Response to the PDPC's Public Consultation on Approaches to Managing Personal Data in the Digital Economy

submitted by the Asia Cloud Computing Association (ACCA)

21 September 2017

Contact:
Ms Lim May-Ann
Executive Director
Asia Cloud Computing Association
Email: mayann@asiacloudcomputing.org
Phone: +65 9847 1950

The Asia Cloud Computing Association (ACCA) is the apex industry association in Asia Pacific that represents stakeholders of the Cloud Computing ecosystem to government and other stakeholders. Our mission is to accelerate the adoption of Cloud computing through Asia Pacific by helping to create a trusted and compelling market environment, and a safe and consistent regulatory environment for Cloud computing products and services. We are committed to strengthening the cybersecurity resilience and developing a robust technology ecosystem which supports a vibrant digital economy.

Personal Data Protection Commission
460 Alexandra Road #10-02
PSA Building
Singapore 119963

Submitted via: corporate@pdpc.gov.sg

21 September 2017

Dear Sir/Madam,

Re: Asia Cloud Computing Association's (ACCA) Response to the PDPC's Public Consultation on Approaches to Managing Personal Data in the Digital Economy

The Asia Cloud Computing Association (ACCA) thanks the Personal Data Protection Commission (PDPC) for the opportunity to provide comments on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy (consultation paper). We commend the PDPC in reviewing the PDPA Act to ensure it remains flexible, agile and relevant in view of technological advances and global developments.

In consultations with our members, we put forth the following comments on the consultation paper.

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

ACCA supports the inclusion of the Notification of Purpose basis for collecting, using and disclosing personal data without consent. We agree with the reasons set out by PDPC in the consultation paper.

Question 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)?

The Notification of Purpose approach should not be subject to conditions.

The legislative framework needs to be precise and unambiguous. Organizations will require greater clarity on what is sufficient to meet the "impractical" or "not expected to have an adverse impact" standards. As it is unclear under what circumstances an organization would be able to meet the proposed conditions, this would hinder reliance on the Notification of Purpose approach.

ACCA notes that imposing conditions on the Notification of Purpose approach does not achieve the outcome of strengthening provisions for parallel bases for collecting, using and disclosing personal data under the PDPA.

ACCA recommends that organizations should be able to rely on the Notification of Purpose, provided that they have conducted a risk and impact assessment (as per paragraph 3.10 of the consultation paper). We agree that organizations should put in place measures to mitigate the risks when relying on the Notification of Purpose to collect, use or disclose personal data.

ACCA commends the PDPC for not prescribing the nature of the risk and impact assessment. This enables organizations to rely on other risk analysis (i.e. global regimes) to meet PDPA's

requirements. This approach ensures the flexibility and agility required to encourage innovation and growth.

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

ACCA supports the inclusion of the Legal or Business Purpose as a basis for collecting, using and disclosing personal data for the reasons set out by the PDPC in the consultation paper.

Question 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)?

The Legal or Business Purpose approach should not be subject to conditions.

As highlighted above in our response to Question 2, conditions create ambiguity. It is unclear what circumstances would fall within the proposed conditions. Organizations would need further clarification and guidance on what is sufficient to meet the "not desirable or appropriate to obtain consent" standard.

ACCA commends the PDPC for looking to industry best practice and global standards, such as the EU General Data Protection Regulation (GDPR). However, we note that the GDPR "legitimate interests" provision is not subject to conditions.

ACCA recommends that organizations should be able to rely on the Legal and Business approach, provided that they have conducted a risk and impact assessment (as per paragraph 3.17 of the consultation paper). This is an appropriate measure in safeguarding the rights of individuals.

Requiring organisations to conduct a risk and impact assessment, ensures the Notification of Purpose approach and the Legal and Business purpose approach are aligned. ACCA recommends uniformity in approach across the PDPA Act as the responsibility of organisations are clearly defined.

Question 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?

ACCA and our members take the obligation to make reasonable security arrangements to protect personal data in their possession or under their control seriously (as per paragraph 4.1 of the consultation paper).

ACCA notes that the PDPC proposes to adopt the following criteria for data breach notification (as per paragraph 6.2 of the consultation paper):

a) Notification to affected individuals and PDPC of a data breach that poses any risk of impact of harm to the affected individuals;

b) Notification to PDPC where the scale of the breach is significant.

Notification to affected individuals and PDPC should not be required when there is only *risk* of impact or harm to affected individuals.

To require notification of a data breach that poses any risk of impact or harm to affected individuals would increase the risk of individuals, organisations and PDPC experiencing "notification fatigue". This may have the unintended consequence of individuals or organisations failing to take the necessary steps to protect themselves.

ACCA recommends that notification to individuals and PDPC only be required when the data breach reaches the threshold of actual serious and material harm to individuals or organisations.

