SEPTEMBER 29, 2017

PDPC'S PUBLIC CONSULTATION ON APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

SUBMITTED BY:
ISACA SINGAPORE CHAPTER
105 Cecil Street, The Octagon, #06-02E, Singapore 069534.

ISACA
Trust in, and value from, information systems
Singapore Chapter

105 Cecil Street
The Octagon, #06-02E
Singapore 069534

Telephone: +65 6221 8078
Website: www.isaca.org.sg
E-mail:MemberServices@isaca.org.sg

Table of Contents

105 Cecil Street
The Octagon, #06-02E
Singapore 069534

Telephone: +65 6221 8078
Website: www.isaca.org.sg
E-mail:MemberServices@isaca.org.sg

Background

ISACA Singapore Chapter ("ISACA SG") was incorporated in 1983 in Singapore and comes under the governance of the ISACA (USA) global association. It serves professional members of ISACA in Singapore through our education, professional development, networking and outreach programs. There are about 2,200 current members. Our members are professionals from the areas of Governance, Assurance, Risk & Compliance and Cyber Security. ISACA has 4 renowned certifications in Information Security. That is CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information System Control) and CGEIT (Certified in Governance of Enterprise IT). In addition there are 2 frameworks (COBIT and CMMI) and CSX Nexus (technical training on Cybersecurity).

There has been increasing incidents of data breaches affecting organisations. This is a major concern for the organisation as well as for the individuals whose personal details were affected. As part of our outreach efforts to provide ISACA Singapore's members with an opportunity for feedback regarding the proposed changes to the Personal Data Protection Act, ISACA SG held a forum on August 23 2017. It was attended by the local chapter members with representatives from PDPC speaking on the proposed changes followed by a Q & A segment. The feedback below was collated by the Singapore Chapter Board based on the 8 questions outlined in the Public Consultation document.

ISACA
Trust in, and value from, information systems
Singapore Chapter

105 Cecil Street
The Octagon, #06-02E
Singapore 069534

Telephone: +65 6221 8078
Website: www.isaca.org.sg
E-mail:MemberServices@isaca.org.sg

1. Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?

The schedules below in the Act specify the situations where consent for collection, use and disclosure of personal data is not required.

- Second Schedule – Collection of personal data without consent
- Third Schedule – Use of personal data without consent
- Fourth Schedule – Disclosure of personal data without consent

Consent is not required in the circumstances and subject to any conditions in the 3 schedules above.

Feedback:
Notification of purpose may be a relaxion of the requirement to obtaining consent. More clarity could be worded in the Act regarding the areas below.

Clarifications:

A) In the situation where after evaluating the conditions in the 2nd, 3rd and 4th schedules and concluding that consent is not required. Would notification of purpose be required?
B) Would the changes proposed for "Notification of Purpose" be applied to Section 13 of PDPA or it would be applied in addition to Section 13 of PDPA?
C) What is the definition of an "organisation" in the context of the Act.
D) "Adverse impact" is subjective and broad. It may take on different meaning when applied to the organisation and the individual. Guidance on the definition of an "adverse impact" should be provided.
E) Would there be an advisory guideline on the Data Protection Impact Assessment (DPIA)?

ISACA
Trust in, and value from, information systems
Singapore Chapter

105 Cecil Street
The Octagon, #06-02E
Singapore 069534

Telephone: +65 6221 8078
Website: www.isaca.org.sg
E-mail:MemberServices@isaca.org.sg

2. Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., impractical to obtain consent and not expected to have any adverse impact on the individual)?

Feedback:
The condition expresses, on a high level, the expectation of PDPC on the organization and frames the context for individuals. Notification should not be subjected to conditions as these are personal information of the individuals. Individuals should be entitled to and clearly understand what information is being collected, its intended use and how it will be shared. There should be more clarity on the areas below.

Clarifications:

A) Are the proposed conditions applied to Section 13 of PDPA or it would be applied on top of the conditions in the 2nd, 3rd and 4th schedules?

B) Define "organisation".

