Public Consultation on Managing Personal Data in the Digital Economy
A point of view from AsiaDPO

29 September 2017

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

Appendix

Asia DPO Detailed Commentary

This represents a compilation of the detailed commentary provided by AsiaDPO membership in a closed-door workshop on 6 Sept 2017 under *the Chatham House Rule*. We aggregate and anonymise feedback from members to the proposals in the PDPC consultation paper in line with AsiaDPO culture and constitution that is designed to increase peer-to-peer collaborations in a safe and open environment.

Notification of Purpose

I. A number of jurisdictions in the region including Australia, Japan and Hong Kong adopt a notification-based approach. We noticed that those jurisdictions do not require fulfillment of the proposed conditions of impracticality, have no expectation of any adverse impact on the individual, and have no requirement to conduct a risk assessment such as a DPIA.

II. The "any adverse impact" condition places the bar at such a high level that it is difficult to see when the Notification of Purpose legal basis could apply. For example, in the drone/recording device example cited in paragraph 3.11 of the PDPC paper, there could be some residual harm to people walking or commuting in those high traffic areas (e.g. individuals who would otherwise not want to be seen together but who are identifiable by their physique and/or what they are wearing despite their faces being obscured).

III. The words "*not* expected to have *any* adverse impact" also introduces a bright-line test that precludes a balancing of the risks against benefits and the consideration of mitigating measures identified and implemented in the ensuing risk assessment (as envisaged in paragraph 3.10 of PDPC paper). The outcome of any risk assessment does not mean the complete eradication of risk, as suggested by the words "*not* expected to have *any* adverse impact". That risks may be managed or minimised has been commonly acknowledged in various jurisdictions that recommend or require privacy risk assessments[1].

IV. The potential unintended consequence of introducing a "no expectation of any adverse impact" condition might be a hard-coding of a high-water mark bright-line test into primary legislation which would prevent the PDPC from subsequently adopting a preferred risk management approach in future regulatory guidance.

V. For risk and impact assessments, the process of conducting DPIAs can be both time and resource intensive. Other jurisdictions have either required or provided guidance that DPIAs should be performed where there is high risk processing[2], that DPIAs are not necessary for every project and

[1] Australia Office of the Australian Information Commissioner's Guide to undertaking privacy impact assessments (May 2014); New Zealand Office of the Privacy Commissioner's Privacy Impact Handbook; Hong Kong Office of the Privacy Commissioner for Personal Data's Privacy Impact Assessment Information Leaflet

[2] Article 35 of the EU General Data Protection Regulation

that organisations should adopt a screening process to determine whether DPIAs are required[3]. Conducting a DPIA in the context of all data processing activity relying on Notification of Purpose may not always be appropriate, resulting in unnecessary burdens being placed on the DPO community and detracting from critical tasks or misdirecting resources.

VI. Given the concerns highlighted above, we would like to suggest that:

a. The consideration of harm or impact should be removed as a pre-condition to the application of Notification of Purpose. Instead, it should be a factor considered under the risk assessment to be conducted by the organization or as part of a standard conducted by an industry driven consortium;

b. The consideration of harm or impact should not be based on "*any*" adverse impact but should be based on a materiality threshold (i.e. material adverse impact to the individual), and again in the context of considering the benefits of the processing and the mitigating measures to address the risks and harms as identified in the risk assessment; and

c. PDPC's clarification in subsequent guidance that flexibility will reside with the DPOs and their organisations to determine whether a DPIA or other non-DPIA assessments are appropriate to identify and manage privacy and data protection risks would be most welcome.

Legal or Business Purpose

I. Given the similarities between Legal or Business Purpose and Notification of Purpose, there exists some degree of uncertainty in the interpretation of Legal or Business Purpose when compared with Notification of Purpose.

II. The distinction between "not desirable or appropriate" and "impracticality" is not clear. Impracticality appears to refer to some form of practical difficulty in implementation. The concept of "appropriateness" may also have considerable overlap with "impracticality" under the Notification Purpose. It would also be inappropriate for the organization (mentioned in the example in paragraph 3.11 of the PDPC paper) to get the consent of individuals given the lack of contact details, and undesirable for the organization to try to get the contact information of the individuals to obtain the consent of the individual.