Question 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?

Notification under other laws and sectoral regulations should be sufficient. Organisations should not be required to notify under multiple legal regimes. Concurrent notification to PDPC by organisations is an unnecessary administrative burden and does not provide any further protection for individuals.

ACCA recommends it is sufficient for notification to be made only to the sectorial or law enforcement agency.

Obligations of Data Intermediary

ACCA is pleased that as per paragraphs 6.6 – 6.8 of the consultation paper, the PDPC intends to make it clear that the responsibility for complying with data breach notification requirements rests predominantly with the organisation (or data controller), rather than the data intermediary (or data processor).

Customers (i.e. the organization who is using the data intermediary) maintain control of personal data when using a cloud service. Therefore, the organization is responsible for data breaches and notifying affected individuals and regulators such as the PDPC.

However, ACCA disagrees with the proposed statutory requirement imposed on data intermediaries. The requirement to notify a data breach and the timeframe for such notification should be determined by industry best practice and contractual agreements between the organization and data intermediary. This is preferable to a prescriptive legal framework that discourages and stifles innovation and growth, and is incompatible with the pace of technological advances.

If such an obligation is to be prescribed by PDPC, ACCA recommends that data intermediaries be required to notify the organisation "as soon as practicable and without undue delay" and only where the data intermediary has actual knowledge of the breach.

Data intermediaries should not be required to inform the organisation "immediately" (as per the proposed requirement in paragraph 6.6 of the consultation paper). This is an impractical requirement as it takes time for the data intermediary to determine what happened and which customers may have been affected by an incident.

Further, data intermediaries should not be held liable to provide timely notification to an organization where they are contractually limited from accessing data to the extent necessary to identify a breach.

Cloud service providers (or data intermediaries) perform a role similar to that of a data processor and do not have visibility or knowledge of the organizations' data that it processes. Data intermediaries are contractually prohibited from investigating the attributes and characteristics of data that an organization uploads to the cloud service.

ACCA encourages the PDPC to have a single notification timeframe across the PDPA Act. We recommended the timeframe of "as soon as practicable and without undue delay" in our response to Question 8 below. Uniformity across the PDPA Act ensures clarity for organisations and their responsibilities.

Requiring a data intermediary to notify customers "without undue delay", is also in line with internationals standards such as Article 33(2) of the GDPR.

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

ACCA supports the proposed exceptions and exemptions from the data breach notification requirements.

In our response to Questions 5 above, ACCA recommended that notification to individuals and PDPC only be required when the data breach reaches the threshold of actual serious and material harm to individuals or organisations.

In line with this recommendation, we further recommend an additional exception that covers an organization that conducted a risk and impact assessment and determined that the risk of harm was low to affected individuals or organisations. This introduces a reasonableness standard.

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

ACCA encourages the PDPC to have a single notification timeframe across the PDPA Act, applicable to all notifications made to affected individuals and the PDPC. Uniformity across the PDPA Act will provide clarity for organisations and increase compliance. This is preferable to multiple timeframes which results in ambiguity and an impact on resources for organisations.

ACCA recommends that the timeframe for notification to all affected individuals and to the PDPC be "as soon as practicable and without undue delay".

Having a single timeframe is preferable, rather than requiring notification to the PDPC within a specific number of hours (such as 72 hours as per paragraph 6.13 of the consultation paper).

If a notice obligation that references a specific number of hours is to be prescribed by PDPC, it should be clear that the obligation is only:

a) applicable to the organisation that originally collected the personal data (as compared to a service provider or data intermediary of that collecting organization); and
b) triggered when that entity has actual knowledge of the breach.

As per our response to the proposed obligations on data intermediaries above (in reference to paragraphs 6.6 – 6.8 of the consultation paper), we recommended that the timeframe should not be

imposed on service providers (data intermediaries). ACCA recommends that data intermediaries be required to notify the organisation "as soon as practicable and without undue delay" and only where the data intermediary has actual knowledge of the breach.

Conclusion

ACCA supports measures that reduce ambiguity for organizations, including:

- implementing the Notification for Purpose approach and the Legal and Business Approach without imposing conditions
- simplifying the legal framework by ensuring a single notification timeframe (for organizations and data intermediaries)
- clarifying the role of organizations and data intermediaries.

We look forward to working with you to craft policy which will continue to safeguard the rights of individuals, while supporting innovation and business vibrancy in Singapore.

I would be happy to speak further with the PDPC on any of these items, or host a vendor-neutral discussion between the PDPC and other members of the industry from the ACCA to provide feedback. Please feel free to contact me if this is of interest.

I look forward to hearing from you, and welcome your response on the issues raised above.

Yours Sincerely,

Lim May-Ann
Executive Director
Asia Cloud Computing Association