C) As "adverse impact" is subjective to the organisation and the individual. **What defines "adverse impact"?**

D) A requirement for entities to perform a risk and impact assessment prior to relying on the Notification of Purpose, as proposed by the Commission, is both, practical and reasonable. That said, we note that the Commission has not set out what risk and impact assessments/data protection impact assessments would entail, and we would appreciate it if the Commission could provide some guidance in this regard. **Would there be an advisory guideline on the Data Protection Impact Assessment (DPIA)?**

E) In addition, we would also like to clarify if organizations may **leverage risk and impact assessments/data protection impact assessments conducted in other jurisdictions for purposes of relying on the Notification of Purpose basis for collecting, using and disclosing personal data?**

ISACA
Trust in, and value from, information systems
Singapore Chapter

105 Cecil Street
The Octagon, #06-02E
Singapore 069534

Telephone: +65 6221 8078
Website: www.isaca.org.sg
E-mail:MemberServices@isaca.org.sg

3. Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?

Feedback:
The basis for collecting, using and disclosing personal data without consent and notification really depends on the circumstances. Per point 3.13 of the consultation paper, the reasonable balance requires definition, guideline and documented reasoning behind the self-evaluation for the final decision on why the collection, use and disclosure of personal data was performed without consent and notification. Self-evaluation can be subjective and may lean into biasness due to corporate self-interests / advantages. Below are some questions that can be addressed by the proposed changes.

Clarifications:
A) Define "not desirable or appropriate to obtain consent" as this is subjective.
B) Would this requirement have any impact to the Singapore Employment Act? What if results of an investigation following this exemption to collect, use and disclose without consent and notification lead to termination of employment relationship?

ISACA
Trust in, and value from, information systems
Singapore Chapter

105 Cecil Street
The Octagon, #06-02E
Singapore 069534

Telephone: +65 6221 8078
Website: www.isaca.org.sg
E-mail:MemberServices@isaca.org.sg

4. Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?

Feedback:
The condition expresses, at a high level, the expectation of PDPC on the organization. However, guidance needs to be defined clearly, with sufficient and specific examples, to lead organization's thought process. This is so that a reasonable balance between the organization and the rights of an individual / employee can be achieved. Guidance should include PDPC expectation of organization in the areas of accountability of decision to proceed without notification and consent as well as documentation of any approval requirements for decisions made.

Clarifications:

A) Define "benefits to the public".

B) As "adverse impact" is subjective to the organisation and the individual. What defines "adverse impact"?

C) Similar to comments under Q2, a requirement for entities to perform a risk and impact assessment prior to relying on the Notification of Purpose, as proposed by the Commission, is both, practical and reasonable. That said, we note that the Commission has not set out what risk and impact assessments/data protection impact assessments would entail, and we would appreciate it if the Commission could provide some guidance in this regard. In addition, we would also like to clarify **if organizations may leverage risk and impact assessments/data protection impact assessments conducted in other jurisdictions for purposes of relying on the Notification of Purpose basis for collecting, using and disclosing personal data.**

D) Would there be advisory guideline on the Data Protection Impact Assessment (DPIA) for this proposed exemption?

105 Cecil Street
The Octagon, #06-02E
Singapore 069534

Telephone: +65 6221 8078
Website: www.isaca.org.sg
E-mail:MemberServices@isaca.org.sg

5. What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? Specifically, what are your views on the proposed number of affected individuals (i.e., 500 or more) for a data breach to be considered of a significant scale to be notified to PDPC?

Feedback:

- The requirement to notify data breach notification to affected individuals is reasonable given the opportunity to take steps to protect themselves from the risks or impact from the data breach. This requirement should include key considerations for individuals to note upon being notified of the breach and expectations of the situation to closure.

- The notification to PDPC by affected organizations should carry more purpose than:
    - Receiving guidance from PDPC on post-breach remedial actions
    - Better oversee the level of incidences and management of data breach at the national level.

  This is especially so for reporting to PDPC where there is no risk of impact or harm to affected individuals.

- There be consideration of sharing the intelligence gathered from PDPC oversight on incidences and management of data breach at the national level for the benefit of organizations looking to improve their controls.

- Significant scale is subjective and should not be fixed to a number. There should be no minimum number for a data breach to be an incident to be reported. For example, the requirement under paragraph 6.2b) of the Consultation Paper of 500 or more individuals may not be applicable in the context of large global companies which deals with millions of records. 500 records may be too low for global MNCs. It is hard to quantify the number as data may be stored offshore and in multiple locations. If the minimum number is set then there must be more thought as 500 may be too high for some and low for others.

- With multiple requirements from different jurisdiction to report data breaches, PDPC should consider streamlining scenarios to PDPC's mandatory data breach notification to those already required in the industry e.g. GDPR.

