Model International Agreement Provisions re Cross-Border Access to Information

Article ___: 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 ___: 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 ___: 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;
   (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 ___: 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.

Model International Agreement Provisions re Digital Trust

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 can help enhance confidence in digital trade and can facilitate the delivery of economic and social benefits to citizens;
2. Promoting interoperability among legal frameworks for personal information protection is important to facilitate cross-border information transfer while protecting digital trust;
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

Article __: 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. 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
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 those found in the Global Cross Border Privacy
Rules Forum.

Article ___: Managing Cybersecurity Risk

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.
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.

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.

“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

“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

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.

“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.

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.