ASIA INTERNET COALITION (AIC) CLOUD WORKSTREAM
International Best Practices for Data Sharing

The World Development Report 2021 hails data's potential for economic development. The COVID-19 pandemic has exposed how rapidly economies may pivot to online models, facilitated by and dependent on platforms that rely on the Internet's data transfer infrastructure. Data flows have been crucial for important aspects of the crisis response, ranging from data sharing for medical research and diagnosis to digital services' adoption for business continuity and online learning models.

The world's economies are increasingly data driven as they move towards "Society 5.0". International trade, industrial production and societal functions depend on efficient access to data, while the costs of data restrictions are also increasing. The future of smart manufacturing, as well as the use of data to tackle challenges such as pandemics and ageing societies, highlights the importance of open and trusted data flows for our societies. Data flows are also the backbone of today's diversified supply chains. Interconnected infrastructure and services mean that international data flows occur sometimes even for local business operations or consumer interactions.

The AIC Cloud Workstream would like to share the following three considerations:

1. Recognize the Shared Responsibility Model

First and foremost, it is important to recognize that security of data is a shared responsibility between cloud service providers (CSPs) and its customers. Many CSPs maintain shared responsibility models, wherein the CSP is responsible for the security of the cloud, such as the host operating system and infrastructure, while the customer is responsible for security in the cloud, including how they manage their data, classify their assets, and use the appropriate tools to apply the appropriate permissions for storing and retrieving data. As CSPs do not have visibility into its customer data, any requests for its customers' data should be directed to the customer. Data sharing mechanisms that are developed should always account for these distinctive roles, in order to avoid conflating responsibilities around data sharing requests.

2. Encourage Cross Border Data Flows

Furthermore, it is critical to ensure trust in data flows between countries. Countries are increasingly fragmented in their approach to data regulation. Data restrictions that prohibit or significantly encumber cross-border data flows have also recently become commonplace in domestic data governance measures. These manifest in different forms and are motivated by a variety of domestic policy objectives, such as privacy, security, access to data and industrial policy.

Free cross-border data flows are essential for the development of the digital economy – the region's engine of trade growth, job creation, innovation and productivity. Allowing data to flow freely across borders will help maximise the potential of Southeast Asia's booming Internet sector, which is poised to exceed US$300 billion by 2025. The OECD states that "cross-border data flows have increased economic efficiency and productivity, raising welfare and standards of living."

Restrictions on data flow, such as data localisation, are likely to hamper inclusive economic growth prospects, dampen foreign investment and innovation, and restrict opportunities for local businesses to grow domestically and globally. Governments must consider the significant losses that will be incurred by local SMEs if faced with data localisation laws of other countries.

The AIC supports and is committed to data privacy and security. However, data localisation requirements can result in the unintended consequence of increasing cybersecurity vulnerabilities, risk, and the cost of doing business.

- Data localization measures do not improve security because data security is based on the technical, operational, and managerial practices used to secure the data – not the location of the data.
- The location of data servers does not determine security. International companies have invested significantly to put world-class systems, processes, infrastructure, talent in place to secure data in a cloud environment.
- For SMEs that do not have an international footprint, the free flow of data across borders enables them to use common infrastructure to serve their customers in multiple markets.

The AIC urges governments to allow free cross border data flows that will promote the growth of a digital economy, harnessing data analytics and creating the best possible ecosystem for local businesses to use digital technologies to thrive beyond borders.

The AIC suggests that countries adopt a comprehensive, consistent, principles-based, risk-based framework, underpinned by compliance with global standards and best practices. Government should create an environment that encourages participation and self-regulation to minimize risk and provide robust personal data protection and management. The policy should encourage accountability to address risk of harm to individuals rather than establish a prescriptive set of compliance requirements. An example of a well thought out risk-based approach for public policy can be found in the APEC Privacy Framework, which recommends adherence to a set of privacy principles: Preventing Harm, Notice, Collection Limitations, Uses of Personal Information, Choice, Integrity of Personal Information, Security Safeguards, Access and Correction and Accountability.

