August 1, 2024

BSA AND GDA COMMENTS ON GENERAL REVIEW OF COMPREHENSIVE AND PROGRESSIVE AGREEMENT FOR TRANS-PACIFIC PARTNERSHIP

We at BSA | The Software Alliance[1] (**BSA**) and the Global Data Alliance (**GDA**)[2] welcome the opportunity to provide inputs to the General Review of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (**General Review** and **CPTPP** respectively).

BSA and GDA are strong supporters of the CPTPP and its robust digital trade rules, which include obligations on non-discriminatory treatment of digital products, cross-border data transfers, and electronic authentication of contracts, as well as prohibitions on data localization requirements, on source code disclosure requirements, and on customs duties on electronic transmissions. We applaud the CPTPP Parties' efforts to ensure that the Agreement continues to set the benchmark for rules on cross-border digital trade.

Per the Terms of Reference for Conducting the General Review (**Terms of Reference**),[3] we note that the General Review will consider how to enhance the CPTPP, which include, *inter alia*, identifying areas of mutual interest, updating existing obligations, developing new provisions and Chapters, as well as ensuring effective implementation and operation of the agreement.

Our submission covers the following key matters, with a specific focus on Chapter 14 (Electronic Commerce) of the CPTPP.

1. Accession to the CPTPP.
2. Elements of the Accession Process.
3. Upgrading the Electronic Commerce Chapter.
4. Implementing the Electronic Commerce Chapter.

Accession to CPTPP

The accession process remains a keystone for the CPTPP's future success. Since its entry into force in December 2018, the CPTPP has garnered significant international interest and attracted many applicants for accession. On July 2023, the United Kingdom (UK) became the first economy to accede to the CPTPP. Other formal applicants for accession include China, Costa Rica, Ecuador, Taiwan, Uruguay and Ukraine.[4]

---

[1] BSA | The Software Alliance is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

[2] The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. GDA member companies are active in a broad array of sectors, including aerospace, agriculture, automotive, energy, electronics, finance, health, logistics, and telecommunications, among others.

[3] Terms of Reference for Conducting the General Review of the CPTPP, November 2023, https://www.dfat.gov.au/sites/default/files/cptpp-general-review-terms-reference-november-2023.pdf.

[4] Impact Assessment of the UK's Accession to the CPTPP, June 2023, https://www.gov.uk/government/publications/cptpp-impact-assessment/impact-assessment-of-the-uks-accession-to-the-cptpp-executive-summary-web-version#fnref:15.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

Per the CPTPP Accession Process,[5] aspirant economies must "demonstrate the means by which they will comply with all of the existing rules contained in the CPTPP". This is critical for the following reasons:

- **Upholds key rules for international trade:** If the CPTPP can ensure predictable compliance by all Parties, it will reinforce the importance of adhering to international trade rules and promote the rules-based trading system. Conversely, if there is a perception that the CPTPP's terms are not strictly followed, it would undermine the CPTPP's reputation as the gold standard for trade agreements and reduce confidence in the rules-based trading system.
- **Benefits its existing Parties:** Only if all Parties meet the CPTPP's standards will it produce benefits for the citizens of the current and future Parties.
- **Is legally operative:** The accession review process is the primary point of leverage to ensure that future Parties fully meet and implement the CPTPP's obligations. While the CPTPP provides a dispute settlement mechanism, this is typically a measure of last resort.

In short, to serve a positive role within the international economic legal system, the CPTPP must be a "living" agreement with force and effect. This requires rigorous and exacting accession review procedures; vigilance against breaches of the agreement; and where necessary, a willingness to invoke dispute resolution procedures to defend the agreement's legal standards. If the CPTPP becomes a mere paper agreement whose norms can be disregarded with impunity, it will harm not only the CPTPP and its Parties, but also the broader *corpus* of international economic law.

