Model Digital Trade Provisions on Cross-Border Data and Digital Trust

Model Provisions re Cross-Border Data

1. **Supporting Cross-Border Access to Information**
2. **Cross-Border Transfer of Information by Electronic Means**
3. **Location of Computing Facilities**
4. **Customs Duties**

Model Provisions re Digital Trust

1. **Supporting Digital Trust**
2. **Protecting Personal Information and Privacy**
3. **Protecting Cybersecurity**
4. **Protecting Source Code Integrity**
5. **Protecting Procedural Limits on Government Access to Privately Held Personal Data**
6. **Protecting Consumers Online**
7. **Protecting Against Unsolicited Commercial Electronic Communications**
8. **Protecting Transparency and Fairness in Digital Standard-Setting**
9. **Promoting Trust in Artificial Intelligence**
10. **Promoting Trust in Government Data**

Model Provisions on Cross-Border Data

Article 1: Supporting Cross-Border Access to Information

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

(a) The legitimate policy objectives of IPEF Parties, including those relating to the protection of the environment, health, privacy, safety, security, and regulatory compliance;
(b) Sustainable economic development and shared economic prosperity, including through greater cross-border connectivity, including for Micro-, Small-, and Medium-Sized Enterprises;
(c) Financial inclusion and security, including for those lacking access to banking resources, as well as fraud prevention, anti-money laundering, and financial transparency;
(d) Healthcare delivery, research and development of new healthcare treatments, cross-border healthcare regulatory collaboration, and global medical humanitarian assistance;
(e) 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;

(f) 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

(g) 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 2: 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;[1] and

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

Article 3: 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 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.[2]

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;

[1] 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.

[2] 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.

(c) require the localization of information in the territory of a Party;

(d) prohibit storage, access, 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;[3]

(ii) licensing requirements and procedures;[4]

(iii) qualification requirements and procedures;[5] or

(iv) other governmental measures that affect trade; or

(f) 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;[6] and

(b) does not impose requirements that are greater than are necessary to achieve the objective.

Article 4: Customs Duties

No Party shall impose customs duties[7] on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of the other Party.

[3] "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

[4] "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

[5] *Id.*

[6] 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.

[7] "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.

Model Provisions on Digital Trust

Article 1: 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.
5. Reflecting a shared commitment among like-minded democracies to ensure that protections for privacy and other human rights and freedoms are in place with respect to law enforcement and national security access to personal data held by private sector entities.

Article 2: Protecting Personal Information

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.[8] 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,

[8] 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.

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 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 6 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 3: 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.

Article 4: 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[9] 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 5: Protecting Procedural Limits on Government Access to Privately Held Personal Data

Each Party affirms its support for the OECD Declaration on Government Access to Personal Data held by Private Sector Entities,[10] and affirms the importance of the seven core principles of that Declaration, including legal basis, legitimate aims, approvals, data handling, transparency, oversight, and redress. Each Party shall adopt or maintain a legal framework that implements these seven principles.

Article 6: 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 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 regarding consumer protection includes cooperation with respect to online commercial activities.

Article 7: 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.

[9] 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
[10] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

5. The Parties shall endeavor to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic communications.

Article 8: 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.[11]
      (j) "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 and Good Regulatory Practices Provisions

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 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 9: Promoting Trustworthy 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

[11] 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.

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 IPEF 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 IPEF 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 10: Promoting Trust in Government Data

1. The Parties recognize that facilitating public access to and use of government information fosters

economic and social development, competitiveness, and innovation.

2. To the extent that a Party chooses to make government information, including data, available to the public, it shall endeavor:

a. To ensure that the information is in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed;
b. To improve data and model inventory documentation to enable discovery and usability; and
c. To incorporate public feedback to improve the quality of information available.

3. Parties shall endeavor to cooperate to identify ways in which each Party can expand access to and use of government information, including data, that the Party has made public, with a view to enhancing and generating business opportunities, especially for small and medium-sized enterprises.

4. Each Party shall encourage the development of frameworks to allow for the voluntary pooling, sharing, or exchanging, on mutually agreeable terms, of information, including data, in machine-readable and open format.