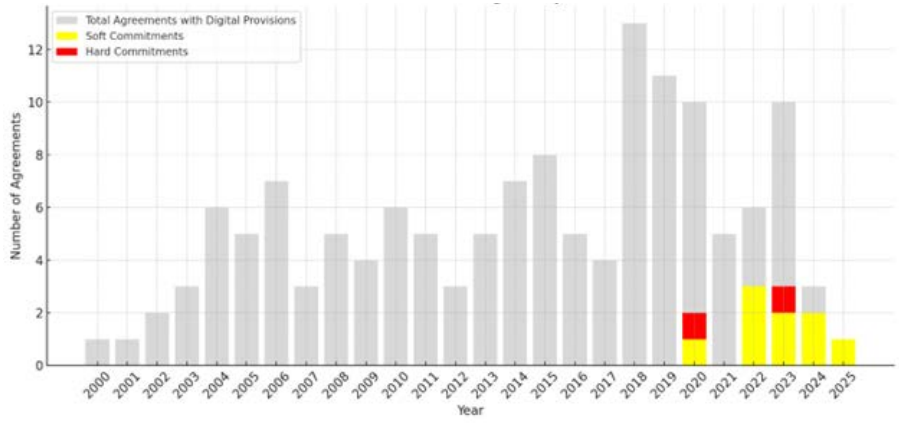
Differences in messaging standards between the domestic payment systems and cross-border payments are a major barrier to efficient cross-border electronic payments. Cross-border payment data exchanged using the SWIFT messaging standard has not been interoperable with domestic payment systems, which vary across economies, causing delays and operational challenges. As a result, adoption of international standards and in particular ISO 20022 has been a focus for building interoperability amongst digital payment systems. Increasing the use of APIs to establish linkages between financial institutions has facilitated data exchange, system interoperability, and real-time transactions between financial institutions. However, APIs have been developed differently across APEC economies, resulting in different formats. This has led to a fragmentation of API technical standards that are barriers and reduce the scope of their ability to support cross-border payments.

ASEAN Payment Connectivity Initiative

In November 2022, five ASEAN member states -Indonesia; Malaysia; the Philippines; Singapore; and Thailand—signed the Memorandum of Understanding (MoU) on Cooperation on Regional Payment Connectivity (RPC), with the aim of strengthening bilateral and multilateral payment connectivity to promote faster, cheaper, more transparent, more inclusive cross-border payments in the region. Since then, four other ASEAN member states have joined – Brunei Darussalam; Cambodia; Lao PDR; and Viet Nam. The initiative aims to strengthen and enhance cooperation on payment connectivity through the development of faster, cheaper, more transparent, and more inclusive cross-border payments which aligns with the shared vision for greater regional economic integration, including payment and settlement systems, under the ASEAN Economic Community Blueprint 2025.

Electronic payments in trade agreements[18]

Commitments on Digital Payments



The number of trade agreements including provisions on electronic payments has gradually increased since 2020. While both soft and hard commitments are present, soft commitments remain more common. Relative to the total number of agreements with digital provisions, electronic payments are still a growing but not yet dominant focus area.

18 This does not account for any commitments on electronic payments that may appear in Financial Services chapters in trade agreements.

Sample Electronic Payments Provision

This sample electronic payments provision is taken from the WTO ECA.

WTO JSI Article 10

...the Parties recognize:

(a) the benefit of supporting the development of safe, efficient, trustworthy, secure, affordable, and accessible cross-border electronic payments by fostering the adoption and use of internationally accepted standards, promoting interoperability of electronic payments systems, and encouraging useful innovation and competition in electronic payments services;

(b) the importance of enabling the introduction of safe, efficient, trustworthy, secure, affordable, and accessible electronic payment products and services in a timely manner; and

(c) the importance of upholding safe, efficient, trustworthy, secure, and accessible electronic payments systems through laws and regulations that, where appropriate, account for the risks of such systems.

10.3 In accordance with its laws and regulations, each Party shall endeavour to:

(a) further to Article 18, make its laws and regulations on electronic payments, including those pertaining to regulatory approvals, licensing requirements, procedures, and technical standards, publicly available in a timely manner;

(b) finalize decisions on regulatory or licensing approvals in a timely manner;

(c) take into account, for relevant electronic payments systems, internationally accepted payment standards to enable greater interoperability between electronic payments systems; and

(d) encourage electronic payments service suppliers and financial service suppliers to facilitate greater interoperability, competition, security, and innovation in electronic payments, which may include partnerships with third-party providers, subject to appropriate risk management.

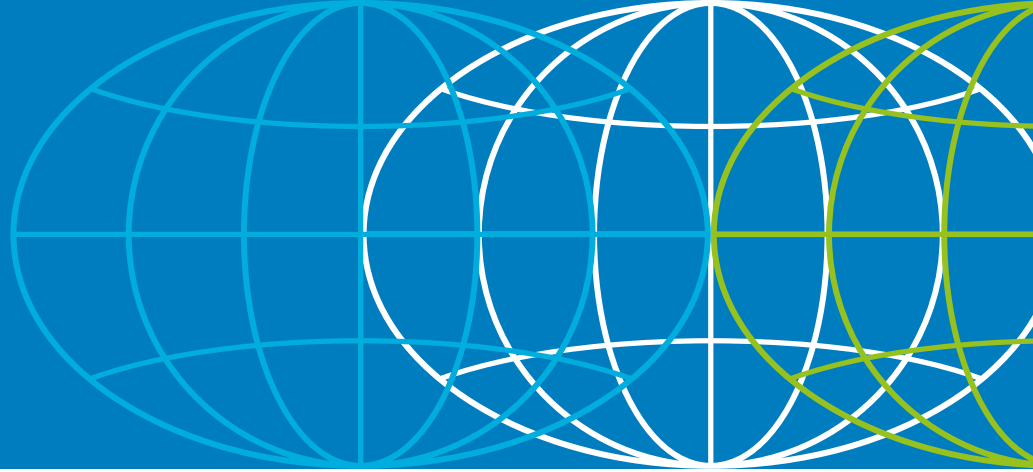
10.4 Subject to any terms, limitations, conditions, or qualifications set out in its Schedule of Commitments to the GATS ("Schedule"), each Party that has undertaken a commitment in its Schedule in respect of Mode 3 (Commercial Presence) supply covering electronic payments services shall grant, on terms and conditions that accord national treatment, financial service suppliers of another Party established in its territory access to payment and clearing systems operated by a public entity.

Policy Checklist: Electronic Payments

Question	Consideration
Should a provision on digital trade be included?	This is a threshold question. The development of a digital payment provision in the WTO ECA points to broad acceptance of including such provisions. At least 11 provisions have appeared since 2020 and are now commonly included.
Should it include commitments on making laws and regulations on electronic payments publicly available?	This is core provision that is binding in the Australia-Singapore DEA but hortatory in other agreements such as the WTO ECA and DEPA.

Should it include commitments to finalise a decision on regulatory or licensing approvals in a timely manner?	This core provision is typically hortatory.
Should it include commitments taking into account or adopting internationally acceptable payment standards to enable interoperability between payment systems?	This core provision is either to take into account international standards as in the WTO ECA and DEPA or the more binding formulation such as in the Australia-Singapore DEA to adopt international standards for electronic payment messaging with a specific reference to ISO 20022.
Should it include a commitment on non-discrimination amongst financial and non-financial institutions?	The WTO ECA includes a restatement of the binding commitment to non-discrimination towards financial service suppliers consistent with each WTO Member's GATS Schedule. The DEPA includes a commitment not to arbitrarily and unjustifiably discriminate between financial and non-financial institutions in relation to access to the services and infrastructure to operate digital payment systems.
Should it include a provision to adopt risk based regulation of electronic payments?	This is a hortatory commitment found in DEPA. It and the Australia-Singapore DEA. It has the effect of having governments focus on whether various barriers to interoperability and access to the infrastructure and services required to operate an electronic payments system is justified based on an assessment of risks.
How does this relate to previous commitments on Electronic Payments?	If your economy has previously committed to a position on Electronic Payments, ensure that the provisions are consistent unless a change in policy is desired.

Section B:
Building Trust



B1: Protection of online personal information

What is protection of online personal information?

Privacy protection commitments help ensure the protection of personal data sent to another APEC economy, strengthening trust and facilitating the cross-border flows of personal data that is required for digital trade.

How do privacy commitments facilitate digital trade and transfers of personal data among APEC economies?

There has been considerable work within APEC as well as other international institutions including the EU and the OECD to develop common privacy principles as well as mechanisms for enabling transfers of personal data across borders. When it comes to strengthening personal data protection to facilitate cross-border data flows, digital trade agreements reference these international privacy principles and interoperability mechanisms as a way of increasing alignment on privacy regulation and in order to build interoperability amongst different domestic privacy regulations, thereby reducing friction or barriers to cross-border transfers of personal data for digital trade purposes.

What are the economic benefits of including privacy commitments in digital trade agreements?

Flows of personal information across borders enables a range of digital trade. For example, B2C e-commerce transactions require name, address and bank account details. The delivery of online digital services, such as professional services and education services also often require access to personal data. Given the extensive range

of digital trade that can require transfers of personal data, restrictions on these transfers can be costly. The aim therefore has not been to eliminate privacy regulation, but to require privacy laws as a basis for building trust when transferring personal data across borders, and to encourage governments to develop interoperability mechanisms that facilitate transfers of personal data across borders. In fact, an APEC study estimated that privacy protection provisions in digital trade agreements increase digitally ordered goods and services trade by 11.2% over two years after implementation.

How can privacy regulation be a barrier to digital trade?

Privacy regulation can impact digital trade by placing requirements or limits on the ability to move personal data across borders. Indeed, APEC Ministers acknowledged when endorsing the 1998 Blueprint for Action on Electronic Commerce, that the potential of electronic commerce cannot be realized without government and business cooperation "to develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy...". The need to ensure that domestic privacy regulation is not undermined when personal data is transferred to other APEC economies has led to requirements in domestic privacy laws that limit or condition in various ways cross-border transfers of personal data. For example, the EU General Data Protection Regulation (GDPR) prevents transfers of personal data to third parties unless that economy has received an 'adequacy finding' from the European Commission, which is an assessment that the economy receiving personal data provides essentially the same privacy protection as would accorded in the EU. In contrast, the US requires that companies transferring personal data across borders comply with applicable domestic privacy laws as well as their privacy policies. Australia has recently updated its Privacy Act which disallows personal data being disclosed to a recipient outside Australia unless 'reasonable steps are taken to ensure that the recipient complies with the Australia Privacy principles'. In addition, personal data can be transferred to economies the government includes on an approved list, without having to comply with any additional measures.

APEC work on privacy

APEC has produced two key outcomes when it comes to developing an APEC-wide approach to protecting privacy and facilitating cross-border transfers of personal data. The first was in 2005 and was updated in the 2015 APEC Privacy Framework, which is a set of information privacy principles. The second is the APEC Cross-Border Privacy Rules (CBPR), which builds on the APEC Privacy Framework and provides a mechanism for enabling transfers of personal data among participating APEC economies. These privacy outcomes have formed building blocks for digital trade commitments.

APEC Information Privacy Principles

1. **Preventing Harm** from misuse of personal data.
2. **Notice** - clear and easily accessible statement about privacy practices and policies.
3. **Collection Limitation**: collection of personal information should be limited to the information relevant to the purposes of collection.
4. **Uses of Personal Information**: personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes.
5. **Choice:** where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.
6. **Integrity of Personal Information:** personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
7. **Security Safeguards:** Personal information controllers should protect personal information that they hold with appropriate safeguards against risks.

8. **Access and correction**: individuals should be able to obtain confirmation of whether personal when it comes to their personal information, have communicated to them the personal information about them, and the ability to challenge the accuracy of personal information and as appropriate have the information rectified, amended or deleted.
9. **Accountability:** personal information controllers should be accountable for complying with measures that give effect to these Principles.