Elements of the Accession Process

The long list of aspirant economies to the CPTPP reflects the Agreement's attractiveness and its potential to bring broad-based benefits to current and future Parties. At the same time, the large number of applicants may lead to complications during upcoming accessions. Fortunately, CPTPP Parties have an opportunity – building on their experience with the United Kingdom's accession – to iterate and refine the accession procedure so that it becomes more robust and rigorous. In this regard, we offer the following observations for the existing CPTPP Parties as they evaluate current applications to accede to the Agreement:

- **Burden of Proof:** Candidates bear the burden of demonstrating that all of their legal measures and practices comply with the CPTPP.
- **General Standard of Review:** All candidates' accession requests should be evaluated according to the same standard of review. Reviews should be performed on a neutral, impartial, and equal basis. All candidates should be expected to meet the same standards as each other to ensure that the CPTPP continues to function smoothly and effectively. This is also important to ensure that the benefits accruing to a Party are not improperly nullified or impaired due to improper differentiation in applicable legal standards.
- **Substantive Legal Standard of Review:** The accession review process should include a comprehensive analysis of all relevant measures, in all sectors and all legal disciplines, that impact cross-border data or the location of computing facilities. CPTPP Articles 14.11 and 14.13 require assessments as to whether *inter alia* any transfer restrictions or localization mandates: (1) are adopted or maintained to achieve a legitimate public policy objective; (2) are applied as a means of arbitrary or unjustifiable discrimination, or a disguised restriction

[5] Accession Process for the CPTPP (Annex to CPTPP/COM/2019/D002), https://www.mfat.govt.nz/assets/Trade-agreements/CPTPP/Accession-Process.pdf.

on trade; and (3) impose transfer restrictions on localization requirements greater than required to achieve the objective.[6]

- **Duration of Review:** The CPTPP Accession Process guidance document makes clear that accession reviews may require a significant time to reach completion. Article 4.3 of the Accession Process document indicates that a favorable accession decision is predicated upon "changes … to domestic laws and regulations." This regulatory reform process may take years, if – for example – there is:
    - A substantial compliance gap between CPTPP obligations and the legal standards reflected in the candidate's domestic laws and regulations; and/or
    - A substantial number of domestic laws and regulations that would need to be amended to bring the candidate into compliance with CPTPP obligations. In prior negotiations, candidates have needed to rescind or amend dozens (or more) laws, regulations, and other legal measures.

  For reference, in the context of WTO accession, the PRC's accession review process took over 15 years, while Russia's accession review process took almost 20 years.

- **Iterative Review Process:** Candidates and the Accession Working Group should engage in an iterative process to ensure that the candidate clearly identifies all measures relevant to the review. Understandably, this process may be more time-consuming in cases involving a lack of transparency or in cases in which not all relevant measures have been notified to the WTO. The Working Group should insist on sufficient information to allow it to identify, analyze, discuss, and assess which measures fall short of CPTPP standards, and how those measures should be modified to ensure compliance. Given the complexity of such discussions, it is not uncommon for accession review processes to involve negotiating rounds spanning years.

- **Treatment of Legal Conflicts:** It is critical that – prior to any accession decision – any candidate resolve any *prima facie* inconsistency between its domestic legal framework and the agreement's obligations by effectuating changes to its domestic laws. For example, whereas CPTPP Article 14.11 allows Parties to restrict cross-border data transfers provided that (among other things) any restrictions are "no greater than required" to achieve a legitimate public policy purpose, one of the CPTPP candidates has adopted dozens of restrictions on cross-border data transfers on many data types (including data that is often publicly available) across many economic sectors. That candidate economy's cross-border data rules appear to stand in direct legal conflict with CPTPP norms, meaning that its domestic rules and the CPTPP norms are mutually incompatible, such that it would be impossible to comply with one without breaching the other. For example, as stated by that candidate's cyberspace regulators on June 18, data transfers are only permitted if the regulator – in its discretion – considers the transfers to be "legitimate" and "necessary."[7]

---

[6] For example, a "disguised restriction on trade" may exist if there is evidence that hundreds of traders have been unable to secure required security assessment approvals to transfer out of a jurisdiction commercial data needed for the conduct of their business. Likewise, the breadth and number of data transfer restrictions or localization requirements – or the existence of prohibitions on transferring broad, undefined types of data (e.g., an indeterminate and vague class of "important data") – may raise concerns as to whether the restrictions are "greater than required" to achieve a legitimate public policy objective. A similar observation exists in a situation in which an authority indicates that tacit approval for cross-border data transfers can be revoked without notice or due process based on a unilateral future determination that the data at issues are "important." The unequal or disproportionate impact of such measures on non-national enterprises may indicate the presence of "arbitrary or unjustifiable discrimination."

