Public Consultation on Public Consultation on Personal Data Protection (Amendment) Bill 2020

A point of view from AsiaDPO

28 May 2020

AsiaDPO is a Singapore registered society of a self-organising peer-to-peer community of Data Protection Officers (DPOs). We are committed to the development and advancement of data protection and privacy domains through a practice-led approach, serving as an expert group with a distinctive voice.

Contact Person
Huey Tan
President AsiaDPO
president@asiadpo.org

A DPO View: Public Consultation on Personal Data Protection (Amendment) Bill 2020

AsiaDPO remains the first and only self-organising, peer-to-peer registered society *by DPOs for DPOs*. AsiaDPO exists to develop and advance practices in data protection and privacy domains, to serve as a trusted resource of industry expertise and to be a distinctive voice for our members. This is the DPO in action, in practice. The DPO is uniquely placed to balance data use and protective outcomes by integrating *privacy, accountability and trust* into critical organisational capabilities. As agents of change in our own right, we have been calling for accountability based practices since at least 2017[1].

[1] See our article in the Dec 2019 edition of DPO Connect that explains our journey: *"Hello Great Expectations, Meet Accountability - Accountability follows the data and why it matters to Data Protection Officers building trust"* - https://www.pdpc.gov.sg/-/media/Files/PDPC/DPO-Connect/Dec-19/Hello-Great-Expectations-Meet-Accountability.

We thank the Ministry of Communications and Information (MCI) and the Personal Data Protection Commission (PDPC) for the opportunity to provide comments. We represent the viewpoints of the AsiaDPO community on the Public Consultation on the Personal Data Protection (Amendment) Bill 2020 is the culmination of dialogues and exchanges since 2017. This submission represents anonymised feedback from AsiaDPO members to the proposals in the Public Consultation, in line with AsiaDPO's constitution, which is designed to increase peer-to-peer collaboration in a safe and open environment.

Accountability and Role of DPO

AsiaDPO continues to encourage policymakers and regulators in the Asia-Pacific region to adopt a balanced and flexible approach to industry self-regulation. We continue to encourage MCI/PDPC to support organisations in investing and re-defining data protection principles, so as to turn principles into practical, repeatable and predictable data management practices that can be applied across diverse jurisdictions in Asia and beyond. We commend MCI/PDPC for recognising the challenges for organisations that translate principles of design into toolkits or frameworks and sustainable long-term practices, with humans embedded in the design of everyday things. Singapore has embraced our calls for accountability-based practices in the Personal Data Protection (Amendment) Bill 2020. In extraordinary times, we are glad to see Singapore's Foreign Minister (speaking about the "TraceTogether" contact tracing app) refer to the accountability principle: *"Maintaining trust, respecting privacy and getting voluntary participation is absolutely essential."*[2] Our DPO community of practice resembles this remark!

Mandatory Breach Notification

AsiaDPO supports breach notification schemes that balance incentives for organisations to maintain robust protections for personal data, while enabling individuals to take actions to protect themselves when their data is compromised[3]. We recognise that mandatory breach notification schemes can serve as a market differentiator and represent an organisation's accountability based practices as part of a DPO's toolbox. We are grateful to MCI/PDPC for incorporating feedback we submitted on behalf of the DPO communities of practice to:

1. limit mandatory breach notification to data breaches which "results in, or is likely to result in, significant harm to the affected individual"; and
2. provide an exception to mandatory breach notification if an organisation has (a) taken remedial action to reduce the likely harm or impact to an affected individual; and (b) implemented technological protection that is of a reasonable security standard such that the data breach is unlikely to result in significant harm to affected individuals.

---

[2] Foreign Minister Vivian Balakrishnan also referred to "TraceTogether" as a "...hybrid system based on public support, keeping public trust, and maintaining privacy": https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2020/05/20200522-Sky-News-Australia-FM

[3] We refer to our previous submissions dated 14 November 2019 (AsiaDPO Perspective: Mandatory Data Breach Notification Scheme (MDBNS)) and 29 September 2017 (Public Consultation on Managing Personal Data in the Digital Economy: A Point of View from AsiaDPO).