The APEC CBPR System

The APEC CBPR system is a government-backed data privacy certification mechanism that companies can join to demonstrate compliance with the APEC Privacy Framework. Participating APEC economies must demonstrate that CBPR program requirements will be legally enforceable against certified companies. To become certified, a company must demonstrate to an Accountability Agent—an independent CBPR System-recognized public or private sector entity— that they meet the CBPR program requirements, and that the company is subject to ongoing monitoring and enforcement. Certified companies must implement security safeguards for personal data that are proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context it is held. Accountability Agents receive and investigate complaints and resolve disputes between consumers and certified companies in relation to non-compliance with its program requirements. While governments may impose additional requirements with which certified companies must still comply, all participants must agree to abide by the 50 CBPR program requirements, facilitating the implementation of the same baseline protections across different legal regimes. The CBPR System also provides a mechanism for cooperation among authorities to enforce program requirements.

<u>The Global CPBR Forum</u>

The Global CPBR Forum was established in 2022 by Australia; Canada; Japan; Korea; Mexico; the Philippines; Singapore; Chinese Taipei; and the USA. The Objectives are to:

a. Establish an international certification system based on the APEC Cross Border Privacy Rules (CBPR)

b. Support the free flow of data and effective data protection and privacy;

c. Provide a forum for information exchange and cooperation on matters related to the Global CBPR and PRP Systems;

d. Periodically review data protection and privacy standards of members to ensure Global CBPR and PRP program requirements align with best practices; and

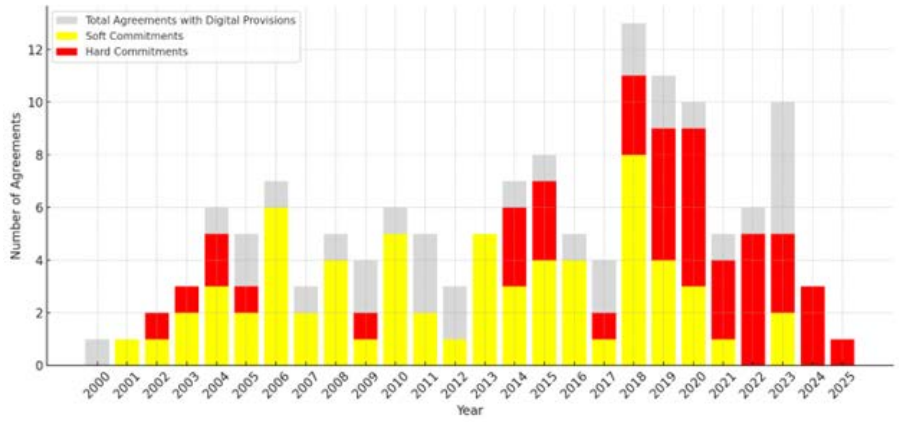
e. Promote interoperability with other data protection and privacy frameworks.

In 2023, APEC established the Global Cooperation Arrangement for Privacy Enforcement (CAPE). CAPE promotes cross-border cooperation between APEC economies and all participants in the Global CBPR Framework to support enforcement of data protection and privacy laws. On a voluntary basis, participants in CAPE have agreed to help with requests for assistance and to share information regarding enforcement of data privacy laws and policies that may target people or personal information controllers located in other members of the Global CBPR Forum. In January 2024, the U.S. Federal Trade Commission announced that it would participate in CAPE, providing added momentum for both CAPE and the APEC CBPR.

In June 2025 the Global CBPR Forum launched the Global CBPR and Privacy Recognition for Processors (PRP) certifications, marking a significant milestone for the Forum. These certifications provide a simple and transparent means for organizations to ensure the protection of personal information that moves across jurisdictions, fostering trust in cross-border data flows.

Digital Trade Commitments on Privacy

Commitments on Data Protection

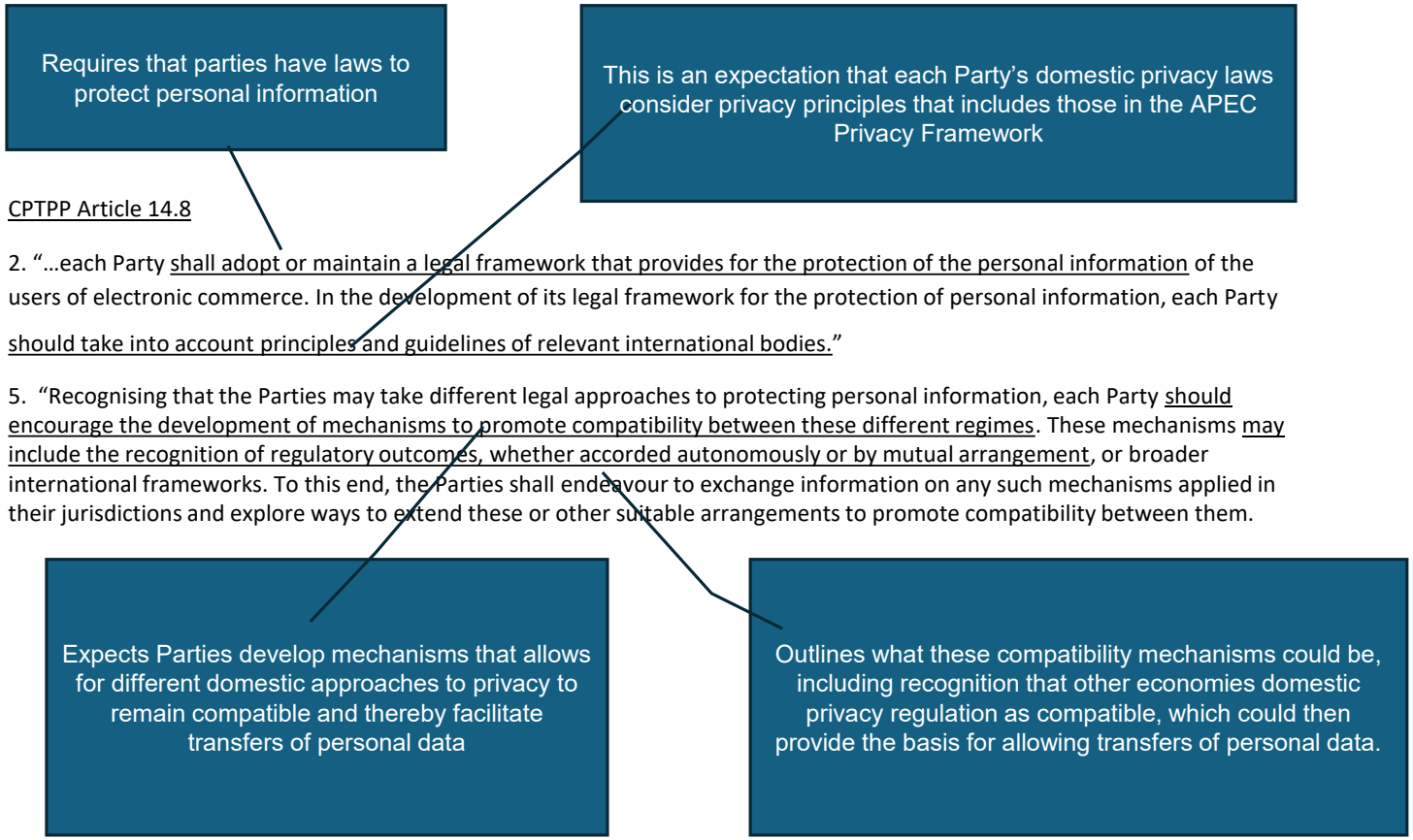


The share of digital trade agreements including such provisions has steadily risen, suggesting widespread recognition of data protection as a foundational component of digital trade. While soft commitments continue to dominate, hard commitments have emerged in more recent years, indicating a maturing legal approach.

APEC economies have undertaken a range of privacy commitments in digital trade agreements that reference and build on the APEC Privacy Framework on the goal of interoperability amongst privacy systems and the role of APEC CBPR in enabling this to happen. The following outlines the key privacy commitments and highlights the main differences.

Sample Privacy Provision

This sample **Protection of Online Personal Information** provision is taken from the **CPTPP** text.



Policy Checklist: Protection of Online Personal Information

Question	Consideration
Should a provision on Protection of Online Personal Information be included?	This is a threshold question. Privacy provisions are increasingly widespread and now appear in the WTO ECA as well as CPTPP, DEPA and RCEP to name a few.
Should it include a core commitment on adopting or maintaining a legal framework for the protection of personal information?	This commitment in trade agreements is typically binding such as in RCEP and CPTPP. This commitment is not included in the WTO ECA.
Should it include commitment to take account of international standards when adopting or maintaining a legal framework for the protection of personal information?	This core provision is hortatory. The key difference is whether to be expansive and refer to international standards, principles and guidelines as in RCEP, to refer to 'broader international frameworks' as in the WTO ECA, or just principles and guidelines as in CPTPP and USMCA. USMCA and the Australia-Singapore DEA refer specifically to the APEC Privacy Framework and OECD Guidelines on Privacy as examples of principles and guidelines.

Should it include commitments to promote compatibility between different privacy regimes with examples?	This is a core commitment. In CPTPP it is a binding commitment to promote compatibility and interoperability, whereas in the WTO ECA the commitment instead is hortatory. The WTO ECA has a binding commitment to encourage adoption of trustmarks as a valid interoperability mechanism, while USMCA and the Australia-Singapore DEA reference the APEC Cross-Border Privacy Rules System as a valid mechanism. In contrast, RCEP only includes a commitment to cooperate on the protection of personal information transfers from a Party.
Should it include a statement of key privacy principles?	USMCA and the Australia-Singapore DEA list key privacy principles, taken from the APEC Privacy Framework.
Should there be a commitment that restrictions on cross-border flow of personal data are necessary and proportionate to the risks?	This commitment is included as hortatory in USMCA and requires regulations affecting cross-border flows of information to be necessary i.e. least trade restrictive, and proportionate to the risk.
How does this relate to previous commitments on Protection of Online Personal Information?	If your economy has previously committed to a position on Protection of Online Personal Information, ensure that the provisions are consistent unless a change in policy is desired.

B2: Cybersecurity

What are cybersecurity provisions?

Cybersecurity provisions aim to strengthen cybersecurity capabilities and to deepen collaboration among APEC economies in addressing cybersecurity threats and harms.

How do cybersecurity commitments facilitate digital trade?

Cybercrime imposes direct and indirect costs on digital trade. Direct costs can include financial losses from theft, fraud, ransomware attacks, and the operational disruptions these cause. There are also costs to digitally delivered services that can be caused by malware, theft of personal information including banking data as well as corruption of the digital service that includes reputation harm. To address these risks of harm, companies must invest in cybersecurity infrastructure and regulatory compliance, particularly when operating across multiple jurisdictions with different data protection laws. Indirectly, cybercrime undermines trust in digital trade.

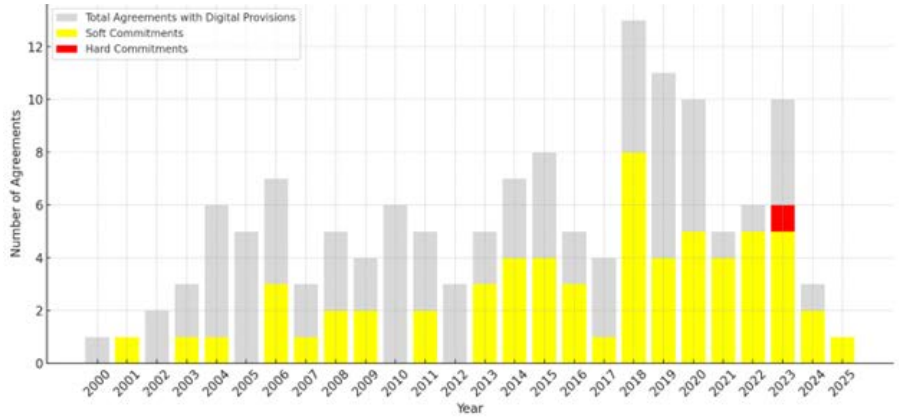
What are the economic benefits of cybersecurity provisions?

Strengthening cybersecurity and reducing cybercrime strengthens consumer and business trust in digital trade. A more secure digital environment also reduces costs to business from incident recovery, regulatory penalties, and insurance. These costs can be particularly burdensome for small and medium-sized enterprises (SMEs), which are also more vulnerable to cyber risks.