[7] *Chinese official outlines criteria to determine 'legitimacy and necessity' of outbound data transfers*, June 2024, https://mlexmarketinsight.com/news/insight/chinese-official-outlines-criteria-to-determine-legitimacy-necessity-of-outbound-data-transfers. The article describes the Policy Briefing on the Management of Cross-Border Data Transfers, hosted by CNCERT/CC and China Electronics Standardization Institute, Beijing, June 18 2024)).

Under CPTPP Article 14.11, restrictions on data transfers are only permitted if those restrictions are "required" to achieve a "legitimate" objective. In this case, the candidate's law turns the CPTPP obligations on their head – subverting their meaning and intent and giving rise to a legal conflict that can only be resolved through a change in that the candidate's law.

- **No Strict Sequencing of Candidates:** Candidates are to be approved when they finally meet the terms agreed with the Parties (CPTPP Article 30.4.1) and ultimately demonstrate their compliance "with all of the existing rules contained in the CPTPP." (CPTPP Accession Process, Article 5.1). Accession should be approved only when a candidate meets all relevant requirements of the CPTPP. As such, later-in-time candidates may accede more rapidly than earlier-in-time candidates. Where – as noted above – a candidate may need to amend a large number of statutory measures as well as subsidiary regulations, the accession process could take many years.
- **Implied Duty of Good Faith and Fair Dealing During Negotiations:** Candidates should meet standards of good faith, reflecting the *bona fides* of their intention to meet the terms of the treaty.
    - In the context of international treaty negotiations, the implied duty of good faith and fair dealing means that during the pendency of its accession review, a candidate should not undertake actions that would fundamentally frustrate or complicate compliance with, or fulfillment of, the terms of the international agreement.[8]
    - For example, during the period of accession review, candidates should not otherwise make binding legal commitments, or enact binding domestic rules, that would be incompatible with the obligations of the international agreement to which the candidate is seeking to accede. For example, since its formal application for accessions, one of the candidate economies adopted numerous new cross-border data restrictions and data localization mandates that appear to be in conflict with CPTPP Articles 14.11 and 14.13. This course of conduct raises questions and concerns.
- **Collateral Effects on Other International Agreements:** CPTPP Parties should consider the potential impacts of a CPTPP accession decision on the accession dynamics or legal interpretative issues in other agreements. First, given that the CPTPP contains many provisions also found in the Digital Economy Partnership Agreement (**DEPA**), a determination of a candidate's ability to comply with CPTPP provisions will have implications on subsequent DEPA accession processes as well. Second, and more generally, similar language is found in numerous other free trade agreements and digital economy agreements around the world (as well as the forthcoming WTO Joint Statement Initiative Agreement on E-Commerce), indicating that decisions made by the CPTPP may have even broader legal interpretative significance.
- **Sensitivity to Future Compliance and Implementation Challenges:** It is recommended that the CPTPP Parties pay close attention to any evidence that an obligation may prove politically difficult for a candidate to implement - especially in instances where the candidate's domestic political system or circumstances would make it politically costly or sensitive to fully and faithfully implement the obligation.