We continue to encourage regulators not to prescribe categories of personal data which, if compromised, would be considered likely to result in significant harm to individuals. In our view, that can create a framework that is overly reliant on checkbox compliance, rather than encouraging organisations to integrate accountability based practices into their personal data protection frameworks in a holistic way. Further, over-categorisation or under-classification has the unintended consequence of reinforcing data classification for the sake of it. It sets a precedent and provides justification for countries to promote their own data categorisation and classification with data localisation effects (for example, India and Indonesia have similar lists for data on-shoring). This has implications for DPOs in managing compliance of data flows, and has wider implications for Singapore in general.

We reiterate our recommendation that assessments of "systemic issues" should be tied to an assessment of harm, and the maturity and effectiveness of an organisation's data governance and management program, rather than a specific threshold (whether set at 500 individuals or otherwise). For example, an employee of an organisation that mistakenly sends personal information of 1,000 customers to a single recipient (bound by confidentiality obligations) on a single file, on a single occasion, may not suggest systemic issues. By contrast, the mistaken disclosure of a single patient's medical history through unencrypted channels (due to a lack of standards or policies) might suggest systemic issues. While the use of a numerical threshold may provide a rule of thumb for some companies to assess harm, this has to be balanced with DPOs and organisations spending time and resources to submit notifications that detract from other DPO responsibilities.

We seek clarification as to the conditions for determining what is "reasonable and expeditious" in the proposed Clause 26C that goes into deciding if a potential breach is notifiable. We would suggest that the actions taken by an organisation in a reasonable and expeditious manner should be linked with the nature of the potential breach and assessment of harm to affected individuals, and this could be included in guidelines for additional clarity for DPOs. As a procedural matter, we seek further revisions to clearly link the proposed definition of "data breach" to the occurrence of a security incident (proposed Section 26A). This could be problematic if the definition is extended to non-security incident linked events. To avoid limb (b) of the "data breach" definition being misinterpreted to include a network service outage that does not lead to individual harm, it could be further clarified in the guidelines to reflect that non-security incident linked events are not included in the definition of data breach.

In addition, we seek to clarify whether section 26D(3)(b) of the PDP Amendment Bill intended to oblige organisations to await a prescribed law enforcement agency or PDPC's instructions before notifying affected individuals of a notifiable data breach.

PSDSRC amendment

We are broadly sympathetic to holding third-parties legally responsible for specific harms, including DIs acting for a public agency. We foresee that the removal of the exclusion for organisations acting on behalf of public agencies as impacting accountability and affecting consumer trust. The confusion can arise as to whether DIs can reasonably take on its relevant obligations (i.e. retention and protection),

given that the principal (i.e. a public agency) is not subject to the PDPA. For example, what are "reasonable security arrangements" pursuant to Section 24 of the PDPA will depend on unpublished "reasonable security arrangements" that are determined by public agencies.

The new criminal offences that hold an individual personally liable for egregious mishandling of personal data in the possession of or under the control of an organisation should address specific harms, rather than a broad policy of excessive criminal penalties for non-compliance. The criminal offences are drafted widely and it is not immediately apparent how the criminal element applies in specific situations or whether this is indeed the policy intention. It will be helpful for MCI/PDPC to provide more examples, given that an individual may be personally liable for an improper or unauthorised use of personal data regardless of whether it is a notifiable breach. We understand that the intent is not to overlap where private recourse exists. In most cases of an improper use of personal data by an employee for his/her personal gain, this would attract liability under breach of confidentiality and duty of fidelity.

Meaningful notice and consent

We had previously welcomed MCI/PDPC's willingness for more flexibility within the existing "consent first" regime for collecting, using and disclosing ("processing") personal data. Since 2017, we have contributed to an industry dialogue on behalf of DPOs and worked together with MCI/PDPC to achieve greater clarity on boundaries of applicable use cases. AsiaDPO is generally in support of the introduction of legitimate interest ("LI") as an appropriate ground for processing personal data under PDPA. As practising DPOs, we encourage reliance upon LI as a ground for processing personal data in discrete, reasonable and commonly occurring processing activities such as fraud detection or prevention, information and system security, implementation of social safeguards, compliance with legal requirements, emergencies, and protecting the rights or property of individuals. It is not an uncommon view that LI generally does not replace consent; instead it is used to supplement consent for similar activities. Organisations would use existing channels to communicate processing of LI where it is the most appropriate ground for processing to signify organisational accountability and responsibility over personal data across all industries.