3. Refer to International Best Practices for Data Sharing Mechanisms

(a) Consistency with International Standards and Best Practices

A data management framework should leverage international industry standards and best practices. Improving security hygiene and data governance should be the main objective of a data protection framework, and international security and privacy standards and code of practices that have proven their efficiency should be recognized as an appropriate voluntary mechanism for demonstrating compliance with domestic privacy laws and frameworks.

International standards can help structure and categorise shared data sets. This will help businesses, especially SMEs build trust with different partners and stakeholders in the region. ISO standards provide clear, comprehensive and transparent framework on how to minimise security risks that might lead to security incidents. Companies should be encouraged to refer to the below ISO standards when managing internal and external data.

- ISO/IEC 9001 Quality Management System
- ISO/IEC 27001 Security Management System
- ISO/IEC 27017 Cloud Specific Controls
- ISO/IEC 27018 Code of Practice for Protection of Personally Identifiable Information in Public Clouds

(b) Mutual Legal Assistance Treaty (MLATs)

Governments should consider diplomatic channels, such as signing a Mutual Legal Assistance Treaty (MLAT) with relevant jurisdictions, and acceding to the Budapest Convention. These steps would create reliable legal channels through which law enforcement officials could request digital evidence from other jurisdictions.

MLATs enable the transfer of information to other countries in response to appropriate legal requests for information (e.g., relating to criminal acts). A MLAT provides a process whereby one country's law enforcement personnel can request information held by a communication service provider in another country. A key limit with MLATs, however, is the time taken to respond to a request for data.

Data localization is a sub-optimal and inefficient option when responding to the challenges facing local law enforcement and in countering the inadequacies of the MLAT process. Instead, two reforms should be considered. The most immediate is reform of the MLAT process to better accommodate requests for electronic data. The second longer term reform is to consider negotiating data sharing agreements—bilaterally or multilaterally.

Clarifying Concerns around the CLOUD Act:

The CLOUD Act does not provide unfettered access to personal data by law enforcement. The CLOUD Act is designed to allow reciprocal access to data between U.S. and bilateral agreement partners, but only through an agreed and approved legal process. It does not ignore, supersede or change another country's local laws.

There is no provision within the CLOUD Act for the decryption of data that CSPs hold on behalf of their users or customers. The act does not expressly allow law enforcement to unencrypt data that is under the control of the end user. This is important: even if data encrypted by the CSP could be forced to be disclosed, data encrypted by the customer could not be decrypted by the CSP.

CSPs can often be a great resource to help organizations navigate the complexities of the CLOUD Act - particularly around how it affects their services. To this end, many CSPs offer services that can support the protection of customer data, such as encryption and key management.

(c) Data Sharing Agreements

This refers to multilateral agreements such as the APEC Cross Border Privacy Rules (CBPR) System and the General Data Protection Regulation (GDPR), as well as bilateral agreements such as the UK-US Bilateral Data Sharing Agreement, and Joint Statement of Intent on Data Connectivity issued by Bangko Sentral ng Pilipinas (BSP) and the Monetary Authority of Singapore (MAS) in November 2020.

i. APEC Cross Border Privacy Rules (CBPR) System

Organizations that choose to participate in the APEC CBPR System should implement privacy policies and practices consistently with the CBPR program requirements for all personal information that they have collected or received that is subject to cross-border transfer to other participating APEC economies. These privacy policies and practices should be evaluated by an APEC-recognized Accountability Agent for compliance with the CBPR program requirements. Once an organization has been certified for participation in the CBPR System, these privacy policies and practices will become binding as to that participant and will be enforceable by an appropriate authority, such as a regulator to ensure compliance with the CBPR program requirements.

Furthermore, the APEC Cross Border Privacy Enforcement Arrangement (CPEA), which is an important component of the CBPR System, creates a framework for the voluntary sharing of information and provision of assistance for data privacy enforcement-related activities. Any Privacy Enforcement (PE) Authority in an APEC economy may participate. The CPEA aims to facilitate information sharing among PE Authorities in APEC Economies (which may include Privacy Commissioners' Offices and Data Protection Authorities that enforce privacy laws).