---

[8] See e.g., Hans Wehberg, *Pacta Sunt Servanda,* 53 American J. Int'l L. 775-786 (1959), https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/pacta-sunt-servanda/E8967A236B1141934DD8D1495FEA2BFA; Josef L. Kunz, *The Meaning and the Range of the Norm Pacta Sunt Servanda* (1945), 39 American J. Int'l La. 180-197 (1945), https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/meaning-and-the-range-of-the-norm-pacta-sunt-servanda/87674E485CBE023C0A16B6B429FA2361; Ejan MacKaay, Good Faith in Civil Law Systems – A Legal-Economic Analysis, published in: Vrank en vrij - Liber amicorum Boudewijn Bouckaert, Jef De Mot (ed.), (2011), https://ssrn.com/abstract=1998924 or http://dx.doi.org/10.2139/ssrn.1998924.

- **Granting Transition Periods or Other Allowances May Have Unintended Consequences:** It is also recommended that the CPTPP Parties approach with caution any suggestions to adopt transition periods for implementation of specific obligations. Vietnam's transition period under CPTPP Articles 14.11 and 14.13 offers a cautionary tale: Since the conclusion of the CPTPP negotiations, Vietnam has implemented numerous rules that appear to contradict these two obligations. This is an unfortunate development, given that the transition period was intended as a period during which Vietnam was to make efforts to bring itself into compliance.

Upgrading the Electronic Commerce Chapter

We recommend that the CPTPP Parties assess and upgrade the Electronic Commerce Chapter to reflect the new realities of trade today. Many economies in the Asia Pacific region, including some CPTPP Parties, have implemented domestic regulations to address issues related to cloud computing, AI and cybersecurity in ways that may impede digital trade. However, these technologies and issues are not referenced in the Electronic Commerce Chapter. In addition, various CPTPP Parties have also entered into Digital Economy Agreements[9] with each other, which cover a significant broader scope of issues than the Electronic Commerce Chapter.

The General Review presents an opportunity to not simply update the Electronic Commerce Chapter, but to incorporate best-in-class digital trade provisions. This will ensure the CPTPP's continued relevance and cement its reputation as the gold standard for trade agreements.

In **Annex I** to this submission, we provide model digital trade provisions for the CPTPP Parties' consideration. These include updated versions of existing provisions in the Electronic Commerce Chapter, as well as brand new provisions covering issues such as AI, cybersecurity, personal information protection and online consumer protection in greater depth.

Implementing the Electronic Commerce Chapter

E-commerce in Asia Pacific has experienced substantial growth, driven by increased internet penetration, mobile device usage and adoption of online sales channels by businesses in region. Implementation of the CPTPP's Electronic Commerce Chapter is critical to the region's economic prospects as businesses seek to internationalize their supply chains and service other markets beyond their own.[10]

There is substantial variance in implementation across the CPTPP Parties. For example, while countries such as Australia, Canada and Singapore have high levels of implementation, the likes of Brunei[11] and Vietnam lag behind. Vietnam, as previously mentioned, appears to have used the transition period under CPTPP Articles 14.11 and 14.14 to lock in domestic legal changes that are incompatible with said obligations. For example, Vietnam's Law on Cybersecurity (No. 24/2018/QH14), promulgated in 2018, contains data localization requirements for both domestic and foreign firms. The subsequent Decree No.53/2022/ND-CP, announced in 2022, implements several articles of the Cybersecurity Law with data localization requirements. In addition, Vietnam's new Personal Data Protection Decree allows cross-border transfers but requires a process for transfers to be effected. We have consistently flagged these compliance issues with Vietnamese authorities in

[9] Most notably, the DEPA between Chile, New Zealand and Singapore, the Singapore-Australia Digital Economy Agreement, the UK-Singapore Digital Economy Agreement. The Australia-UK Free Trade Agreement also contains a robust and comprehensive Digital Trade Chapter and a first-of-its-kind Innovation Chapter.

[10] Enforcement of the CPTPP is rated as the top priority for firms in the CPTPP regarding the CPTPP's future. See: The Implementation of the CPTPP's E-Commerce Chapter in 2023 and toward CPTPP 2.0, February 2024, p. 12-14, https://www.csis.org/analysis/implementation-cptpps-e-commerce-chapter-2023-and-toward-cptpp-20

[11] Brunei is still in the process of enacting its Personal Data Protection Order, which will impose obligations on organizations when collecting, using or processing personal information. Brunei also does not appear to have laws against unsolicited commercial electronic messages.