Stronger cybersecurity supports emerging sectors like telemedicine, e-learning, and AI-driven services. Stronger cybersecurity can also help foster greater regulatory cooperation and the development of secure interoperable systems that in turn, can reduce barriers to digital trade. The APEC study on the economic benefits of digital trade provisions estimated that cybersecurity provisions in trade agreements increased digitally deliverable services trade by 25% over 2 years. As the study notes, this benefit may be on the lower side once the benefits for digitally order but physically delivered goods are also taken into account.

Cybersecurity Commitments in Trade Agreements

Cybersecurity Provisions in Trade Agreements.



Cybersecurity provisions in trade agreements involving at least one APEC member have become more common since 2018. While commitments remain relatively modest as a share of total digital trade agreements, the number of agreements with both soft and hard commitments has increased steadily. This reflects growing recognition of the importance of cybersecurity in enabling trusted digital trade.

Key cybersecurity commitments are to build domestic cybersecurity capabilities and to collaborate in addressing cybersecurity risks.

Sample Cybersecurity Provision

This sample cybersecurity provision is taken from the WTO ECA.

WTO Members have made this a binding commitment to develop domestic capabilities and to collaborate in order to better identify and address cyber threats

USMCA Article 19.15 is a very similar cybersecurity commitment

WTO JSI Article 17

17.2 The Parties further recognize the evolving nature of cyber threats. In order to identify and mitigate cyber threats and thereby facilitate electronic commerce, the Parties shall endeavour to:

(a) build the capabilities of their respective national entities responsible for cybersecurity incident response; and

(b) collaborate to identify and mitigate malicious intrusions or dissemination of malicious code that affect a Party's electronic networks, to address cybersecurity incidents in a timely manner, and to share information for awareness and best practices.

17.3 Noting the evolving nature of cyber threats and their negative impact on electronic commerce, the Parties recognize the importance of risk-based approaches in addressing such threats while minimizing trade barriers. Accordingly, to identify and protect against cybersecurity risks, detect cybersecurity events, and respond to and recover from cybersecurity incidents, each Party shall endeavour to use, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on risk management best practices and on standards developed in a consensus-based, transparent, and open manner.

This commitments reflects a recognition of the need to balance addressing cyber threat using a risk- based approach while also minimizing trade barriers that can arise as a result.

This is hortatory commitment to use risk-base approaches. The commitment to “rely on” suggests a strong link between the domestic cyber measure and the risk management best practices and standards

Policy Checklist: Cybersecurity

Question	Consideration
Should a provision on cybersecurity be included?	This is a threshold question. Provisions have appeared in 64 agreements since 2001 and are now typically included in agreements where digital trade provisions are present.
Should it include a core commitment to build domestic cybersecurity capacity?	This is core provision found in all cybersecurity commitments, and is typically one of 'best endeavors'.
Should it include a core commitment to collaborate with other economies to identify and mitigate malicious intrusions and address cybersecurity incidents in a timely manner?	This is core provision found in all cybersecurity commitments and is typically one of 'best endeavors'.
Should it include commitments to workforce development in the area of cybersecurity?	This provision is found in the DEPA for example and aims to address challenges economies have in finding the skills needed to build domestic cybersecurity capacity.
Should it include a commitment to use risk-based approaches to addressing cybersecurity threats while minimizing trade barriers?	This commitment is found in the WTO ECA and aims to ensure that cybersecurity measures don't become unnecessary restrictions on trade and develop according to international best practice.
How does this relate to previous commitments on cybersecurity?	If your economy has previously committed to a position on cybersecurity, ensure that the provisions are consistent unless a change in policy is desired.

B3: Consumer Protection

What are Consumer protection provisions?

Consumer protection provisions in trade agreements facilitate trust and increased use of B2C cross-border e-commerce.

How do consumer protection provisions facilitate digital trade?

Online consumer protection provisions in digital trade agreements enhance digital trade by building consumer trust, especially in cross-border transactions. Clear rules on disclosures, returns, and dispute resolution reduce uncertainty and risk, encouraging more people to engage in cross-border e-commerce. This is especially important as the OECD has identified lack of trust as one of the most significant barriers to digital trade.

For businesses, particularly small and medium enterprises (SMEs), transparent consumer protection laws and cooperation among consumer protection agencies that strengthen enforcement can make it easier to operate across multiple jurisdictions. Trade agreements that include consumer protection provisions (like CPTPP, USMCA, and DEPA) help firms scale more efficiently and can incentivize e-commerce platforms to vet sellers and monitor marketplace integrity, improving product quality and consumer satisfaction.

What are the economic benefits from digital trade commitments on consumer protection?

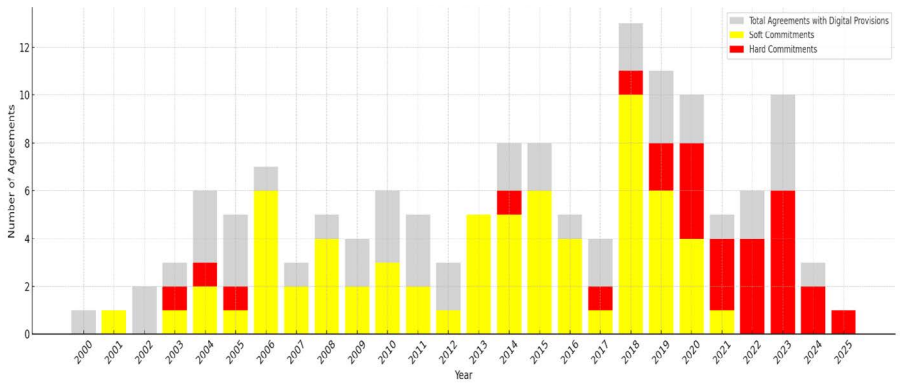
The APEC study on the economic benefits of digital trade provisions found that provisions that increase consumer protection including with specific consumer protection provisions increased digitally ordered products by over 21% in the next two years following adoption.

What are the main barriers to consumer protection in digital trade?

Effective consumer protection when it comes to digital trade and specifically cross-border e-commerce faces barriers such as legal uncertainty and weak enforcement. Consumers often don't know which economy's laws apply or how to pursue redress if something goes wrong, and even when rights exist, enforcing them across borders is often slow, costly, or impractical. The absence of accessible online dispute resolution systems further discourages consumers from seeking help, reducing trust and limiting participation in digital trade.

Other key challenges include inconsistent consumer protection standards between economies. Varying rules on returns and warranties for instance can create confusion and compliance burdens, while unclear or misleading information from sellers undermines consumer confidence when it comes to cross-border e-commerce.

Commitments on Consumer Protection



Commitments on consumer protection have grown steadily since 2003, with a notable rise in the number of hard commitments from 2014 onwards. While soft commitments were dominant in earlier years, recent agreements increasingly include hard provisions, indicating a growing willingness to codify enforceable rules in this area. By the early 2020s, consumer protection commitments were present in most digital trade agreements, comprising a substantial portion of all digital-related provisions.

Key consumer protection commitments are to adopt or maintain consumer protection laws and strengthen cooperation among the Party's consumer protection agencies. Ensuring that each economy has consumer protection laws strengthens trust in digital trade for consumers and cooperation among agencies is needed to address the various challenges outlined above when it comes to enforcing consumer rights and complying with consumer protection laws in the context of digital trade. Some trade agreements such as the WTO ECA and DEPA go further and list the requirements that consumer protection laws should address such as requiring goods to be delivered in an acceptable and satisfactory quality and provide consumers with appropriate redress.

Sample Consumer Protection Provision

This sample Consumer Protection provision is taken from the WTO ECA.

Article 14: Online Consumer Protection

14.1 For the purposes of this Article, "misleading, fraudulent, and deceptive commercial activities" include:

(a) making material misrepresentations[11], including implied factual misrepresentations, or false claims as to matters, such as the qualities, price, suitability for purpose, quantity, or origin of goods or services;

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

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

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

14.2 The Parties recognize the importance of transparent and effective measures that enhance consumer confidence and trust in electronic commerce. To this end, each Party shall adopt or maintain measures to proscribe misleading, fraudulent, and deceptive commercial

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

[10] For the purposes of this subparagraph, the Parties recognize that an Internet access service supplier that offers certain content only to its end-users would not be acting inconsistently with this principle.

[11] For the purposes of this Article, "material misrepresentations" means misrepresentations that are likely to affect a consumer's conduct or decision to use or purchase a good or service.

activities that cause harm, or potential harm, to consumers engaged in electronic commerce.[12]

14.3 To protect consumers engaged in electronic commerce, each Party shall endeavour to adopt or maintain measures that aim to ensure:

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

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

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

14.4 The Parties recognize the importance of affording to consumers engaged in electronic commerce consumer protection at a level not less than that afforded to consumers engaged in other forms of commerce.

14.5 The Parties recognize the importance of cooperation between their respective consumer protection agencies or other relevant bodies, including the exchange of information and experience, as well as cooperation in appropriate cases of mutual concern regarding the violation of consumer rights in relation to electronic commerce in order to enhance online consumer protection, where mutually decided.

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

Policy Checklist: Consumer Protection

Question	Consideration
Should a provision on Consumer Protection be included?	This is a threshold question. Consumer Protection provisions have appeared in almost 100 agreements since 2001 and are now typically commonly included.
Should it include a commitment to adopt or maintain domestic consumer protection laws for e-commerce?	This is a core provision that could either be binding (e.g. shall), qualified (e.g. endeavour to) or not included. It is now common for this core provision to be binding.
Should it include commitments on the content of what consumer protection laws should provide when it comes to e-commerce?	This an increasingly common and binding provision, found in the WTO ECA as well as DEPA.
Should it include commitments to promote cooperation on consumer protection for e-commerce?	This is an increasingly common provision. Trade agreements often have consumer protection chapters where cooperation is addressed in detail and can be applied to e-commerce, such as the CPTPP and RCEP, whereas DEAs require additional commitments on cooperation.
Should it include a commitment that the level of protection provided to consumers for e-commerce be no less than that for online commerce?	This provision, such as the one found as a hortatory statement in the WTO ECA, aims to avoid different standards of protection that disadvantage consumers engaged in online commerce versus other forms of commerce.
How does this relate to previous commitments on Consumer Protection?	If your economy has previously committed to a position on Consumer Protection, ensure that the provisions are consistent unless a change in policy is desired.

B4: Unsolicited commercial messages

What are unsolicited commercial messages?

Unsolicited commercial messages—sometimes called "spam"—are electronic messages sent for marketing or promotional purposes to people who haven't asked to receive them. These messages are typically delivered by email, and are often sent in bulk. A key feature of unsolicited commercial messages is that the recipient has not given their consent or has already requested not to receive such communications.

Trade agreements usually define these messages as those sent for commercial or marketing purposes without being requested by the recipient. Consent of the recipient is the central feature of trade agreement commitment on spam.

What are the economic benefits from unsolicited commercial messages?

The adoption of provisions that build consumer trust and confidence in e-commerce, including those that specifically target the reduction of spam, has shown a **statistically significant and positive relationship with the flow of digitally ordered goods and services.** The adoption of such provisions in APEC economies is linked to an **increase of 32.5% in digitally ordered trade value over the subsequent two years** following its implementation. This is a substantial gain against the volume of exports in the year the provision comes into force.

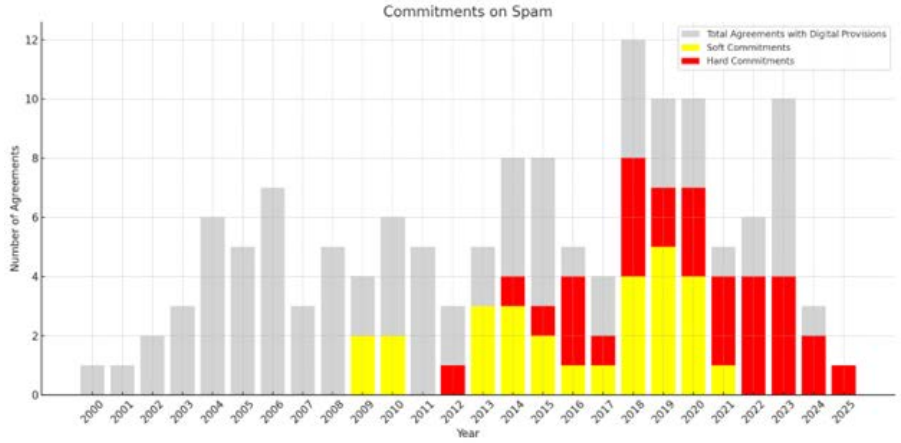
What are the main barriers to unsolicited commercial messages?