III. The conditions of "adverse impact" and "benefits to the public (or a section thereof) clearly outweigh[ing] any adverse impact or risks to the individual" are two sides of the same coin. The "adverse impact" condition exists in both the Notification of Purpose and the Legal or Business Purpose legal basis. The only discernable substantive difference between two legal bases is the additional requirement to consider the benefit to the public (limiting the Legal or Business Purpose).

[3] Australia Office of the Australian Information Commissioner's Guide to undertaking privacy impact assessments (May 2014); UK Information Commissioner's Office Code of Practice on Conducting Privacy Impact Assessments (February 2014)

IV. We foresee practical difficulties arising from the requirement for organisations to weigh the "benefits to the public (or a section thereof)" with any adverse impact or risks to the individual. Most organisations are not in the best place to determine what is only beneficial to the public and to subsequently assess whether a *benefit to the public* (as the sole consideration) would outweigh the risks to the individual, as they neither have the data nor resources to quantify the benefit. On the other hand, organisations are best positioned to determine what would be a legitimate purpose in the context of their *own business activities*. We suggest that the weighing test should be one that requires organisations to also consider the benefits to their organisations (in addition to any public interest considerations) versus the adverse impacts or risks to the individual.

V. Given our comments above, we propose for the Legal or Business Purpose to embody the legitimate interests test in other jurisdictions. We believe that there are practical reasons for doing so:

   a. Organisations are familiar (and will be increasingly familiar) with the concept of legitimate interest as a legal basis that already exists in numerous countries (as mentioned above). This familiarity will aid in its application and implementation. Products and services designed in Singapore, and reviewed by the DPO, can then rely on similar legal basis for processing.

   b. Convergence in terms of laws makes for better work by DPOs, having fewer legal variations to manage across jurisdictions. A DPIA could apply legitimate interest as the legal basis in countries where it is already recognized. This has cost savings implications (e.g. obtaining legal advice) as more variances in the guidance for legitimate interests are being developed, and for processing that spans multiple jurisdictions requiring to account for the legitimate interests test.

Mandatory Data Breach Notification

The following comments discuss the direct relationship between notification and addressable harms.

I. The proposed threshold of notifying affected individuals and the PDPC is "any risk of impact or harm". This will result in notification of any data breach regardless of the degree of harm, as all data breaches have a degree of risk of harm (covering a wide range of possible harms including physical, emotional, reputational, psychological, harm to reputation, economic and financial harms.) Instead, the threshold based on assessing that the data breach poses a real or likely risk of serious harm to the affected individuals would be more consistent with notification requirements in other established jurisdictions[4]. Factors that could be considered are whether the organization has or will take steps to mitigate the harm, the identity of recipients of the data, the type and sensitivity of the data involved, the nature of the harm arising from the disclosure of the data.

II. While we agree that NRIC numbers, health information, financial information and passwords are more sensitive data elements, in practice the disclosure of such information may not result in harm to the individual in all cases. It is not always apparent that the data disclosed may be considered as personal

[4] "Real risk of significant harm" under Canada's Personal Information Protection and Electronic Documents Act; and "likely to result in serious harm" under the Privacy Amendment (Notifiable Data Breaches) Act

data. For instance, the disclosure of an account number without more, should not qualify as personal data if the recipients of the account number cannot re-identify an individual. As highlighted by PDPC in its Advisory Guidelines on Key Concepts in the PDPA, whether a certain piece or set of data is personally identifiable will depend on context. The disclosure of an account number (being a string of digits) without more, does not allow the unintended recipient to operate the account or perform fraudulent transactions. Hence, a deeming provision to operate independently of a real or likely risk of serious harm principle will likely give rise to notification of incidents which are of no material consequence to the individual, and which will result in notification fatigue.