May 2024, June 2023,[12] December 2022,[13] December 2021,[14] November 2021,[15] September 2021,[16] and April 2021,[17] but they remain unaddressed.

Vietnam's transition period has since expired. Given prevailing industry concerns, we urge CPTPP Parties to work with Vietnam to improve its implementation of the CPTPP and to bring its domestic regulations into compliance with its obligations in the agreement.

Conclusion

We thank the CPTPP Parties for your consideration and review of this submission and look forward to any questions that you may have. Please direct any questions to gdainfo@bsa.org.

Sincerely,

Tham Shen Hong
Senior Manager, Policy – APAC

[12] GDA Comments on the Cross-Border Data Transfer Elements of the Personal Data Protection Decree, June 2023, https://globaldataalliance.org/wp-content/uploads/2023/07/en0630202gdapdpd.pdf.

[13] GDA Comments on Draft Law on Telecommunications, December 2022, https://globaldataalliance.org/wp-content/uploads/2022/12/en12232022gdavtdfttelecom.pdf.

[14] GDA Comments on Proposed Amendments to Draft Decree 72, December 2021, https://globaldataalliance.org/wp-content/uploads/2022/01/en123021gdacmtsdrfde72.pdf.

[15] GDA Comments On Proposed Amendments To Draft Decree On Sanctions Against Administrative Violations In the Field of Cybersecurity, November 2021, https://globaldataalliance.org/wp-content/uploads/2021/11/en11182021gdaadminviocybersec.pdf.

[16] GDA Comments on Proposed Amendments to Draft Decree 72, September 2021, https://globaldataalliance.org/wp-content/uploads/2021/09/en09062021vtdrftdecree72.pdf.

[17] GDA Comments on Draft Viet Nam Personal Data Protection Decree, April 2021, https://globaldataalliance.org/wp-content/uploads/2021/07/en04092021gdavnpdpd.pdf.

ANNEX I: Model Digital Trade Provisions

Article __: Supporting Cross-Border Access to Information

The Parties recognize that the ability to access, store, process, and transmit information across borders supports:

1. The legitimate policy objectives of the Parties, including those relating to the protection of the environment, health, privacy, safety, security, and regulatory compliance;
2. Sustainable economic development and shared economic prosperity, including through greater cross-border connectivity, including for Micro-, Small-, and Medium-Sized Enterprises;
3. Financial inclusion and security, including for those lacking access to banking resources, as well as fraud prevention, anti-money laundering, and financial transparency;
4. Healthcare delivery, research and development of new healthcare treatments, cross-border healthcare regulatory collaboration, and global medical humanitarian assistance;
5. Scientific progress, including through cross-border access to knowledge and information, cross-border data analytics, and cross-border research and development (R&D) needed to develop technological solutions to meet global challenges;
6. Cybersecurity, including through an enhanced ability to detect cybersecurity risks, respond to cybersecurity threats, and recover from cybersecurity incidents through real-time cross-border data access and visibility; and
7. Climate change response, including through improved cross-border carbon emissions tracking and predictive climate modeling based on multi-regional data sets that can help communities to prepare for climate-related risks and identify mitigation and remediation strategies.

Article ___: Cross-Border Transfer of Information by Electronic Means

1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.
2. In the case of transfers of financial information, no Party shall prevent a covered person from transferring information, including personal information, into and out of the Party's territory by electronic or other means when this activity is for the conduct of business within the scope of the license, authorization, or registration of that covered person.
3. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary 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;[18] and
    b. does not impose restrictions on transfers of information greater than are necessary to achieve the objective.

Article ___: Location of Computing Facilities

1. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.
2. In the case of financial information, 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

[18] A measure does not meet the conditions of Paragraph 2(a) if it accords different treatment to transfers of information solely on the basis that those transfers are cross-border and if it does so in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party.