As a point of clarification, paragraph 40 of the Public Consultation paper indicates that the business improvement exception can apply to a group of companies (e.g. subsidiaries of the organisation). We do not think clause 32 of the draft PDP (Amendment) Bill currently captures this intent. We would request further clarification how this exception would apply specifically, as it affects transfer obligations between group companies.

Data portability

In discussions with PDPC in 2018, AsiaDPO was of the view that data portability may be difficult to implement in an Asian context due to a prevalence of small and open economies with different data protection frameworks, different notions of personal data, and the lack of harmonisation in the APEC and ASEAN frameworks with no consensus on portability. We felt that interoperability did not benefit from a fundamental personal right to data portability, and was largely incompatible with the current

PDPA, requiring a change in law. We sounded a warning bell about being overly prescriptive on data formats/interfaces due to the compliance heavy culture in Asia that could negatively impact innovation. We asked PDPC to take a wait-and-see approach, as the GDPR pioneered the evolution of the processes involved in data portability. We still continue to encourage Singapore to adopt a wait-and-see approach until the utility of data portability can be demonstrated, and not to place undue burdens on DPOs and their organisations to implement this.

In this regard, we thank MCI/PDPC for scoping the data portability obligation to:

1. User provided data and user activity data held in electronic form;
2. Individuals who have an existing, direct relationship with the organisation; and
3. Receiving organisations that have a presence in Singapore.

While MCI/PDPC intends to prescribe details of how the data portability obligation should be applied in regulations, we would request for a two-year transition period. Many organisations will require time to build solutions to implement data portability and to be compliant. For example, the European Union allowed organisations impacted by the GDPR a two-year transition period (from 25 May 2016 to 25 May 2018).

We would also recommend for the proposed "whitelist" of data categories to be narrowly scoped to meet the purpose of individuals switching to new service providers more easily. If the data portability obligation is widely scoped, it would undermine Singapore's competing national policy of promoting data innovation. Organisations would be discouraged from investing in data innovation and research if they are forced to port data that is commercially sensitive or may be reverse engineered (sharing the fruits of their investment with competitors for free). For example, it may be helpful for online retail users to port transaction details of their shopping history. However, data generated from specific features offered by a company, such as browse and discovery tools, or dedicated loyalty or gift card programmes, is unlikely to be readily usable by other companies. Such data should be treated as confidential and proprietary commercial information (that could be abused by competitors, and is typically generated for business improvement purposes) and excluded from the data portability obligation. Further, most types of user-generated content are sensitive in nature and sharing across companies could gravely undermine the privacy of both the requesting individual and third parties. To summarise, we recommend that the "whitelist" of data categories exclude types of data that provide no clear value to individuals' ability to switch providers, and/or take time for organisations to process, including (i) user activity data generated from the use of proprietary tools or features, (ii) user-generated content (such as voice recordings, videos, images, customer reviews and feedback), and (iii) unstructured data.

Separately, paragraph 48 of the Public Consultation document states that exceptions to the Data Portability Obligations will mirror those to the Access Obligation under the Fifth Schedule to the PDPA; however, we note that these exceptions are not included in the PDP Amendment Bill. We recommend that these exceptions (and the further exclusions we propose above) be codified in regulations. We recommend that MCI/PDPC should provide more exceptions to data portability than those listed in the

Fifth Schedule of the PDPA, as the data portability obligation imposes a heavier regulatory compliance and resource burden on organisations than the access obligation. We request for an additional exception - organisations should be allowed to refuse porting requests where it can be shown that such requests are not required for individuals to switch to a new service provider. This is in line with MCI/PDPC's objective of allowing individuals to switch to new service providers easily.

