GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

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.[1] 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.

[1] 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.