The biggest challenge with unsolicited commercial messages is the potential for abuse. When businesses or individuals send mass messages without consent, it leads to consumer frustration, privacy violations, and cybersecurity risks (such as phishing scams). Inconsistent or unclear rules across economies can also create confusion for businesses that operate internationally.

From a trade perspective, the lack of common standards or enforcement mechanisms makes it harder to manage cross-border complaints or regulate bad actors. Without proper safeguards, spam can flood communication networks, reduce productivity, and damage trust in digital transactions. That's why modern rules aim to empower consumers, clarify responsibilities for businesses, and enable legal remedies for misuse.

Unsolicited commercial messages in trade agreements

Commitments on Spam



Commitments on spam regulation began appearing around 2009, with a marked increase in both soft and hard provisions after 2014. From 2017 onward, hard commitments have dominated over soft ones, indicating a stronger legal orientation toward combating spam. The proportion of agreements with spam provisions has grown steadily, with more than half of recent digital trade agreements incorporating such measures.

These rules are typically found in the e-commerce or digital trade chapters of agreements like the CPTPP, RCEP, and DEAs such as the Australia–Singapore Digital Economy Agreement.

Provisions on spam usually require economies to adopt or maintain laws that:

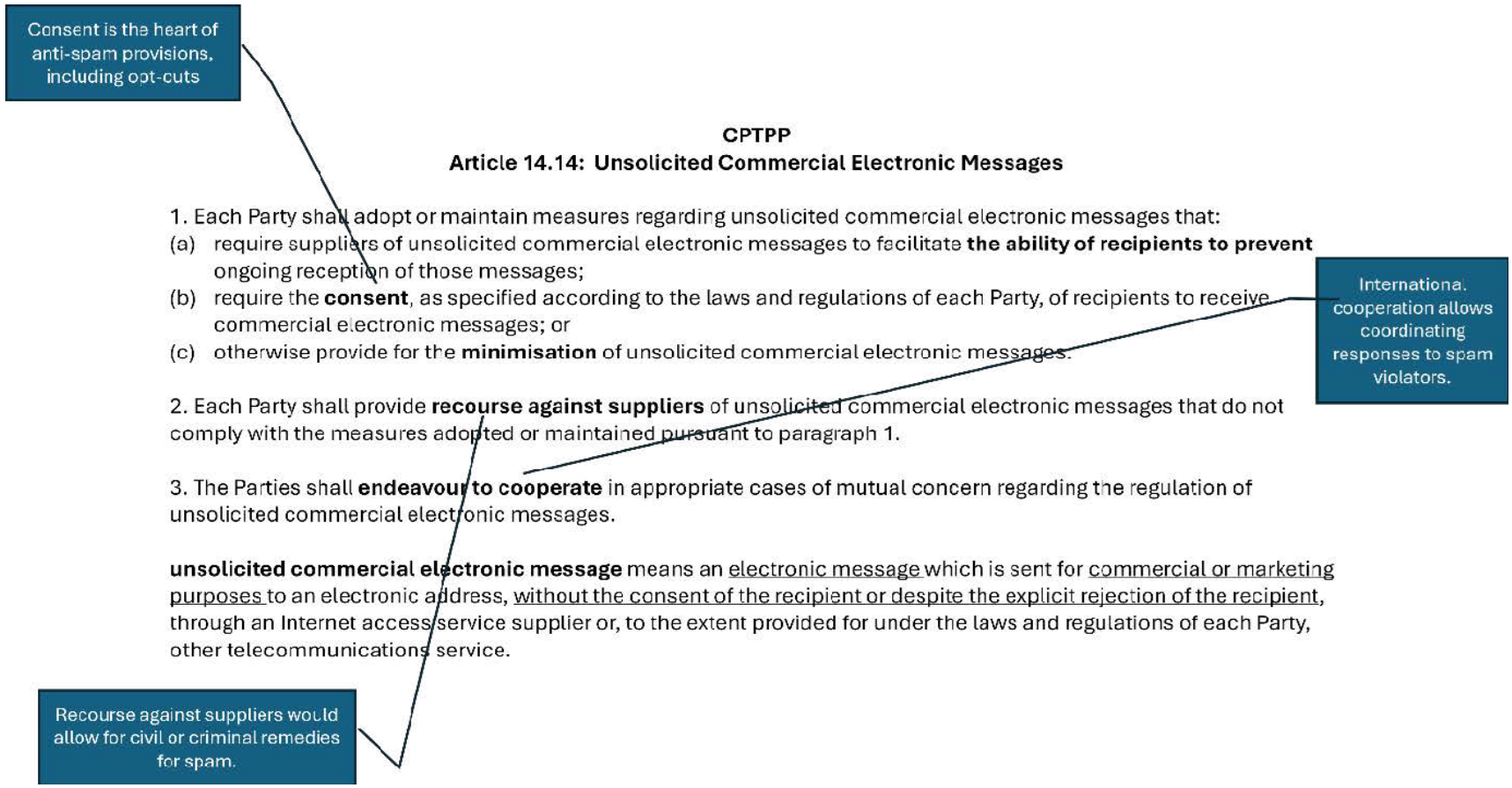
- Give consumers the ability to stop receiving unwanted messages,
- Ensure that consent is required before sending such messages,
- Mandate transparency (e.g., identifying the sender and offering opt-out options), and

More recently, trade agreements include requirements that the parties will provide legal recourse, for example civil remedies or criminal penalties, against senders who violate the rules. As some legal systems do not yet provide these remedies, these obligations are sometimes qualified by 'endeavour to ensure' or similar language, which requires parties to make reasonable efforts.

Many trade agreements also encourage cooperation between economies to share best practices and handle cross-border issues, as spam often originates from multiple economies. As such, international cooperation and coordination is an important part of minimising the prevalence of unsolicited commercial messages.

Sample Unsolicited Commercial Messages Provision

This sample unsolicited commercial messages provision is taken from the CPTPP text.



Policy Checklist: Unsolicited commercial messages (Spam)

Question	Consideration
Should a provision on unsolicited commercial messages be included?	This is a threshold question. Spam provisions have appeared since 2009 and are now typically included in more than half of all trade agreements where digital trade provisions are present.
Should it include commitments on consumer consent for unsolicited commercial messages?	This provision could either be binding (e.g. shall), qualified (e.g. endeavour to) or not included. It is common for this provision to be binding.
Should it include commitments on recourse against senders of unsolicited commercial messages?	This provision could either be binding (e.g. shall), qualified (e.g. endeavour to) or not included. It is common for this provision to be binding or endeavours.
Should it include more detailed commitments on spam regulation?	Further detailed regulation such as requiring opt-out free of charge are common. This provision could be either binding (e.g. shall), qualified (e.g. endeavour to) or not included.
Should it include agreement to cooperate on issues of mutual concern?	It is common for cooperation to be included given the cross-border nature of spam.
How does this relate to previous commitments on unsolicited commercial messages?	If your economy has previously committed to a position on unsolicited commercial messages, ensure that the provisions are consistent unless a change in policy is desired.

Section C: Data Flows

C1: Cross-border Data Flows

What are commitments on cross-border data flows?

Commitments to cross-border flows of information enable digital trade while balancing the scope for governments to restrict data flows for legitimate public policy reasons.

Data is foundational for digital economies and for engaging in digital trade. According to the McKinsey Global Institute, global data flows grew at nearly 50 percent per annum between 2010-2019 and around 40 percent annually between 2019-2021. The OECD notes that the creation of economic and social value increasingly depends on the ability to move and aggregate data across a number of locations scattered around the globe. This includes global e-commerce which relies on digital search and ordering as well the online cross-border delivery of services. Indeed, the global B2B e-commerce market was valued at USD 36 trillion in 2026 with manufacturing, energy, healthcare and professional business services driving sales, with the Asia-Pacific region gaining most market share.[19]

Global B2C e-commerce is expected to reach USD 5.5. trillion by 2027 with significant growth in APEC economies such as Canada; China; Indonesia; Mexico; Russia; and the US. Cross-border e-commerce requires the ability to collect customer data, fast and cost-effective electronic payments, and efficient customs and delivery services, which also rely on cross-border data flows to track and trace goods to their destination. The World Bank has highlighted the role of data flows in enabling supply chains. Data is also an input into manufacturing operations, where data is used to train robots and deepen insights into operations to increase operational efficiencies. Cross-border information flows also give small businesses access to professional business services in the cloud, such as software and AI. Allowing cross-border information flows also support development outcomes, provides growth opportunities for platform-based business models in low- and middle-income economies.

19 US International Trade Administration B2B e-Commerce Forecast https://www.trade.gov/ecommerce-sales-size-forecast

Economic benefits of cross border information flows and in avoiding data localisation requirements

A 2025 OECD/WTO paper estimates that eliminating the ability to move data across borders would lead to global GDP losses of 4.5% and a reduction in exports of 8.5%. Another study assessed the GDP impact of removing restrictions on cross-border data flows and found that on average, service imports would increase by five percent, benefitting domestic companies and consumers through access to cheaper and better international services, and lead to an average increase in Total Factor Productivity of 4.5 percent.

In other modeling of the economic impacts of restrictions on cross-border data flows, increases in regulations restricting data flows negatively impacted an economy's trade and its productivity, while increasing prices. In the model, a one-unit increase in a economy's Digital Services Trade Restrictiveness Index (calculated using data from the OECD Product Market Regulation database) was associated with a seven percent decrease in gross output traded, a 2.9 percent decrease in the productivity of downstream industries, and a 1.5 percent increase in the price of goods and services from these industries, such as finance and insurance, petroleum, computers and electrical equipment, and chemicals.

What are the barriers to allowing cross-border information flows?

Governments have a range of reasons for wanting to restrict or place conditions on flows of information across borders. These data flows restrictions can be grouped into four categories:

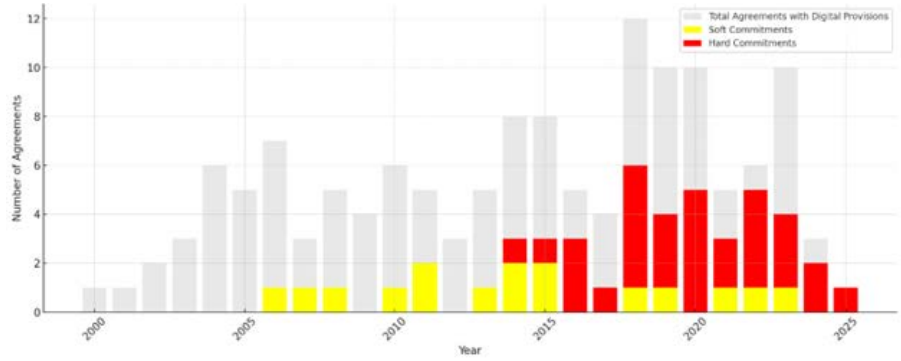
- To preserve domestic regulatory standards. For example, privacy regulation can prevent personal data being sent to another APEC economy, or condition these information flows on the receiving economy providing similar levels of privacy protection.
- Security concerns can lead governments to restrict access to information or require data to be localized. For example, governments might require data localisation of sensitive or secure data, or block access to information for domestic security purposes.
- Industrial policy and/or competition policy goals where data is required to be localized in order to compel investment in local data centers and to limit data flows in order to protect domestic companies from competition with online suppliers from other APEC economies.