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.[19]

3. Examples of measures that would breach paragraphs 1 and 2 include those that:
    a. require the use of computing facilities or network elements in the territory of a Party;
    b. require the use of computing facilities or network elements that are certified or approved in the territory of a Party;
    c. require the localization of information in the territory of a Party;
    d. prohibit storage or processing of information outside of the territory of the Party;
    e. provide that the use of computing facilities or network elements in its territory, or the storage or processing of information in its territory, is a condition of eligibility relating to:
        i. technical regulations, standards, or conformity assessment procedures;[20]
        ii. licensing requirements and procedures;[21]
        iii. qualification requirements and procedures;[22] or
        iv. other governmental measures that affect trade; or
        v. condition market access upon the use of computing facilities or network elements in its territory or upon requirements to store or process information in its territory.
4. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary 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;[23] and
    b. does not impose requirements that are greater than are necessary to achieve the objective.

Article __: Customs Duties

No Party shall impose customs duties[24] on electronic transmissions, including content transmitted

---

[19] 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. 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.

[20] "Technical regulation", "standard" and "conformity assessment procedure" have the meaning set forth in the WTO Agreement on Technical Barriers to Trade, Annex 1, at: https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm.

[21] "Licensing requirement and procedure" has the meaning set forth in the WTO Reference Paper on Services Domestic Regulation, at: https://docs.wto.org/dol2fe/pages/ss/directdoc.aspx?filename=q:/wt/l/1129.pdf&open=true

[22] *Id.*

[23] A measure does not meet the conditions of Paragraph 4(a) if it modifies conditions of competition to the detriment of service suppliers of another party by according different treatment on the basis of the location of computing facilities used, or on the basis of the location of data storage or processing.

[24] "Customs duty" includes any duty or charge of any kind imposed on or in connection with the importation of a good, and any surtax or surcharge imposed in connection with such importation, but does not include any:(i) charge equivalent to an internal tax imposed consistently with Paragraph 2 of Article III of the GATT 1994; (ii) fee or other charge in connection with the importation commensurate with the cost of services rendered; or (iii) antidumping or countervailing duty.

electronically, between a person of a Party and a person of the other Party.

Article __ : Supporting Digital Trust

The Parties place a high value on building and strengthening public trust in the digital environment, and in that regard, recognize that:

1. Promoting personal information protection, consumer protection, and safeguards against unsolicited electronic communications can help enhance confidence in digital trade and can facilitate the delivery of economic and social benefits to citizens;
2. Protecting the integrity of source code and algorithms from malicious cyber-related compromise or theft necessitates limits on forced technology transfer and access mandates, but – at the same time – regulatory bodies and judicial authorities can have legitimate regulatory or judicial reasons to require that source code or algorithms be preserved or made available for a specific investigation, inspection, examination, enforcement action, or judicial proceeding;
3. Protecting cybersecurity through cyber-incident detection, response, and recovery depends in part upon effective cybersecurity risk management and real-time cross-border access to cybersecurity-related technologies and cyber threat indicators; and
4. Adopting Artificial Intelligence (AI) risk management frameworks can help ensure that AI is developed and deployed to produce benefits for the health and well-being of citizens, to safeguard democratic values, and to help enterprises map, measure, manage, and govern high-risk uses of AI, including those that may result in unlawful discrimination.

Article __: Protecting Personal Information and Privacy

1. Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade.[25] In the development of this legal framework, each Party should take into account principles and 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 Transborder Flows of Personal Data (2013).
2. The Parties recognize that pursuant to paragraph 1, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. The Parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented.
3. Each Party shall adopt or maintain non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction.
4. Each Party shall publish information on the personal information protections it provides to users of digital trade, including how:
    a. a natural person can pursue a remedy; and
    b. an enterprise can comply with legal requirements.
5. Recognizing that the Parties may take different legal approaches to protecting personal information, each Party shall encourage the development of mechanisms to promote compatibility and interoperability between these different approaches. These mechanisms include:
    a. broader international and regional frameworks, such as the APEC Cross Border

[25] For greater certainty, a Party may comply with the obligation paragraph 1 by adopting or maintaining measures such as comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.

