Asia Business Trade Association

Issue Paper

Issue 01-19 June 2019

FTA Digital Trade Regulations Comparison

This Issue Paper tracks and highlights digital trade provisions in seven different FTAs on 16 dimensions of importance

Digital tools and e-commerce have rapidly altered trade patterns. The proliferation of the digital economy has extended the capacities of firms of all sizes enabling them to engage in cross-border trade in ways that continue to rapidly evolve.

The size of the digital economy continues to grow exponentially, making it increasingly important for policymakers to think through sensible frameworks to provide the best enabling environment for consumers and companies to thrive for the future.

Digital trade is intertwined with often domestically sensitive issues such as cross-border data flows, data collection and storage, cybersecurity and privacy.

Parties signing free trade agreements (FTAs) have begun adding new rules to regulate and harmonize provisions of importance to companies trying to operate across multiple jurisdictions. This paper highlights the similarities and differences between this set of cutting-edge agreements in some of the keys areas of interest to digital trade.

Examining FTAs

Table 1 identifies sixteen key digital provisions across seven FTAs.

All seven FTAs, described more fully below, have only two provisions in common. All contain provisions to include the elimination of customs duties on digital products or electronic transactions, and cooperation elements.

The remaining 14 elements, however, show variation across the FTAs under examination.

The United States/Canada/Mexico (USMCA) and Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), show the most advanced provisions under review in this paper.

Both agreements, as an example, include safeguards to protect developers' rights over their software source code against the demands of disclosure. In addition, the USMCA incorporates source code-related algorithms into the subject of protection, which makes this FTA distinct from previous agreements. This amendment should facilitate implementation by providing greater clarification on source code.

When it comes to financial services, all seven FTAs allow carve-outs for prudential reasons. Only Australia/Hong Kong (A-HKFTA) guarantees cross-border transfer of information by electronic means and prohibits data localisation for financial services.

The Seven FTAs

The analysis in Table 1 includes seven FTAs that all have digital trade provisions included across the agreement:

- The United States-Mexico-Canada Agreement (USMCA)
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)
- Australia-Hong Kong FTA (A-HKFTA)
- Sri Lanka-Singapore FTA (SLSFTA)
- Korea-United States FTA (KORUS FTA)
- EU-Japan Economic Partnership Agreement (EUJEPA)
- EU-Singapore FTA (EUSFTA)

Understanding Table 1

This Issue Paper analyses whether or not these agreements have a separate article on each of the sixteen provisions throughout the agreement. It focused largely on the chapters on the digital trade (or electronic commerce) and financial services.

The criteria for labelling were the following:

YES - means the provision is included in a separate article and the definition of the provision is fully covered;

PARTIAL - means the provision is included in a separate article, but the definition of the provision is not fully addressed;

NO - means the provision is not included in a separate article and there is no specific mention of the provision throughout the agreement.

16 Key Elements and Definitions Covered

1. ***Elimination of customs duties on digital products and/or electronic transmissions***

   The parties are prohibited from imposing customs duties, fees or other charges on cross-border electronic transmission of digital products. (However, parties are not precluded from imposing internal taxes.) The elimination of customs barriers for digital products and electronic transmissions is a key measure to facilitate digital trade between the FTA members. It reduces the costs incurred by customers and helps businesses to access new markets.

2. ***Non-discrimination against digital products***

   Non-discriminatory treatment of imported digital products is another fundamental measure to support open digital economy between the FTA members. Equal treatment of digital products ensures healthy market competition and provides better quality and more affordable choices for consumers.

3. ***Electronic authentication and electronic signatures***

   The provision refers to a mutual recognition of electronic process of identity verification and validity of electronic signatures. Unless they do not meet certain performance standards or are not certified by an accredited authority, the FTA parties should not prohibit electronic authentication methods or deny the legal validity of the e-signatures. This provides flexibility for users of authentication technologies and e-signatures, facilitates trade processes and eases the efficiency of transactions.

4. ***Paperless trading***

   The FTA parties should ensure there is a transparent platform that provides access to all measures related to electronic commerce and make trade administration documents available to the public in electronic form. Unless there is a legal requirement for the printed version, each party should accept trade administration documents submitted electronically as the legal equivalents. This increases the effectiveness of trade administration documents' processing.

5. ***Domestic electronic transactions framework***

   Domestic electronic transactions framework refers to the domestic legal frameworks governing electronic transactions adopted by FTA members. These frameworks should be consistent with the principles of the UNCITRAL Model Law on Electronic Commerce adopted in 1996. Individual parties are encouraged to avoid unnecessary regulatory burdens on electronic transactions and facilitate the participation of interested stakeholders in the development of the domestic legal framework. The framework facilitates enforcement of the FTA rules governing electronic transactions between the FTA parties and provides clear regulations for conducting cross-border business in those countries.

6. Online consumer protection

The parties should provide the same protection measures against fraudulent or deceptive commercial activities for online consumers as they do for any other consumers. The measures should be transparent and effective to protect consumers and proscribe activities that can cause harm or potential harm to consumers engaged in online commercial activities. This provision is important for enhancing consumer welfare and establishing firm consumer trust in digital trade.

7. Personal information protection

Parties should proactively protect personal information by designing a legal privacy framework to prevent a misuse of individual information of consumers engaged in electronic commerce. The framework should not discriminate against any users of digital trade, and the FTA parties should be responsible for ensuring compliance with these measures within their territories. Compliance guidelines and information on how a person can pursue a remedy in case of privacy breach should be publicly available.

Although personal information protection prevents damage of trust in the underlying digital economy and has its own social and economic benefits, there are risks that online privacy policies may create barriers to the digital trade. Consumer data is essential for businesses to facilitate transactions, analyse marketing information, detect patterns and develop competitive innovation. Therefore, the parties have to balance between two policy objectives: protect the privacy and security of the digital trade users and facilitate free flow of data for better commerce and communication.