Clause 16 of the PDP Amendment Bill allows PDPC to review a fee required in relation to a data porting request. However, there is no other reference in the PDP Amendment Bill allowing organisations to charge a fee for processing a data porting request. Organisations may have to dedicate substantial financial and manpower resources to building solutions to meet the data portability obligation. The costs of such solutions may differ depending on the complexity of the data and industry. We request that MCI/PDPC allow organisations to charge a reasonable fee for processing a data porting request and to codify this fee in legislation. We would also urge MCI/PDPC to clarify the computation of such fees in guidelines.

Exclusion of "derived personal data" from Correction and Data Portability obligations

We seek clarification as to what would be considered "*derived personal data*" in clause 2 of the PDP Amendment Bill and the use of "*prescribed means or method*" does not appear to have been scoped or defined.

Paragraph 76 of the Public Consultation paper excludes "derived personal data" from Data Portability and Correction obligations, for reasons stated in paragraphs 48 and 49. We appreciate there are policy considerations for such exclusions, to protect business innovation and commercially sensitive information that safeguards investments by organisations to innovate. As such, it follows that "derived personal data" is also exempted from the Access obligation consistent with such policy considerations. We note the current Section 21 PDPA (Access requirement) arguably does not include "derived personal data", since "derived personal data" is a new concept introduced into the PDPA and would have an effect of broadening the current Access obligation on organisations.

Enforcement

We request that MCI/PDPC reconsider the proposal to impose a maximum financial penalty of 10% of an organisation's annual turnover (where a direction is given to an organisation with an annual turnover exceeding $10 million) for 2 primary reasons:

1. Such a financial penalty may be viewed as disproportionate to penalties under current sectoral laws and regulations. For example, section 13(1)(v) of the District Cooling Act allows the imposition of a financial penalty not exceeding 10% of the annual turnover derived from the provision of district cooling services. Similarly, section 54(1)(d) of the Casino Control Act allows the imposition of a financial penalty not exceeding 10% of a casino operator's annual gross gaming revenue only in the event of a serious breach. By comparison, the proposed financial penalty in clause 17 of the PDP Amendment Bill would apply to an organisation's annual

turnover in general and does not scale in proportion to the financial penalties that might be imposed by a sectoral regulator.

2. The Consultation Paper refers to the European Union's General Data Protection Regulation (which provides for a maximum financial penalty of 4% of an organisation's global annual turnover); and section 69(4) of the Singapore Competition Act (which allows the Competition and Consumer Commission of Singapore to impose a financial penalty of up to 10% an organisation's turnover in Singapore). As a frame of reference, breaches of EU competition law attract fines of up to 10% of the overall turnover of a company[4].

As can be seen, the penalties under EU data protection law are lower than the penalties under EU competition law. The differing penalties are justifiable, as the harm from a breach of competition law disrupts the normal functioning of a free market economy as a whole, whereas harm from breaches of data protection law is narrower in scope and typically accrues to individuals. Correspondingly, the proposed financial penalty in clause 17 of the PDP Amendment Bill should be lower than the financial penalty under section 69(4) of the Singapore Competition Act.

We seek to clarify that the PDP (Amendment) Bill is based on turnover in Singapore as per PDPC's intention in paragraph 58 of the Public Consultation document. To avoid penalising organisations that act in good faith, PDPC may also wish to consider introducing a provision that it may impose a financial penalty only if the infringement has been committed knowingly or recklessly. PDPC may also wish to consider encouraging the reporting of data breaches to PDPC by specifying that it will consider, as a strong mitigating factor, a reduction of financial penalties for organisations that demonstrate cooperation with PDPC and voluntary disclosure of potential breaches. This will mitigate the risk of organisations concealing potential breaches especially with the significant increment in financial penalties.

Conclusion

The laws and regulations of today can greatly shape the DPO profession of tomorrow. Balanced and flexible approaches to regulations, moving towards consistency across borders, will promote the development of DPO capabilities for predictable and complementary data management across jurisdictions. This can create real value to business development and consumer protection, and move the DPO up the value chain of executive decision making. We are encouraged by many facets of the PDP Amendment Bill to achieve protective outcomes while remaining flexible, drawing from practice-led experience. Again, we thank MCI/PDPC for taking into account the complexities of information flows and convergences across systems, territories and cultures; as set out in our first DPO viewpoint in 2017.

[4] Art 23(2), Council Regulation (EC) No 1/2003