29 June 2020

Subject: Asia Internet Coalition (AIC) Comments on the Guide to Managing Data Intermediaries (DIs) under the Singapore Personal Data Protection Act ("PDPA")

Comments and Recommendations

---

1. Contract between data controller and data intermediary

It is not clear from the Guide whether the Personal Data Protection Act ("PDPA") itself will make it mandatory for there to be a contract between the data controller ("DC") and the data intermediary ("DI"). For example:

- Paragraph 2.1 suggests that the DI is defined as an organisation that processes personal data on behalf of a DC pursuant to a contract. The DI may carry out any operation or set of operations in relation to the personal data which may include, but are not limited to, the following: a) recording; b) holding; c) organisation, adaptation or alteration; d) retrieval; e) combination; f) transmission; and g) erasure or destruction. However this does not appear to be set out in the PDPA or the draft amendment of the Act.

- Paragraph 3.9 states that the 'primary means' by which a DC can ensure appropriate protection and retention of personal data processed by a DI is through a contract. However, it is not clear whether this provision is mandatory.

- Paragraph 3.10 suggests that there should be a binding contractual agreement in place between the DC and the DI. However if there is no contract made in writing, the key obligations and responsibilities should be evidenced in writing.

- Paragraph 3.16 suggests there is a requirement in the PDPA for a contract. If a contract is mandatory, this should be made clear in the PDPA itself and in the Guide.

2. Reference to international standards/certification

We recommend PDPC to tie in / recognise international standards and certifications where appropriate. Paragraph 3.7 should also acknowledge other certifications in APEC and ASEAN. These include Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) System, APEC Privacy Recognition for Processors (PRP) System certifications and ASEAN Framework on Personal Data Protection.

Further, several Singapore could also recognise that an exporting organisation may discharge its data transfer obligations where an overseas organisation adheres to a locally approved Code of conduct or Privacy Code. This option is interesting to explore as Privacy Codes already play an important role to supplement the data protection frameworks of several jurisdictions in the region. Such recognition would be subject to the legally binding nature of the Code and the conclusion of a contract between both the exporting and importing organisations to ensure that the safeguards of the Code (in particular, those concerning the rights of data subjects) are applied and enforced in the receiving jurisdiction. To build coherent policies on such Codes, regulators and the industry could work together on several building blocks: the criteria by which such Codes may be approved; the conditions under which Codes may be found legally binding in multiple jurisdictions; determination of appropriate recourse mechanisms for individuals in case of breach occurring overseas; criteria for accreditation of the monitoring body that will ensure compliance with the Code, to ensure equality in independence, competence, adequate resourcing, and accountability; the identification of sufficient and clear benefits of signing up to a Code to ensure that organisations obtain a return on the investment to joining that Code.

In evaluating a potential DI, the DC should be satisfied that the DI has the necessary data protection framework, and some recommended privacy standards and certifications for PDPC to consider include:

International Standards	Description
ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems – Requirements[1]	Specifies the requirements for establishing, implementing, maintaining and improving an information security management system within the context of an organization. It includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature. ISO/IEC 27001 should be a default cybersecurity standard to be implemented by all organizations and is already widely adopted by many governments in ASEAN.
ISO/IEC 27701:2019: Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management –	Specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

[1] https://www.iso.org/standard/54534.html

Requirements and guidelines[2]	This standard also specifies PIMS-related requirements and provides guidance for PII controllers and PII processors which are responsible and accountable for PII processing.
ISO/IEC 29100:2011: Information technology – Security techniques – Privacy framework[3]	Provides a privacy framework through the use of a common privacy terminology; defines the actors and their roles in processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology. It is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.
ISO/IEC 29101:2018: Information technology – Security techniques – Privacy architecture framework[4]	Defines a privacy architecture framework that: specifies concerns for ICT systems that process PII; lists components for the implementation of such systems; and provides architectural views contextualizing these components. This document is applicable to entities involved in specifying, procuring, architecting, designing, testing, maintaining, administering and operating ICT systems that process PII. It focuses primarily on ICT systems that are designed to interact with PII principals.
ISO/IEC 27018:2019: Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors[5]	Establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect PII in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.
Multi-Tier Cloud Security (MTCS) Standard For Singapore (SS 584) (2013)[6]	The Multi-Tier Cloud Security (MTCS) Standard for Singapore builds upon recognized international standards such as ISO/IEC 27001, and covers such areas as data retention, data sovereignty, data portability, liability, availability, business continuity, disaster recovery, and incident management. It also includes a mechanism for customers to benchmark and rank the capabilities of CSPs against a set of minimum baseline security requirements.

[2] https://www.iso.org/standard/71670.html
[3] https://www.iso.org/standard/45123.html
[4] https://www.iso.org/standard/75293.html
[5] https://www.iso.org/standard/76559.html
[6] https://www.imda.gov.sg/-/media/Imda/Files/Inner/About-Us/Newsroom/Media-Releases/2013/1311_cloudasia/MTCSFactSheet.pdf?la=en

	MTCS includes a total of 535 controls, covering basic security in Tier 1, more stringent governance and tenancy controls in Tier 2, and reliability and resiliency for high-impact information systems in Tier 3. MTCS Tier 3 certification is generally regarded as necessary for providing cloud services to regulated sectors such as financial services, healthcare, and highly confidential business data.

3. Considerations on Developing Contract Clauses

Contractual controls could contain at least the following information:

- description of envisaged transfers;
- applicable data protection principles;
- warranties, rights and obligations of the parties (including with regard to management of data breach notification procedures);
- measures to ensure that the data protection rights of individuals are implemented overseas;
- recourse of individuals, complaints and compliance mechanisms;
- liability and enforceability by third parties;
- applicable law; and
- dispute resolution.

At the same time, model contracts or standard clauses should allow for flexibility in implementation (e.g. allowing for data protection clauses to be inserted into master or multi-party agreements; allowing variation of model clauses to accommodate different industries and sectors or specific data, etc).

On 11 May 2020, the Office of the Privacy Commissioner of New Zealand has announced that it is working on developing a model set of contract clauses for New Zealand agencies, on which it will publicly consult in August 2020. It is also worth underlining that ASEAN Members are contemplating the development of *ad hoc* model clauses for data transfers as one of the components of the ASEAN Cross-border Data Flow Mechanism.