The G20 approach to cross-border information flows

In 2019 G20 leaders recognized that "data free flow with trust will harness the opportunities of the digital economy."[20] The following year in Saudi Arabia, G20 Leaders noted "the importance of data free flow with trust and cross-border data flows," a formulation also repeated by Leaders during the Italian G20 in 2021 and Indonesian G20 in 2022.[21] The G7 has also provided guidance on how to support data flows and digital trade, with the G7 Digital Trade Principles in 2021 which state that "data should be able to flow freely across borders with trust" and identify the need to balance opportunities from data flows with domestic regulation.[22]

Cross-border information flows in trade agreements

Commitments on Data Flows

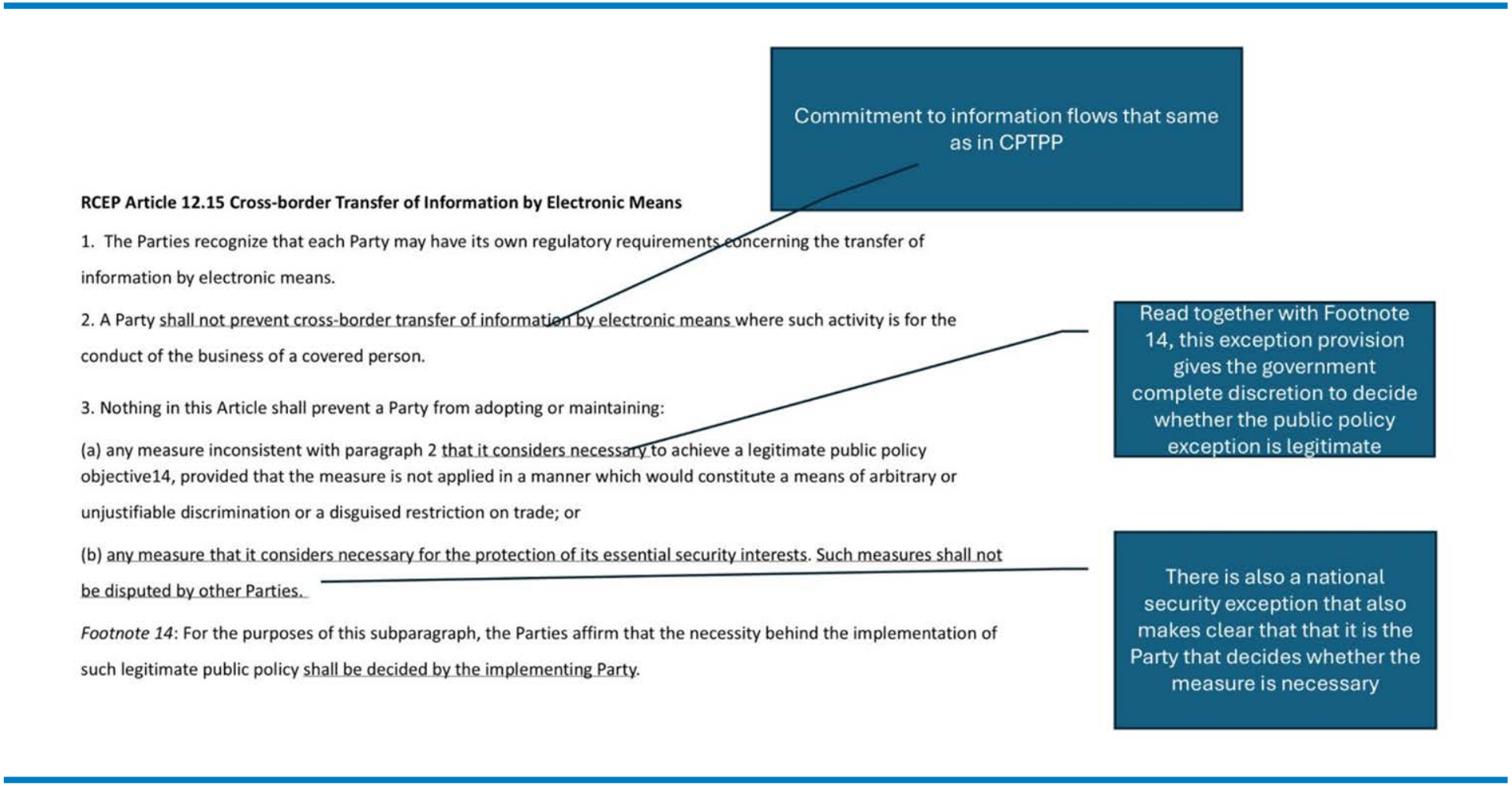


From 2014 onwards, both soft and hard commitments began to emerge, with hard commitments seeing a sharp rise beginning in 2016. By the late 2010s and early 2020s, hard commitments on cross-border data flows outnumbered soft commitments, reflecting a growing confidence among economies to bind themselves to enforceable digital trade rules.

20 G20 Osaka Leader's Declaration, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html
21 G20 Saudia Arabia Leaders' Declaration para 19, November 21, 2020, https://www.g20.utoronto.ca/2020/2020-g20-leaders-declaration-1121.html ; G20 Rome Leaders' Declaration para 48, http://g20italy.org/wp-content/uploads/2021/10/G20-ROME-LEADERS-DECLARATION.pdf; G20 Bali Leaders' Declaration, para 24 https://www.g20.org/wp-content/uploads/2024/09/2022-11-16-g20-declaration-data.pdf
22 G7 Digital Trade Principles, 22 October 2021 https://www.gov.uk/government/news/g7-trade-ministers-digital-trade-principles

Sample Cross-Border Data Flows Provision

This sample Cross-Border Information Flow provision is taken from the **RCEP** text.



Policy Checklist: Cross-Border Data Flows

Question	Consideration
Should a provision on Cross-Border Data Flows be included?	This is a threshold question. Cross-Border Data Flows provisions have appeared since 2006 and are now typically included in trade agreements with digital provisions.
Should it include commitments to cross-border data flows?	This is the core provision and is typically binding. It can be phrased either as a commitment to allow cross border transfers of information as in CPTPP or to not prohibit or restrict these transfers, as in USMCA. The latter commitment is more aligned with the architecture of the internet where data flows freely unless governments intervene and restrict data flows.
	Many commitments to cross-border information flows such as in CPTPP and RCEP include a specific exception provision that provides more flexibility to regulators to restrict data flows than a GATS article XIV style exception provision that also typically applies to digital trade commitments.
Should it include a specific exception provision?	Many commitments to cross-border information flows such as in CPTPP and RCEP include a specific exception provision that provides more flexibility to regulators to restrict data flows than a GATS article XIV style exception provision that also typically applies to digital trade commitments.
How does this relate to previous commitments on Cross-Border Data Flows?	If your economy has previously committed to a position on Cross-Border Data Flows, ensure that the provisions are consistent unless a change in policy is desired.

C.2 Data Localisation

What are commitments on data localisation?

Data localisation requires data to be kept local, often in domestic data centers. The digital trade commitment is to not require data to be localized as a condition of doing business.

Economic benefits of cross border information flows and in avoiding data localisation requirements.

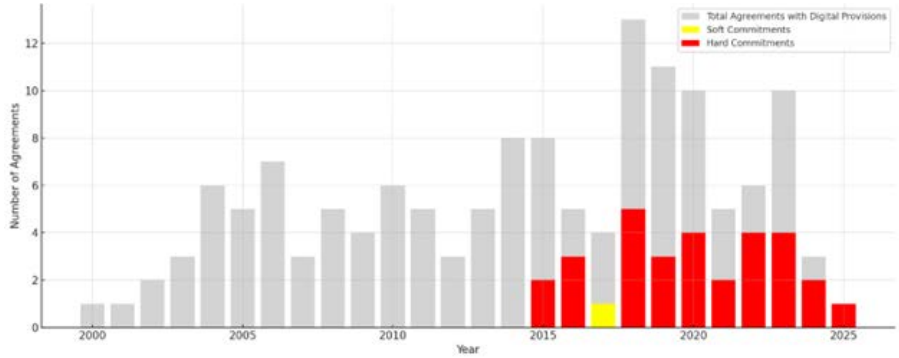
Not requiring data localisation as a condition for conducting business allows businesses to use global cloud infrastructure rather than building or leasing local data centers in every market, lowering fixed costs, improving scalability, and enabling more efficient trade in digital services, particularly for SMEs. A Leviathan Security Group study in 2016 estimated that data localisation measures raise firms' cost of hosting data by 30-60%.

What are the barriers to allowing cross-border information flows and avoiding data localisation requirements?

According to a 2023 OECD study nearly 100 data localisation measures were in place across 40 economies and that more than half of these have emerged in the last decade. Data localisation measures are also increasingly restrictive. Again according to the OECD, data localisation measures can raise data management costs by 15-55%, leading to higher prices for downstream users of data centers as well as reduced resilience.

Data localisation requirements are being introduced for a variety of reasons. Key ones are to reduce cybercrimes, address concerns about how personal data is treated in their economies and to ensure that regulators have access to data needed to achieve their regulatory goals. Data localisation requirements can also be used to require the development of local data centers.

Commitments on Data Localisation



The inclusion of data localisation provisions in digital trade agreements has grown significantly in recent years. From 2015 onwards, there has been a sharp increase in hard commitments—legally binding restrictions on forced data localisation—peaking in 2018–2023, aligning with the proliferation of digital economy agreements and more ambitious digital chapters in FTAs. Notably, almost no agreements before 2015 addressed this issue, indicating how recent and rapidly evolving this policy area is.

The key commitment is to not require use of local computing facilities as a condition for doing business in that Party's territory. In some trade agreements such as CPTPP the data localisation commitment does not apply to financial services providers. The USMCA applies data localisation to financial services providers but balances this commitment with the requirement that financial regulators have "immediate, direct, complete and ongoing access to the data."

Sample Data Localisation Provision

This sample data localisation provision is taken from **USMCA**.

USMCA Article 17.18: localization of computing facilities for financial information

1. The Parties recognize that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on that access.

2. No Party shall require a covered person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory, so long as the Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party's territory.

3. Each Party shall, to the extent practicable, provide a covered person with a reasonable opportunity to remediate a lack of access to information as described in paragraph 2 before the Party requires the covered person to use or locate computing facilities in the Party's territory or the territory of another jurisdiction.

Upfront statement of the regulatory need for access to information

Commitment not to require data localization but conditional on regulators have "immediate, direct, complete and ongoing access" to information

This commitment balances giving 'covered persons' a 'reasonable opportunity' to remediate a situation where the access to information is not consistent with subparagraph two before requiring data to be localized

Policy Checklist: Data Localisation

Question	Consideration
Should a provision on Data Localisation be included?	This is a threshold question. Data Localisation provisions have appeared since 2015 and are now frequently included in trade agreements containing digital provisions.
Should it include commitments to not require data localisation as a condition of doing business in a Party's territory?	This is the core provision and is typically binding.
Should it include a specific exception provision?	Many commitments to data localisation such as in CPTPP and RCEP include a specific exception provision that provides more flexibility to regulators to restrict data flows than a GATS article XIV style exception provision that also typically applies to digital trade commitments.
When it comes to the financial service providers, should the no data localisation apply as in USMCA or not apply at all as in CPTPP and RCEP?	USMCA provides an example of how to balance the economic benefits from a no data localisation requirement while ensuring financial regulators have access to the timely data needed for regulatory purposes.
How does this relate to previous commitments on data localisation?	If your economy has previously committed to a position on Data Localisation, ensure that the provisions are consistent unless a change in policy is desired.

C3: Access to source code

What is access to source code?

Source code refers to the lines of code written by programmers to instruct a machine to perform a given task and can include the model weights in AI models which are the parameters of a neural network that determine how the AI model process input data to generate outputs.

What are the economic benefits from access to source code?

A trade commitment to not require access to source code as a condition of market access gives businesses confidence that they will not need to disclose proprietary software, algorithms, or AI model weights to other governments, thereby reducing the risk of IP theft and forced technology transfer. This protection makes businesses more willing to sell, license, or deliver digital products and services across borders, expanding market opportunities and boosting digital trade.

What are the reasons that governments might want access to source code?