Clarifications:

A) Define "impact and harm to affect individuals" as the term is subjective to organization and individuals.
B) Define "individuals" i.e. Singapore residents, Singapore registered businesses?
C) Are there any expectations from the organization by PDPC when there is a breach with no risk of impact or harm to affected individuals but of a significant scale?

ISACA
Trust in, and value from, information systems
Singapore Chapter

105 Cecil Street
The Octagon, #06-02E
Singapore 069534

Telephone: +65 6221 8078
Website: www.isaca.org.sg
E-mail:MemberServices@isaca.org.sg

6. What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?

Feedback:

- With multiple requirements from different jurisdiction to report data breaches, PDPC should consider harmonizing PDPC data breach reporting and format to those already used in the industry e.g. GDPR or MAS TRM Notice.

- Consider working with sectorial regulators as deputy commissioner, like that proposed in the CSA Cyber Security Bill. To which, an organization's point of contact is kept to one and regulatory bodies work together on the backend.

Clarifications:

- Certain regulator may require reporting in parts e.g. interim and final submissions. Would PDPC require organizations to include PDPC in both the interim and final submissions?

- Should a separate reporting process be decided by PDPC, would a template for reporting be provided?

ISACA
Trust in, and value from, information systems
Singapore Chapter

105 Cecil Street
The Octagon, #06-02E
Singapore 069534

Telephone: +65 6221 8078
Website: www.isaca.org.sg
E-mail:MemberServices@isaca.org.sg

7. What are your views on the proposed exceptions and exemptions from the data breach notification requirements?

Feedback:

- The exclusion under Section 6.10b of the public consultation paper regarding the proposed breach notification provision is reasonable.
- The exception proposed in Section 6.10 of the public consultation paper is reasonable.

Clarifications:

- Define and gives examples of “technological protection exception”.
- Define “reasonable standard” for encryption of breached personal data.
- Would the same explanation under footnote 42 on EU GDPR “implemented appropriate technological and organisational protection measures and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it” be applicable to this exemption?
- Is it a requirement for breach that falls within the technological protection exception be reported as a significant scale reporting requirement to PDPC? Should the exception apply to personal data that is already publicly available?

ISACA
Trust in, and value from, information systems
Singapore Chapter

105 Cecil Street
The Octagon, #06-02E
Singapore 069534

Telephone: +65 6221 8078
Website: www.isaca.org.sg
E-mail:MemberServices@isaca.org.sg

8. What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?

Feedback:

- 72 hours seems reasonable provided interim reporting based on available information at the point of discovery is considered acceptable by PDPC.

- With multiple requirements from different jurisdiction to report data breaches, PDPC should consider harmonizing PDPC data breach notification reporting and format to those already used in the industry e.g. GDPR or MAS TRM Notice.

- Consider working with sectorial regulators as deputy commissioner, like that proposed in the CSA Cyber Security Bill. To which, an organization's point of contact is kept to one and regulatory bodies work together on the backend.

Clarifications:

- Should reporting happen at the time of the breach or at the point of breach discovery?
- The proposed 72 hours is just for PDPC? Or it includes individuals as well?
- What would be the requirement if there is an unknown source of breach, both to PDPC and to the individuals? Would the Act have some provision to these new sources of threats that have not be considered?

105 Cecil Street
The Octagon, #06-02E
Singapore 069534

Telephone: +65 6221 8078
Website: www.isaca.org.sg
E-mail:MemberServices@isaca.org.sg

Conclusion

The proposed amendments to the PDPA is a step in the right direction. There will be more threats that may lead to data breaches as we are moving towards a "SMART" digital economy. The interconnectedness of our systems and technology innovation will create opportunities but may expose gaps that can be exploited. The Act is not prescriptive but rather the onus is on data owners to secure their data.

Another note is the legacy use of NRIC. This is an important part of the individual identity together with other attributes such as date of birth, credit and contact information. Most organisations uses data intermediaries (DI) to collect, process and store their data. Perhaps the PDPC can consider a form of "licensing" for the DI to ensure that they have the required processes and systems to protect their customers' data.

Lastly a minimum number of breach records should not be specified before it becomes a reporting requirement such as greater than 50 or 500. Most records are stored electronically in a database. When the records are breached the perpetrator has access to all records. It is not prudent to specify a minimum number. Visibility is important to the regulator. There could be differing levels of penalties depending on the scale of the breach. Even if the breach is small this time, it serves as an opportunity for organisations to improve their processes which may prevent a major breach down the line.