Privacy Rules;

b. mutual recognition of comparable protection afforded by their respective legal frameworks, national trustmarks or certification frameworks; or

c. other avenues of transfer of personal information between the Parties.

6. The Parties shall endeavor to exchange information on how the mechanisms in paragraph 5 are applied in their respective jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility and interoperability between them.

7. The Parties recognize that the APEC Cross Border Privacy Rules System and/or APEC Privacy Recognition for Processors System are valid mechanisms to facilitate cross-border information transfers while protecting personal information.

8. The Parties shall endeavor to jointly promote the adoption of common cross-border information transfer mechanisms, such as the APEC Cross Border Privacy Rules System.

Article __: Protecting Source Code Integrity

1. No Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.

2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available[26] the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure.

Article ___: Protecting Cybersecurity

1. The Parties shall endeavor to:

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

   b. strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices.

2. Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity incidents.

3. Given that cybersecurity certification requirements and other measures may increase risk when they contain elements that impair cross-border coordination or access to cybersecurity technologies, each Party's cybersecurity certification standards and other measures shall treat service suppliers from other Parties no less favorably than domestic service suppliers, including in respect of the domicile, nationality, or degree of foreign affiliation or ownership of the service supplier; in respect of the country of origin of the technology; and in respect of the location of computing facilities and the cross-border transfer of information.

[26] This making available shall not be construed to negatively affect the software source code's status as a trade secret, if such status is claimed by the trade secret owner.

Article ___: Promoting Trust in Artificial Intelligence

1. Each Party recognizes the importance of developing governance frameworks for the trusted, safe, and responsible development and use of AI technologies. To that end, each Party should take into account the OECD Principles on Artificial Intelligence. The Parties endorse the OECD's five recommendations to policymakers pertaining to national policies and international co-operation for trustworthy AI, namely: (2.1) investing in AI research and development; (2.2) fostering a digital ecosystem for AI; (2.3) shaping an enabling policy environment for AI; (2.4) building human capacity and preparing for labor market transformation; (2.5) and international co-operation for trustworthy AI.
2. Consistent with OECD Recommendations 2.2 – 2.3, the Parties acknowledge the benefits of supporting interoperable legal frameworks and voluntary consensus-based standards and best practices relating to AI. Each Party shall encourage organizations within their jurisdiction that develop and deploy AI systems to risk-based approaches that rely on consensus-based standards and risk management best practices to map, measure, manage, and govern high-risk uses of AI.
3. Consistent with OECD Recommendation 2.5, each Party recognizes that AI systems should not result in unlawful discrimination on people based on their race, color, religion, sex, national origin, age, disability and genetic information or any other classification protected by the law of the Party. Each Party also recognizes that existing nondiscrimination laws remain enforceable in instances involving the use of AI.
4. Consistent with OECD Recommendation 2.4, and recognizing the importance of workforce development for AI-related technical skills to empower and enable current and future generations of workers and to improve the quality of life of our people, the Parties shall, subject to the availability of resources, upon request, and on mutually agreeable terms and conditions, exchange information and best practices, and otherwise cooperate, to:
    a. develop programs to train and reskill workers for AI and other high-demand technology skills;
    b. invest in apprenticeship programs and other alternative pathways to future employment that require AI and other high-demand technology skills;
    c. explore public-private partnerships to expand the availability of real-time labor data that can improve employer and worker visibility into the AI and other digital skillsets that are most in-demand in their markets, allowing them to make informed choices about the types of reskilling efforts that will generate the most opportunity; and
    d. invest in inclusive science, technology, engineering and math education, with an emphasis on computer science, at all levels of the educational system.
5. Consistent with OECD Recommendation 2.1, each Party shall promote sustained investment in AI R&D and public-private collaboration across the region. The Parties shall, subject to the availability of resources, upon request, and on mutually agreeable terms and conditions, collaborate to:
    a. take stock of and utilize existing science and technology cooperation and multilateral cooperation frameworks involving Parties;
    b. recommend priorities for future cooperation, particularly in R&D areas where the Parties share strong common interests, face similar challenges, or possess relevant expertise;
    c. coordinate as appropriate the planning and programming of relevant activities, including promoting collaboration among government entities, the private sector, and the scientific community;
    d. promote AI R&D, focusing on challenging technical issues, and protecting against efforts to adopt and apply these technologies in the service of authoritarianism and repression; and
    e. explore the development of sharing best practices on public data sets to unlock AI innovation and exchanges of information on regulatory frameworks to remove barriers

to innovation.