III. The inclusion of a numerical threshold of 500 individuals would increase the burden on DPOs and their organisations, and increase the cost of remediating the incident given the need to notify regardless of harm caused. Again, a principle-based approach should be adopted where organisations are required to notify individuals and the PDPC only where the breach poses a real or likely risk of serious harm to the affected individual. For example, an accidental sending by Company A of an email containing a file of personal data of 501 individuals to a small group of recipients in Company B, and which email and file was deleted by the recipients in Company B, and official confirmation of the deletion was provided by Company B to Company A, is unlikely to result in any harm for the individuals.

IV. We welcome the proposed inclusion of exceptions. We would suggest that the technological protection exception remains technology neutral. The specific reference to encryption should be removed as other present-day or future techniques and procedures may also prevent the use of the data. We suggest that an exception should apply where appropriate technological and organizational protection measures are employed such that the data disclosed is rendered unintelligible or usable to any person not authorized to access it. This would allow the breach notification obligation in the PDPA to remain flexible and adaptable to fast-changing developments in technology, and would allow the PDPC to identify in future guidelines technology or techniques (including encryption) that may render information usable. We would also suggest that an additional exception applies where the organization has taken remedial action following a data breach, such that it is unlikely to cause serious harm to the affected individuals[5]. This would address an accidental/unintentional sending of information by an organization to a group of recipients to an unintended recipient, and the organization has obtained official confirmation of the deletion of the information by the recipients, and the recipients have deleted the information. To ensure the effectiveness of the exception and reduce harm to individuals, PDPC may wish to consider adding a corresponding obligation on recipients (individuals and organisations) to delete, upon request by the sending organization, personal information which was unintentionally or accidentally sent to the recipient by the organization or where the recipient was the unintended recipient of the personal information.

V. In a data breach, the focus of the DPO is to identify pertinent facts and to contain the incident[6]. Depending on the complexity of the incident[7], the practical reality is that information may not be

[5] A similar exception appears in Australia's mandatory breach notification regime, and the EU GDPR

[6] This is one of the insights from the Data Breach Management Workshop by AsiaDPO at the PDPC seminar this year. The comments in this section are informed by what we heard from the participants of this workshop.

readily available and the situation may be extremely fluid. We believe that a 72-hour timeframe is not realistic: it adds unnecessary pressure to the incident management team (including DPOs), and diverts time and resources away from the important task of identifying the facts and containing the incident. One study cites the average time to contain a breach (vital for incident management) is about 66 days[8] – during which time, the organization may not have any information to share because of various factors (e.g. the "fog of the breach", the ability of the intruders covering their tracks, etc.). Timeliness of information sharing can be adversely impacted by rigid rule setting, and ignore the complexities of information flows across different systems and boundaries. This runs the risk of perpetuating security risks by forcing organisations to share information prematurely before getting to root causes. A rush to notify has been identified as a factor that increases the per capita cost of data breaches[9]. We would suggest applying a standard of "as soon as practicable" to be consistent with the timeframe adopted for notifying individuals.

VI. We welcome the clarification of the duties of data intermediaries for data breaches, and whether mandatory data breach notification applies equally in view of the Protection Obligation. The discussion above relating to the linking of notification to the likelihood of addressable harms and premature notification requirements would similarly apply to data intermediaries. Data intermediaries may have the added practical difficulty in notifying the organization when it is unable to access the data necessary to identify the occurrence of a breach. For example, where the data intermediary is prohibited under contract from investigating the attributes and characteristics of the data it is processing or hosting for the organization. We suggest applying the same standards of notification that is based on a real or likely risk of serious harm, and "as soon as practicable" to data intermediaries, for the sake of consistency and predictability in incident management practices.

|END OF DOCUMENT|

[7] There is a distinct lack of discourse to account for the cross border management of breach notifications requirements under differing legal standards and business practices even within the framework of the APEC CBPR and PRP systems.

[8] Figure 21, Ponemon Institute, 2017 Cost of Data Breach Study

[9] Figure 9, Ponemon Institute, 2017 Cost of Data Breach Study