The CPEA provides a mechanism to promote effective cross-border cooperation between authorities in the enforcement of CBPR program requirements and privacy laws generally, and encourages cooperation on privacy investigation and enforcement with PE Authorities outside APEC (including by ensuring that the CPEA can work seamlessly with similar arrangements in other regions and at the global level).

ii. General Data Protection Regulation (GDPR)

The European Parliament adopted the GDPR in April 2016. It requires that any company that stores or processes personal information about EU citizens within EU states must comply with the GDPR, even if they do not have a business presence within the EU.

As a general rule, transfers of personal data to countries outside the European Economic Area (EEA) may take place if these countries are deemed to ensure an adequate level of data protection. There are, however, some exceptions to the general rule. Personal data can be transferred to a third country even in the absence of an adequacy decision if the controller or processor exporting the data has himself provided for appropriate safeguards; and on the condition that enforceable data subject rights and effective legal remedies are available in the given country.

The appropriate safeguards can be laid down via the following instruments:

- Binding corporate rules which are internal codes of conduct adopted by multinational groups of undertakings, and allow transfers between different entities of the group;
- Standard contractual clauses adopted by the European Commission or by a national supervisory authority and approved by the European Commission;
- Other ad hoc contractual clauses agreed between the data exporter and the data importer which can be deemed to be appropriate if they have been submitted and authorized by the competent national supervisory authority.

In the absence of an adequacy decision or of appropriate safeguards as listed above, a cross-border transfer may still take place exceptionally in one of the specific situations listed in Article 49.

iii. UK-US Bilateral Data Sharing Agreement

The Agreement was signed in October 2019 and came into force in July 2020. It is not yet in use, as it remains subject to law enforcement putting data minimisation processes in place. It is considered the first of its kind, and will dramatically speed up investigations by enabling law enforcement, with appropriate authorisation, to issue overseas production orders (OPOs) directly to foreign tech companies in order to access their clients' data, rather than through governments using the traditional mutual legal assistance (MLA) route, which can take years.

The effect of the Agreement is that law enforcement in either the UK or the US can - under the appropriate domestic legislation (being the CLOUD Act 2018 in the US and Crime (Overseas Production Orders) Act 2019 (COPOA) in the UK) - when armed with appropriate court authorisation require companies that provide clients with an ability to communicate, process or store data, such

that they amount to 'communication service providers' (CSPs), to produce documents. The novel element of the process is that it is to be controlled by the courts of the requesting state.

iv. BSP-MAS Joint Statement of Intent on Data Connectivity

The BSP and MAS have issued a joint statement to announce their intent to promote the adoption and implementation of policies and rules that facilitate the following goals with respect to the operation of banks and non-bank financial institutions falling within the jurisdiction of either BSP or MAS ("covered institutions"):

- Covered institutions should be allowed to transfer data, including personal information, across borders by electronic means provided this activity is for the conduct of the business within the scope of their license, authorisation, or registration.
- The location where covered institutions can store and process their data should not be restricted as long as BSP and MAS have full and timely access to the data necessary to fulfill their regulatory and supervisory mandate.
- If BSP or MAS is unable to access the data, covered institutions should have the opportunity to remediate such lack of access before being required to use or locate computing facilities locally.

v. Data Free Flow with Trust (DFFT)

In his landmark speech at the World Economic Forum (WEF) Annual Meeting 2019 in Davos-Klosters, Japan's Prime Minister Shinzo Abe invited leaders to build an international order for Data Free Flow with Trust (DFFT). In June that same year, trade and digital economy ministers at the G20 Ministerial Meeting in Tsukuba under Japan's chairmanship stressed the significance of cross-border data flows for productivity, innovation and sustainable development.