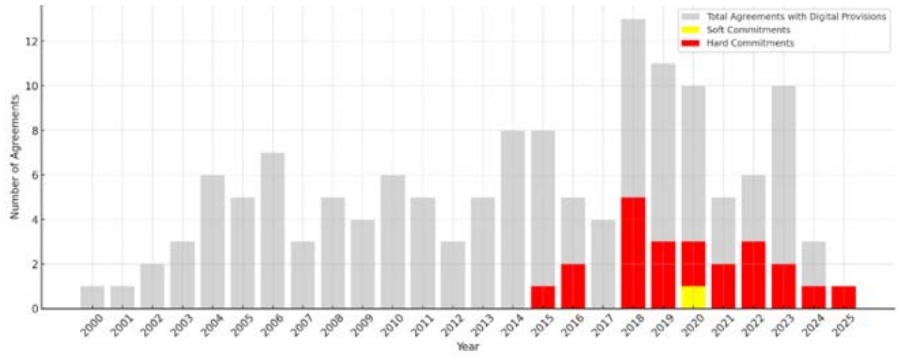
There are a range of legitimate reasons for governments to require access to source code. Some of the main ones are:

- Regulatory and judicial needs: where access is required to regulate or enforce laws relating to competition, privacy, non-discrimination or bias, or product safety laws.
- Consumer protection: where access is needed to ensure that the operation of the software or AI is consistent with consumer protection standards and requirements.
- Understanding security risks: ensuring that software performs as claimed and does not impose security risks.

The key regulatory challenge is to balance the digital trade enhancing opportunities from prohibiting access to source code while giving governments access to source code for legitimate goals.

Access to source code in trade agreements

Commitments on Access to Source Code



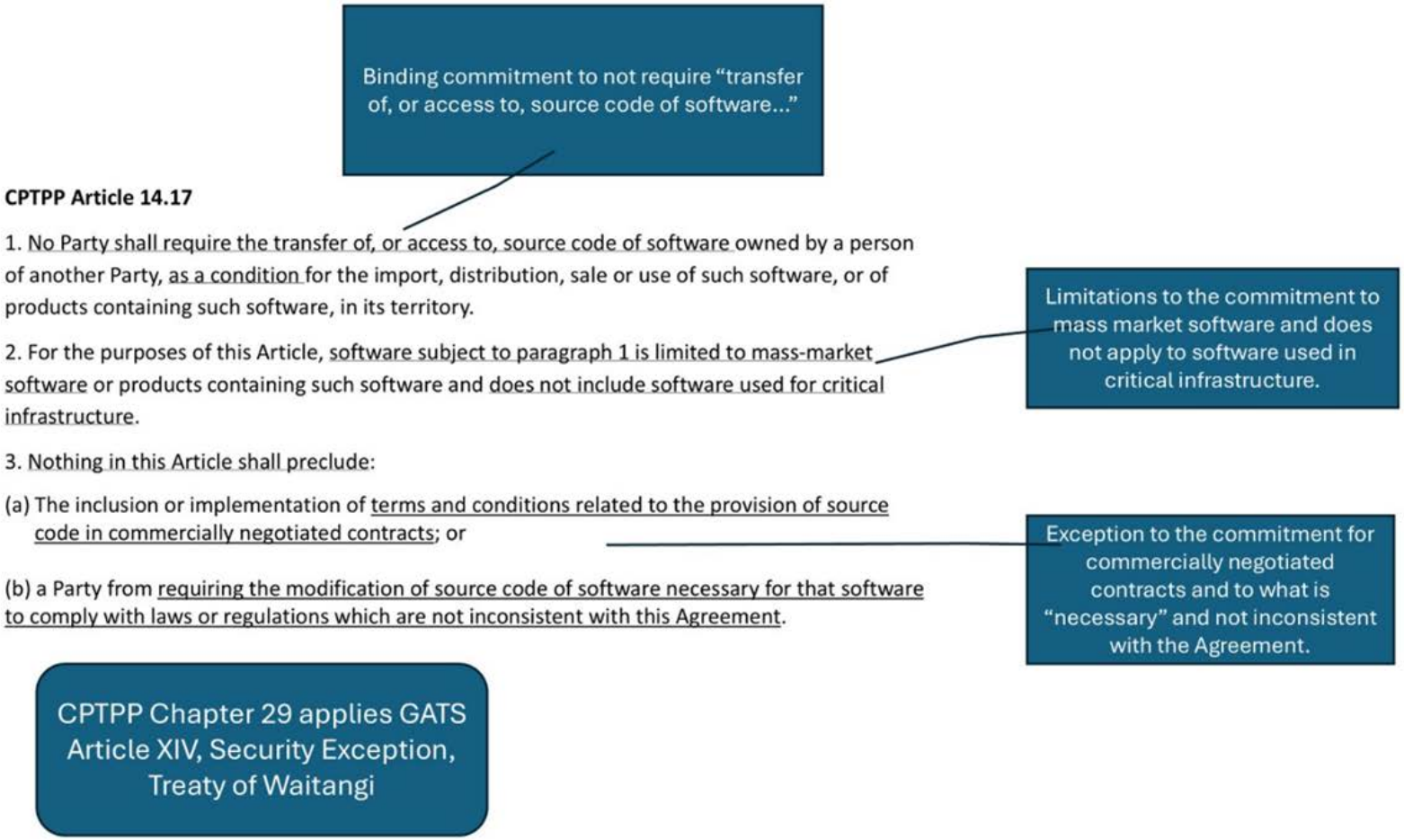
Commitments on access to source code began appearing in trade agreements around 2015, with hard commitments dominating from the outset. While there is some fluctuation, recent years (2018–2023) show a consistent trend of including hard commitments, although the overall frequency has slightly declined. Soft commitments remain rare in this area, suggesting a preference for binding language when source code provisions are included.

The key commitment is to not require the transfer to or access to source code of software as a condition for trade.

Various trade agreements include exceptions to this, including for critical infrastructure projects, requirements for access to source code that are the result of commercially negotiated contracts, and requiring access to source code to a regulatory body for investigations, enforcement action and judicial proceedings.

Sample Source Code Provision

This sample source code provision is taken from the **CPTPP** text.



Policy Checklist: Access to Source Code

Question	Consideration
Should a provision on source code be included?	This is a threshold question. Provisions have appeared since 2008 and are included in a small number of trade agreements.
The core commitment is to not require access to source code of software as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory?	When a commitment on source code is included, this is the core provision and is always binding.
Should the commitment to not requiring access to source code be limited to mass-market software or clarify that access to source code can be included in commercially negotiated contracts?	Both these limitations to the core commitment were included in CPTPP, but not in USMCA. The Australia-Singapore DEA states that the commitment does not prevent requiring access to source code in commercially negotiated contracts which raises the question as to what is a non-commercial or non-negotiated contract, and when this is not mass-market software.

Under what circumstances can a Party require modification or preservation of source code?	CPTPP allows a Party to require modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with the agreement. USMCA and the UK-Japan Comprehensive Economic Partnership refined and tightened the approach in CPTPP by allowing regulatory and judicial authorities to require a person to preserve and make available the source code of software or 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.
How does this relate to previous commitments on Access to Source Code?	If your economy has previously committed to a position on Access to Source Code, ensure that the provisions are consistent unless a change in policy is desired.

Section D:
Emerging Issues

D1: Artificial Intelligence

What is artificial intelligence?

The Organisation for Economic Co-operation and Development (OECD) defines an "AI system" as "a machine based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".[23]

What are the economic benefits from artificial intelligence?

According to PwC's Global Artificial Intelligence Study, with accelerated development and uptake of AI, global GDP could be 14 percent or almost USD 16 trillion higher by 2030. According to Goldman Sachs, LLMs could raise global GDP by 7 percent and lift productivity growth by 1.5 percent over 10 years.[24]

AI is also expected to expand international trade in various ways. For example, AI can reduce trade costs including by making customs more efficient as AI is used to improve custom's risk-based targeting of imports.[25] AI chatbots can overcome language barriers, increasing opportunities for AI-enabled services. For example, eBay's machine translation service has led to a 17.5% increase in exports to Spanish-speaking Latin America.[26] AI driven insights and analytics can also strengthen supply chains by identifying risks and optimizing routes.[27]

Allowing trade in AI also provides access to the types of models best calibrated to be trained on the available data in order to serve the local market.[28]

23 OECD2024
24 Generative AI Could Raise Global GDP by 7%. https://www.goldmansachs.com/intelligence/pages/generative-ai-could-raise-global-gdp-by-7-percent.html
25 WTO/WCO Study Report on Disruptive Technologies, June 2022
26 Brynjolfsson, E, X Hui, and Meng Liu (2018), "Does Machine Translation Affect International Trade? Evidence from a Large Digital Platform
27 Trading with Intelligence: How AI shapes and is shaped by international trade, WTO 2024
28 Brooke Tanner and Cameron Kerry, Can small language models revitalize Indigenous languages?, Brookings. March 19, 2025 https://www.brookings.edu/articles/can-small-language-models-revitalize-indigenous-languages/

Why is AI a trade issue?

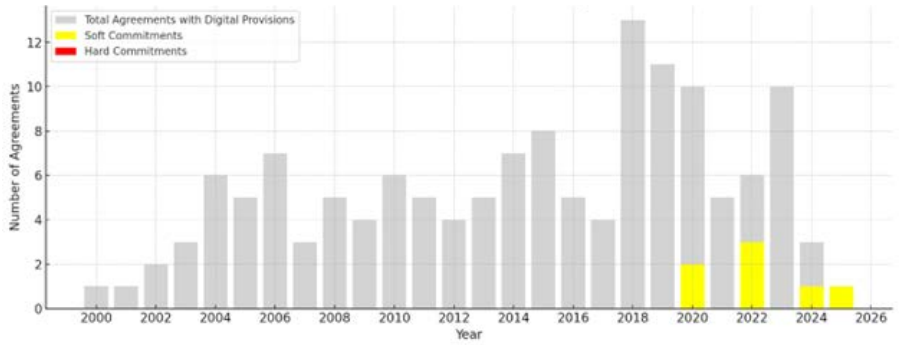
Different domestic AI regulations can create barriers and increase the cost of trade in AI - whether embedded in a product or as a service. Addressing regulatory diversity, such as by developing international AI standards and using these as a basis for domestic AI regulation, are ways that trade agreements can balance achieving legitimate domestic regulatory goals while minimizing the trade costs of regulatory diversity. Developing mutual recognition of AI testing and certification requirements is another area where trade agreements can help.

Various existing digital trade commitments can also support trade in AI. For example, AI requires access to data, which can be located domestically and overseas. Commitments to cross-border data flow can therefore enable development of AI.

Access to AI computing is increasingly located in the cloud is also critical. Trade commitments to avoiding data localisation requirements can reduce the cost of access to AI compute. Commitments by governments in trade agreements to protecting the IP in AI models, including the source code and model weights, also reduces the risk of trade in AI goods and services.

Artificial Intelligence in trade agreements

Commitments on Artificial Intelligence



AI specific commitments in trade agreements have only recently emerged, with the first soft provisions appearing from 2020 onward. There have been no hard commitments to date, and the number of soft commitments remains modest, though increasing slightly in recent years. This reflects the evolving nature of AI governance in trade, with economies beginning to explore cooperation while avoiding binding obligations.

An increasingly common AI commitment is to recognize the importance of developing ethical and governance frameworks for trusted safe and responsible use of AI and the need to align such frameworks, such as taking

into consideration international standards and guidelines on AI, which in the case of the NZ-UK FTA includes a specific reference to the work of the OECD and the Global Partnership on AI (GPAI). This aims to address the need for AI governance on the one hand and the need to avoid divergent regulatory outcomes that become barriers to trade in AI. Another commitment aims to deepen international cooperation on AI innovation and research. The Australia-Singapore DEA and NZ-UK FTA for instance includes a commitment to share research and industry best practice and encourage commercialisation opportunities and collaboration between researchers, academics and industry.