Article __: Protecting Transparency and Fairness in Digital Standard-Setting

1. Scope and Definitions
    a. Scope: This section applies to technical regulations, standards and conformity assessment procedures regarding the development, distribution, and supply of digitally enabled services.
    b. Definitions:
        i. Digitally enabled services are services that are performed or delivered electronically. They include services that relate to a process or a production method associated with a product. They also include services that do not relate to such a process or method.[27]
        ii. "Technical regulations," "standards," and "conformity assessment procedures" are defined as set forth in the WTO Agreement on Technical Barriers to Trade.
2. Affirmation of the Right to Regulate

    The Parties reaffirm the right to regulate within their territories through measures necessary to achieve legitimate policy objectives as set forth in GATS Article XIV.
3. Application of WTO Domestic Regulations text and Good Regulatory Practices Provisions to digitally enabled services standards and conformity assessment procedures

    For greater certainty, the provisions of the Domestic Regulations and Good Regulatory Practices provisions included in this Agreement shall apply to digitally enabled services standards and conformity assessment procedures.
4. Best Regulatory Practices Regarding Digitally Enabled Services Standards and conformity assessment Procedures.

    To promote transparency, interoperability, and non-discrimination, each Party agrees to:
    a. treat non-national products, services, or technologies no less favorably than like domestic products, services, or technologies in relation to technical regulations, standards and conformity assessment procedures;
    b. adhere to relevant international standards, where they exist or their completion is imminent;
    c. provide an explanation and justification if the Party does not adhere to a relevant international standard; and
    d. commit to provide adequate notice and consultation periods prior to adopting any new technical regulation, standard, or conformity assessment procedure relating to digitally enabled services.

Article __: Protecting Democratic Accountability in Government Access to Privately Held Data:

Each Party affirms its support for the OECD Declaration on Government Access to Personal Data held by Private Sector Entities and affirms the importance of the seven core principles of that Declaration, including legal basis, legitimate aims, approvals, data handling, transparency, oversight, and redress.

[27] For greater certainty, digitally enabled services technical regulations and standards that relate to product characteristics or their related processes and production methods, or the terminology, symbols, symbols, packaging, marking or labelling requirements as they apply to a product, process or production method are within the scope of the WTO TBT Agreement and therefore subject to its requirements and procedures.

Each Party shall adopt or maintain a legal framework that implements these seven principles.

Article __: Protecting Consumers Online

1. The Parties recognize the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent or deceptive commercial activities as referred to in Article ___ (cross reference to Consumer Protection) when they engage in digital trade.
2. Each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.
3. The Parties recognize the importance of, and public interest in, cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border digital trade in order to enhance consumer welfare. To this end, the Parties affirm that cooperation under consumer protection under Article __ (cross reference) includes cooperation with respect to online commercial activities.

Article __: Protecting Against Unsolicited Commercial Electronic Communications

1. Each Party shall adopt or maintain measures providing for the limitation of unsolicited commercial electronic communications.
2. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic communications sent to an electronic mail address that:
    a. require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or
    b. require the consent, as specified in the laws and regulations of each Party, of recipients to receive commercial electronic messages.
3. Each Party shall endeavor to adopt or maintain measures that enable consumers to reduce or prevent unsolicited commercial electronic communications sent other than to an electronic mail address.
4. Each Party shall provide recourse in its law against suppliers of unsolicited commercial electronic communications that do not comply with a measure adopted or maintained pursuant to paragraph 2 or 3.
5. The Parties shall endeavor to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic communications.