Later at the G20 Osaka Summit, heads of government agreed to work towards the DFFT vision. The Osaka Leaders' Declaration states that legal frameworks – both domestic and international – should be respected. At the same time, the interoperability between each framework must be enhanced to allow data to flow more freely. The world leaders also confirmed the value of the "Osaka Track" – a collective term for the global governance processes needed to unleash the benefits of more open and trusted data flows.

The Osaka Track invites discussion on how stakeholders should cooperate across all regions and disciplines to achieve the vision of open and trusted data flows. The WEF is heeding the call through a dialogue involving experts, businesses and other stakeholders to develop the architecture for a more trusted and freer digital economy. The exercise maps the governance frameworks needed to realize the DFFT vision and the role of business and experts to support greater interoperability for information and knowledge that can be shared in safe and secure ways – through both technical as well as regulatory means.

(d) Model Contractual Clauses (MCCs)

The MCCs are template contractual terms and conditions that may be included in the binding legal agreements between businesses transferring personal data to each other across borders. This helps reduce the negotiation and compliance cost and time especially for SMEs while ensuring personal data protection when data is transferred across borders.

MCCs are an important component of data sharing agreements, as evident from the GDPR's Standard Contractual Clauses (SCCs). In January 2021 the ASEAN Digital Ministers' Meeting also approved the ASEAN Data Management Framework (the DMF) and the Model Contractual Clauses

for Cross Border Data Flows (the MCCs). While the MCCs are primarily designed for intra-ASEAN flow of personal data, parties may adapt these clauses with appropriate modifications at their discretion for transfers between businesses intra-country in ASEAN Member States (AMS), or transfers to non-AMS, particularly those with legal regimes based upon the principles of the APEC Privacy Framework or OECD Privacy Guidelines, from which the principles in the ASEAN Framework on Personal Data Protection (2016) are derived.

ASEAN has not stated that the use of the MCCs will ensure compliance with national data protection laws, and in fact the template includes optional clauses that will need to be tailored to specific national law requirements. In its guidance on the MCCs, ASEAN encourages organizations to check for local law guidance and templates and states that the MCCs are intended to help organizations identify issues arising in respect of cross border transfers and help achieve compliance with mandatory requirements.

(e) Trade Agreements

Comprehensive, multilateral free trade agreements have gained new value in the last decade and shape the regulatory environment for digital data flows across borders.
The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) has delivered important breakthroughs in promoting the free flow of data across borders for service providers and investors as part of their business activities. CPTPP countries have committed not to impose data localization requirements that would force businesses to build data storage centres or use local computing facilities in CPTPP markets, providing certainty to businesses considering their investment choices. Therefore, while CPTPP governments have retained the ability to maintain and amend regulations related to data flows, they have undertaken to do so in a way that does not create barriers to trade.

The Regional Comprehensive Economic Partnership (RCEP) echoes the CPTPP and other agreements' commitment to data mobility. RCEP uses CPTPP as its blueprint but modifies it in a way that retains countries' ability to craft restrictive data policies when they deem it necessary, i.e.; the rule is to not require the use of domestic computing facilities or to restrict the cross-border transfer of information. Exceptionally, such measures may be deployed under certain conditions. It is in this regard that RCEP deviates from TPP.

Other trade agreements with similar provisions to the CPTPP include the **United States-Mexico-Canada Agreement (USMCA)** and the **US-Japan Digital Trade Agreement.**

In line with the CPTPP model, **digital economic agreements (DEAs)** also establish common frameworks and rules for digital trade that will enable companies in a given country to connect digitally with their overseas partners more seamlessly. The DEAs will support cross border data flows while safeguarding personal data, and align digital rules and standards, and facilitate interoperability between digital systems.

Singapore, for example, has embarked on a range of DEAs, including the **Digital Economy Partnership Agreement (DEPA)** between Singapore, Chile and New Zealand and the **Singapore-Australia Digital Economy Agreement (SADEA).** The city-state has also begun negotiations on the **Korea-Singapore Digital Partnership Agreement.**