Sample AI Provision

This sample AI provision is taken from the **Australia-Singapore DEA.**

Policy Checklist: Artificial Intelligence

Question	Consideration
Should a provision on Artificial Intelligence be included?	This is a threshold question. Artificial Intelligence provisions have appeared in 7 trade agreements since 2020. While not commonly included, their inclusion is growing.
Should it include commitments that recognize the importance of developing ethical and governance frameworks for trusted safe and responsible use of AI, and the need for such frameworks to be internationally aligned?	This core provision is typically a best endeavors commitment. There are two approaches to this commitment in trade agreements so far. One is to "recognize' the importance of developing ethical government frameworks for trusted, safe and resulting use of AI technologies, as in the Australia-Singapore DEA and DEPA. The other is to agree to "endeavor to develop" these frameworks, as in the NZ-UK FTA.
Should a provision supplement the core commitment above with a commitment to take into consideration or take into account internationally-recognized principles or guidelines?	This core provision is typically best endeavours. It could however include a reference to the work of the OECD and GPAI. The NZ-UK FTA also includes a commitment to use risk-based or outcomes based approaches tor regulation that take into account industry-led standards.
Should it include a commitment to participate activity in international fora?	This commitment in the Australia-Singapore DEA supplements the commitment to take into account international guidelines.
How does this relate to previous commitments on AI?	If your economy has previously committed to a position on AI, ensure that the provisions are consistent unless a change in policy is desired.

D2: Cryptography

What is cryptography?

The Australian DEA defines cryptography as "the principles, means or methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorised use; and is limited to the transformation of information using one or more secret parameters, for example, crypto variables, or associated key management."

What are the economic benefits from cryptography?

Cryptography provides key economic benefits by enabling secure and trustworthy digital transactions, reducing the risk of fraud and data breaches, and supporting compliance with data protection regulations. It lowers the cost of doing business online by safeguarding sensitive information and thereby facilitates digital trade. Cryptographic tools like digital signatures and secure hashing also ensure the authenticity and integrity of documents such as electronic invoices, certificates of origin, and customs declarations, enabling paperless trade and regulatory compliance. In addition, cryptography supports trust and legal certainty in cross-border digital interactions by enabling secure digital identities and e-signatures.

Various studies confirm potentially significant economic benefits from cryptography. For example, studies in 2001 and 2018 by the US National Institute for Standards and Technology showed a USD 250 billion economic benefit from industry adoption of its advance encryption standard.[29]

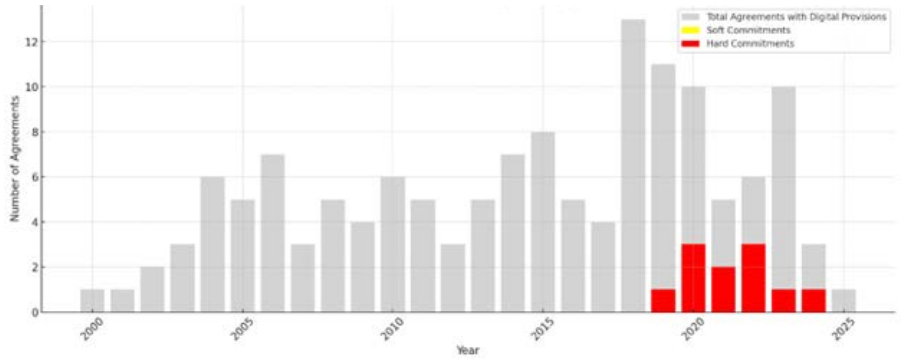
What are the main barriers to cryptography?

There are various technical, legal, and organizational challenges to adopting strong cryptographic tools. Cryptographic tools can be complex to implement correctly and require specialized knowledge. High costs and a lack of skilled personnel—especially for small and medium-sized enterprises—limits adoption. Many organizations also struggle with compliance and interoperability, as cryptographic standards and regulations vary across jurisdictions. Some governments impose restrictions on the use of strong encryption or demand lawful access mechanisms, raising concerns about privacy, trust, and data security.

29 NIST's Encryption Standard Has Minimum $250 Billion Economic Benefit, According to New Study | NIST accessed on 15 July 2025.

Cryptography in trade agreements

Commitments on Cryptography



Commitments on cryptography in trade agreements involving APEC economies have only emerged in recent years, with hard provisions first appearing in 2018. These commitments became more frequent between 2019 and 2023 but remain relatively limited overall. The absence of soft commitments suggests that when cryptography is addressed, it is typically through binding language, reflecting its sensitive and strategic nature.

First, these trade provisions on cryptography include key definition as to what is 'cryptography', 'encryption' and a 'key'. The main commitments so far are agreement not to require as a condition of imports, manufacture, sale or distribution of product, access to a particular technology, use of a particular cryptographic algorithm or partners with a person in that economy. These commitments are typically balanced with an exception for requirements to networks owned or controlled by a government and for measures taken pursuant to regulation related to financial institutions or markets.

Sample Cryptography Provision

This sample cryptography provision is taken from the **Australia-Singapore DEA.**

ARTICLE 7

Information and Communication Technology Products that Use Cryptography

1. For the purposes of this Article:

   (a) "cryptographic algorithm" or "cipher" means a mathematical procedure or formula for combining a key with plaintext to create a ciphertext;

   (b) "cryptography" means the principles, means or methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorised use; and is limited to the transformation of information using one or more secret parameters, for example, crypto variables, or associated key management

   (c) "encryption" means the conversion of data ("plaintext") into a form that cannot be easily understood without subsequent re-conversion ("ciphertext") through the use of a cryptographic algorithm; and

   (d) "key" means a parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot.

2. This Article shall apply to information and communication technology products

that use cryptography.[3]

3. With respect to a product that uses cryptography and is designed for commercial applications, neither Party shall impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of the product, as a condition of the manufacture, sale, distribution, import or use of the product, to:

(a) transfer or provide access to a particular technology, production process or other information, for example, a private key or other secret parameter, algorithm specification or other design detail, that is proprietary to the manufacturer or supplier and relates to the cryptography in the product, to the Party or a person in the Party's territory;

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

(c) use or integrate a particular cryptographic algorithm or cipher,

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

4. Paragraph 3 shall not apply to:

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

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

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

Policy Checklist: Cryptography

Question	Consideration
Should a provision on cryptography be included?	This is a threshold question. Provisions have appeared in at least 11 trade agreements since 2019 and are included in about one-third of recent agreements.
Should it include a commitment defining the key terms?	Typically the commitment includes a definition of what is cryptography, encryption and a key.
Should it include a commitment not to impose various conditions on use or transfer of cryptographic keys as a condition for sale or trade?	This is the key commitment and is typically binding. The conditions that the parties agree not to require are also usually aligned and listed in the above example provision from the Australia-Singapore DEA Article 7.3.
Should the provision be subject to a specific exception?	The commitment typically includes a specific exception as outlined in the above provision in the Australia-Singapore DEA Article 7.4.
How does this relate to previous commitments on Cryptography?	If your economy has previously committed to a position on customs duties on electronic transmissions, ensure that the provisions are consistent unless a change in policy is desired.

D.3: Review Clause

Some digital trade agreements [30] include a commitment to review whether to include a particular digital trade provision, within a specific period of time. For example, the 2019 EU-Japan Economic Partnership, the parties included, under the heading "Free flow of data" the following commitment:

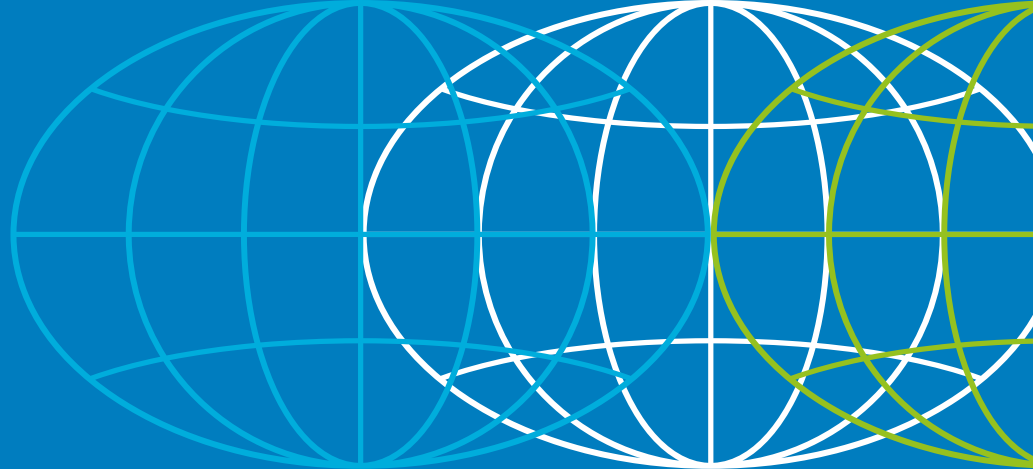
"The Parties shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data."

While Japan had already undertaken a commitment to the free flow of data in the CPTPP, the EU was then still working out to balance its interests in data free flow with its regulation of privacy under GDPR. In 2024 both economies finalized a protocol that amended the agreement to include provisions on the free flow of data.

A review clause could also be used to assess whether new commitments are needed on emerging technologies such as AI where new commitments may be needed, and in areas such as quantum computing that are yet to be subject to commitments in a trade agreement.

30 TAPED analysis shows, for APEC economies, these provisions are only included in the EU-Japan EPA, the EU-Mexico EPA, the EU-NZ EPA and, to a lesser extent, in the RCEP.

Section E:
General and Security Exceptions and Scope



Exceptions

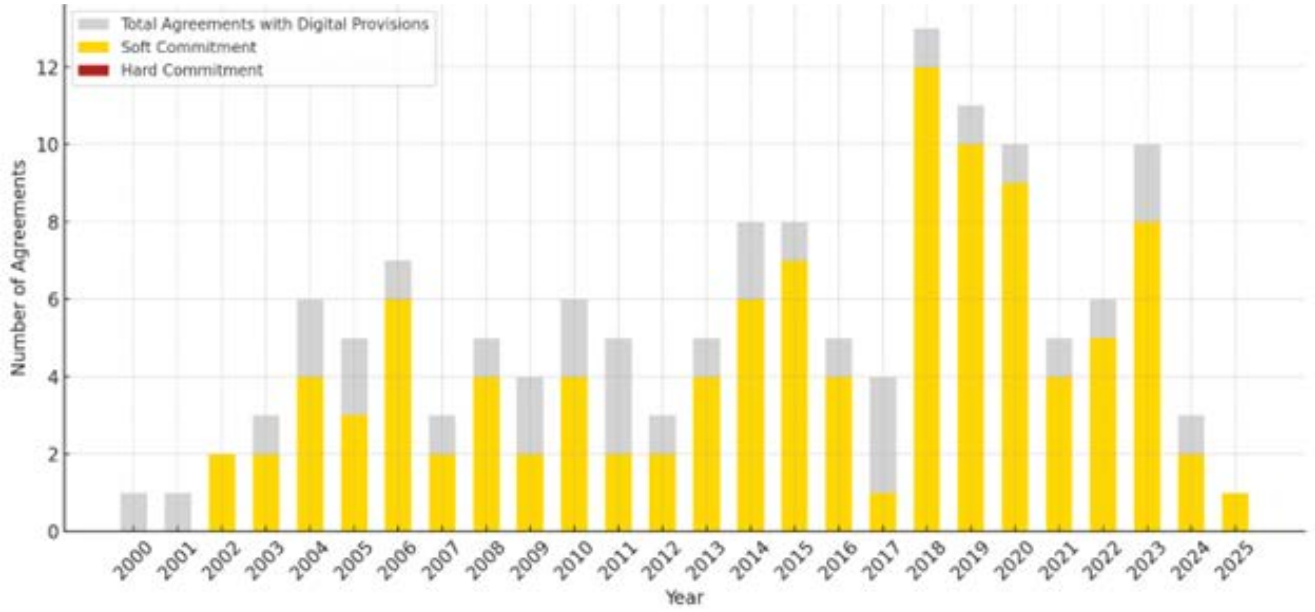
Exceptions provisions allow APEC member economies to introduce laws or regulations that may otherwise conflict with their digital trade commitments. These provisions play a crucial balancing role— they support digital trade while giving economies the flexibility to pursue other policy objectives. To fully understand the potential impact of any digital trade commitment, it is important to also consider how the exceptions provision might limit or reduce that impact by allowing departures from the commitment.