There are examples of privacy guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Trans-border Flows of Personal Data, which could be considered as valid mechanisms to protect individual privacy in the least-restrictive way possible.

8. Measures against unsolicited commercial electronic communications

Colloquially known as 'spam messages,' unsolicited commercial electronic communications are messages sent in-bulk to recipients in forms such as advertisements, product updates, or trade offers from various sources. Acknowledging the detrimental effect these communications may have on the digital consumer experience, certain FTAs have taken steps to regulate unsolicited commercial electronic communications. Such measures include obtaining a personal consent of the consumers to receive such messages, their right to opt out from receiving unwanted messages, and appropriate recourse if suppliers do not respect such regulations.

9. Cybersecurity

As cyber-attacks pose a significant risk to participants of the digital trade, the FTA members should build the capacities of their respective national agencies responsible for ensuring cybersecurity, responding to cyber threats, mitigating the effects of any malicious intrusions, recovering from them and spreading general awareness of cyber-attacks. Risk-based approaches and preventive practices are usually encouraged as more effective ways rather than prescriptive regulation in addressing cyber threats.

10. Cross-border transfer of information

Free movement of data and transfer of information by electronic means across borders are essential for building effective and sustainable international digital trade. Decisions related to business development, marketing, innovation and development of comparative advantage cannot be made without cross-border data flows.

Data flow-restrictive measures should only be imposed as regulations necessary to protect consumer privacy and security, and never as digital trade restrictive and protectionist measures. Facilitation of cross-border transfer of information for business purposes should be a common goal for countries facing the digital age as it decreases the costs of doing cross-border trade, increases productivity, helps to meet consumer demands and enhance innovation.

11. Prohibition of data localisation

Data localisation refers to the digital trade regulation imposed by a country, which requires a covered person to use or locate computing facilities in the country's territory as a condition for conducting business there. Data localisation measures target both personal and non-personal types of data such as company and tax records. Prohibitions of data localisation allow businesses to be free from storing and replicating data locally. The provision may become of particular interest to multinational businesses, as it allows outsourcing of data, reduces costs of doing business internationally and promotes an open and flexible global technical infrastructure.

12. Cross-border transfer of information by electronic means and prohibition of data localisation for financial services

The provision allows cross-border transfer of information by electronic means (including personal information) and prohibits data localisation for financial services when these activities are in connection with the conduct of the business of a covered *financial* person.

13. Liability of intermediary service providers

Intermediary service providers are suppliers of interactive computer services. The provision refers to a liability distinction between intermediary service providers and their service users, i.e. the information content providers. It prevents the intermediary service providers from being held legally accountable for harms related to information stored, processed, transmitted, distributed, or made available by their service users. The provision also allows intermediary service providers to moderate online content by restricting harmful or objectionable material. The provision does not apply to intellectual property protection measures.

14. Non-disclosure of software source code and related algorithms

A source code of software or an algorithm expressed in the source code often contain trade secrets and information that grant a competitive advantage to the owning party. If the owners are required to disclose the source code of their software or related algorithms as a condition for trade, they risk losing the exclusive right over their technologies. Provisions that ban any party from requiring access to the source code or related algorithms ensure a more secure trade environment.

15. Open government data

Open government data is a digital provision that makes government information, including data, readily available for public consumption. Though no more than a recommendation (i.e. non-binding), this provision emphasises the positive impact that electronically-available non-sensitive public data can have on innovation, competitiveness, and economic development.

16. Cooperation

Cooperation refers to parties' commitments to collaborate on various regulatory measures, their implementation steps, and further enforcement. These cooperation practices include exchanging information and sharing experiences on regulations, personal information protection, security in electronic communication, spam prevention, establishment of safeguards etc. The provision encourages the parties to commit to building a more inclusive and safer world for the digital trade, assisting SMEs to overcome obstacles to the use of FTAs, and engaging the private sector in the development of self-regulation tools.

Table 1: Digital Trade Provisions across FTAs

NO.	Digital Trade Provisions	USMCA	CPTPP	A-HKFTA	SLSFTA	KORUS FTA	EUJEPA	EUSFTA
1	Elimination of customs duties on digital products and/or electronic transmissions	YES	YES	YES	YES	YES	YES	YES
2	Non-discrimination against digital products	YES	YES	NO	YES	YES	NO	NO
3	Electronic authentication and electronic signatures	YES	YES	YES	YES	YES	YES	PARTIAL
4	Paperless trading	YES	YES	YES	YES	YES	NO	PARTIAL
5	Domestic electronic transactions framework	YES	YES	YES	YES	YES	PARTIAL	NO
6	Online consumer protection	YES	YES	YES	YES	YES	YES	NO
7	Personal information protection	YES	YES	YES	YES	NO	NO	NO
8	Measures against unsolicited commercial electronic communications	YES	YES	YES	NO	NO	YES	NO
9	Cybersecurity	YES	YES	NO	NO	NO	NO	NO
10	Cross-border transfer of information	YES	YES	YES	YES	PARTIAL	YES	YES
11	Prohibition of data localisation	YES	YES	YES	YES	NO	NO	NO
12	Cross-border transfer of information by electronic means and prohibition of data localisation for financial services	NO	NO	YES	NO	PARTIAL	NO	NO
13	Liability of intermediary service providers	YES	NO	NO	NO	NO	NO	PARTIAL
14	Non-disclosure of software source code and related algorithms	YES	PARTIAL	PARTIAL	NO	NO	PARTIAL	NO
15	Open government data	YES	NO	NO	NO	NO	NO	NO
16	Cooperation	YES	YES	YES	YES	YES	YES	YES