The two key exceptions in digital trade agreement (and trade agreement more broadly) relate to various public policies such as protecting human health, consumer protection or ensuring the privacy of personal data – referred to as **'general exceptions'.** The other types of exceptions provisions relate to national security policy – referred to as **'national security exceptions'.**

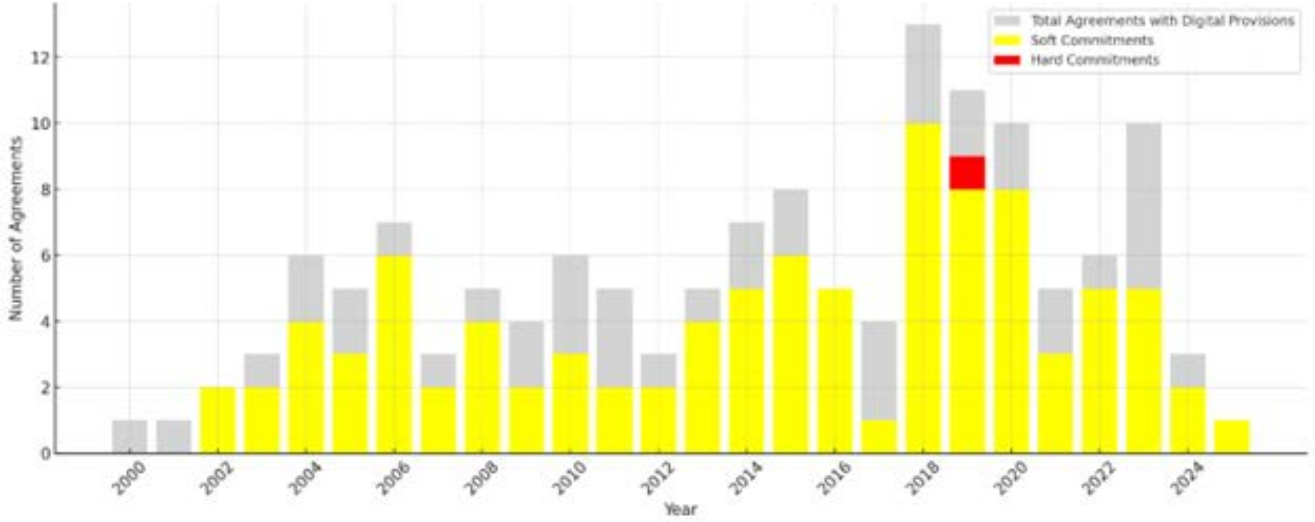
Most commonly, General & Security Exceptions apply to the whole agreement (including digital trade provisions). However, recent agreements have included **specific general and security exceptions within chapters or provisions on digital trade.** There are also other exceptions that can be relevant in a digital trade context such as prudential exceptions, Indigenous Peoples exceptions and tax exceptions.

As can be seen in the graphs below, General and Security Exceptions are very common in trade agreements, including trade agreements with digital trade provisions. Across APEC economies, both types of exceptions are almost always included – most often applying to the whole trade agreement, rather than the specific digital trade provisions only.

Security Exceptions in Digital Trade Agreements



Commitments on General Exceptions



Types of Exceptions provisions – General and National Security

There are two related ways that general exception provisions have been incorporated into digital trade agreements. The first is by incorporating a broad, legitimate public policy objective exception as part of the specific digital trade commitment to the free flow of information and to no data localisation. This has happened in agreements such as CPTPP, RCEP and DEPA.

The second way is by applying the general exception provision to the entire digital trade chapter or agreement. These provisions are modeled on or specifically incorporate the general exception provision in GATS Article XIV (and GATT Article XX).

There is also the exception for measures taken for national security purposes. These provisions are often based on the GATS and/or GATT national security exception, which are essentially the same. These exception provisions allow parties to adopt laws and regulations that are inconsistent with their digital trade commitments in order to achieve national security goals.

All digital trade agreements and FTAs with digital trade chapters include a general exception and national security exception.

Specific exceptions provision to the free flow of information

The following exception is found in CPTPP (and is the same in DEPA) in the commitment to free flow of information and to no data localisation.

CPTPP Article 14.11: Cross-Border Transfer of information by Electronic Means

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.

This exception provision is modeled on the chapeau (introductory paragraph) of GATT Article XX and GATS Article XIV, but with some important differences. Most notably, it refers to a "legitimate public policy objective" rather than listing specific policy exceptions, as GATT and GATS do.[31] What qualifies as a legitimate public policy would need to be interpreted in light of WTO jurisprudence and the broader context of the trade agreement in which the provision appears.

For example, the preamble to the CPTPP refers to goals such as promoting corporate social responsibility, cultural identity and diversity, environmental protection, gender equality, Indigenous rights, labour rights, inclusive trade, sustainable development, traditional knowledge, and the right to regulate in the public interest. These references suggest that measures aimed at advancing any of these objectives could be considered legitimate public policies under the exception provision.

The CPTPP exception also mirrors key elements of the GATT/GATS chapeau. Specifically, Article 14.11.3(a) reflects WTO Appellate Body findings that a measure is considered arbitrary or unjustifiable if it lacks a rational connection to the stated policy objective. Article 14.11.3(b)

31 It is important to note that GATS Article XIV includes a non-exhaustive listing of measures, in particular, under sub-paragraph (c).

further requires that any restriction on the transfer of information must not be "greater than are required" to achieve the objective. No trade panel has yet specifically addressed the scope of this standard. Whether a measure is greater than is required may be similar to the GATS necessity test or could allow for more flexibility. Whether a measure is "necessary" has been interpreted to mean that no less trade-restrictive alternative is available.

Another approach to specific exceptions to the commitment to free flow of information is found in RCEP and is as follows:

RCEP Article 12.15 Cross-border Transfer of Information by Electronic Means

3. Nothing in this Article shall prevent a Party from adopting or maintaining:

(a) any measure inconsistent with paragraph 2 that it considers necessary to achieve a legitimate public policy objective,14 provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or

Footnote 14: For the purposes of this subparagraph, the Parties affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party.

This exception provision shares important similarities with the embedded exception clauses in the CPTPP and DEPA but also contains notable differences. Like those agreements, it allows for exceptions based on a "legitimate public policy objective." However, this provision goes further by stating that it applies to any measure that a Party "considers necessary" to achieve such an objective.

Footnote 14 clarifies that "the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party." This differs significantly from the WTO context, where a measure is considered "necessary" only if no less trade-restrictive alternative is reasonably available. In contrast, under this provision, each RCEP Party has the discretion to determine for itself whether a measure is necessary.

As a result, regulators under RCEP have greater flexibility to justify measures that might otherwise be inconsistent with commitments on the free flow of information. This level of discretion exceeds that available under CPTPP and DEPA, where justifying such measures requires meeting stricter necessity tests.

Security Exception in USMCA, CPTPP and others

There are broadly two different approaches to the security exception found in FTAs and digital trade agreements. Both models draw on language from the WTO national security exception but include important differences. One of these models is found in agreements such as CPTPP and USMCA and is as follows:

CPTPP Article 29.2

Nothing in this Agreement shall be construed to:

(a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or

(b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.

Focusing on subparagraph (b), a first point of difference with the security exception found in the GATS and GATT, is that the exception has two components, namely obligations with respect to maintenance or restoration of international peace or security, which mirrors subparagraph GATT Article XXI b(iii), and would seem to cover action such as those taken pursuant to a UN security council resolution. The other element in subparagraph (b) applies to measures to protect "its essential security interests". Here, a WTO Panel has found that it is up to each WTO Member to determine what are its essential security interests. [32] The right to take measures that "it considers necessary" is the same in the WTO provisions and would require that these measures are exercised consistent with the international legal rule of good faith.

Another approach to national security found in trade agreements is found in RCEP. Here there are two security exception provisions at play. The first exception is specific to the commitment to the free flow of information. It reads as follows.

RCEP Article 12.15 Cross-border Transfer of Information by Electronic Means

3. Nothing in this Article shall prevent a Party from adopting or maintaining:

(b) any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties.

This exception coupled with the language that these measures are not to be disputed by other parties has the effect of giving each RCEP Party unfettered discretion to decide when to rely on this exception to justify a measure that otherwise is inconsistent with the commitment to the free flow of information.

In addition, RCEP includes the following exception provision that applies to the entire e-commerce chapter (and RCEP agreement). This provision specifies that the goal of protecting critical public infrastructure falls under essential security interests. Otherwise, the provisions are very similar to the GATT Article XXI national security provision.

32 WTO Panel Report, Russia-Measures Concerning Traffic in Transit, DS512, 26 April 2019, para 7.131

RCEP Article 17.13 Security Exception

Nothing in this Agreement shall be construed:

(a) to require any Party to furnish any information the disclosure of which it considers contrary to its essential security interests;

(b) to prevent any Party from taking any action which it considers necessary for the protection of its essential security interests:

i. relating to fissionable and fissionable materials or the materials from which they are derived;

ii. relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials, or relating to the supply of services, as carried on directly or indirectly for the purpose of supplying or provisioning a military establishment;

iii. taken so as to protect critical public infrastructures including communications, power, and water infrastructures;

iv. taken in time of national emergency or war or other emergency in international relations; or

(c) to prevent any Party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.

Scope Limitations

Digital trade chapters in FTAs and DEAs may sometimes include defined scope limitations. One common exclusion relates to government procurement and data held or processed by or on behalf of a government. These exclusions reflect longstanding sensitivities around national security, regulatory autonomy, and public-sector data management.

Scope can also be indirectly limited by cross-referencing reservations or non-conforming measures listed in other chapters of the agreement — particularly those covering investment, cross-border services, and financial services. In such cases, commitments made in the digital trade chapter do not override existing reservations taken elsewhere in the agreement.

For example, in the **CPTPP**, certain digital trade obligations—such as non-discrimination, cross-border data transfers, and prohibitions on data localisation—do not apply to the non-conforming aspects of measures listed in the investment, services, and financial services chapters. Similarly, the **RCEP** agreement excludes commitments on data localisation and cross-border data flows where reservations have been taken under the investment and trade in services chapters.

These scope limitations are an important tool to preserve regulatory flexibility while still advancing key digital trade disciplines. When drafting digital trade provisions, negotiators should ensure alignment with other provisions in the agreement and carefully consider how horizontal reservations (for example, reservations in the services chapter) may affect digital commitments.

Policy Checklist: General & Security Exceptions

Question	Consideration
Should a General and/or Security Exception be included?	General Exceptions are almost universal in trade agreements which include digital trade provisions. Security Exceptions are also present in the vast majority of agreements.
Should it include specific general exception provisions to the data flows and data localisation commitments?	Whether to develop a specific general exception for commitments to cross border information flows and to no data localisation, such as in CPTPP, DEEPA and RCEP. The alternative is to rely on a general exception provision that applies to the entire set of digital trade commitments, as happens in USMCA.
Should the exception provision be modeled on CPTPP or RCEP?	A specific exception provision modeled on the provisions in CPTPP, compared to GATS Article XIV, provides more flexibility for regulators to adopt measures otherwise inconsistent with the data flow and no data localisation commitment. The specific exception in RCEP gives regulators even more flexibility than in CPTPP or DEEPA.
Should it include a specific national security exception for the commitments on data flows and data localisation?	RCEP includes a specific national security exception that effectively leaves it up to each Party to decide whether a measure is for national security purposes, with no ability for the Parties to challenge this categorization or use of the exception.
Should the scope of digital trade provisions be limited in any way?	Are there any intended limitations to the scope of digital trade commitments, such as data collected by Government agencies, or policy space reserved in other parts of the agreement (such as in services commitments)? If so, these should be identified explicitly in the digital trade provisions to ensure the intended outcome.

Are there other exceptions required on the basis of the rules included in scope?	Digital trade agreements can include a range of different exceptions based on economies domestic context and the rules including a digital chapter or agreement, for example prudential, tax and Indigenous Peoples exceptions.