6 September 2017

Personal Data Protection Commission
460 Alexandra Road #10-02 PSA Building
Singapore 119963
Email: corporate@pdpc.gov.sg

Dear Sir/Madam

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

Salesforce is pleased to make this submission to *PDPC's Public Consultation for approaches to managing personal data in the digital economy.*

About Salesforce

Salesforce is a provider of software as a service ("SaaS") and platform as a service ("PaaS") offerings. Customer trust is our number one value. Our success depends on delivery reliable services to our customers in Singapore, and around the globe.

Salesforce formed in 1999, is a pioneer of cloud computing – and has been operating in Singapore since 2004. The company was founded with a vision to create a new kind of enterprise software company, with a new technology model based in the cloud, a new pay-as-you-go business model, and is considered a global leader in Customer Relationship Management (CRM).

According to an IDC report commissioned by Salesforce, through our ecosystem of customers, partners and developers we expect to create over Salesforce's cloud technology 3,076 direct new jobs in 2017 with a further 5,821 indirect jobs in 2017 in Singapore. In terms of business revenue in Singapore, the revenue from the use of cloud computing is expected to be $739 million in 2017 and is forecasted to contribute $1.2 billion by 2020.

Salesforce & Privacy

Salesforce is committed to protecting the privacy of our customers. Salesforce has been awarded TRUSTe's Privacy Seal signifying that this Privacy Statement and associated practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements including transparency, accountability, and choice regarding the collection and use of your personal information.

PDPC Consultation

Salesforce has endeavored to respond to the specific questions raised by the PDPC:

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

Yes, the PDPA should provide for "Notification of Purpose" as a basis for collecting, using and disclosing personal data without consent for the many reasons the PDPC has stated above.

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)?

No, the "Notification of Purpose" approach should not be subject to conditions. Organizations should be able to rely on the "Notification of Purpose" at their discretion. For example, the organization may have also conducted a risk and impact assessment and/or put in place measures to mitigate the risks when relying on Notification of Purpose to collect, use or disclose personal data that can mitigate risk. Conditions around the "Notification of Purpose" can create ambiguity and can hinder reliance on the "Notification of Purpose" approach in the event an organization is unclear on what is sufficient to meet the "impractical" or "not expected to have adverse impact" standards. These conditions are subjective, and may result in uneven application of the conditions. Accordingly, relying on companies to, for example, conduct a risk and impact assessment instead would enable more adoption of this approach. This also enables entities to harmonize their privacy programs, including by addressing PDPA's requirements through security and privacy frameworks in place for global compliance purposes.

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?

Yes

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)?

Conditions are acceptable but not required. The proposed conditions are sound, but organizations would need further clarification and guidance about what would fall within those conditions. For example, what does it mean for it to be *"not desirable or appropriate to obtain consent."*

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?

Notification to PDPC should only be required in very limited circumstances: notice should not be required when there is only *risk* of impact or harm to individuals, but instead notice to PDPC should only be required if there is actual serious and material harm to individuals or organizations and where the breach is significant.

Material harm to consumers and individuals could mean, for example, personal information paired with bank information, credit card, or government issued identification that could be used for identity theft.

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?

Notice under other laws and sectoral regulations should be sufficient, an entity should not be required to notify under multiple legal regimes.

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

The exceptions are helpful, and an additional exception should be added that covers a situation where the entity that experienced the breach makes a determination that risk of harm is low and notice need

not be provided given that an individual has not been impacted adversely. This introduces a reasonableness standard.

Furthermore, when a breach involves a contractor, the principal, rather than the contractor should make the disclosure to the data subject. For example, if Company A uses a third party contractor to store personal information about Company A's customer and the contractor has a breach, Company A should notify its customers (who may be the data subject or may have to then notify the impacted data subject). If Company A is not the data subject itself, then it would be the entity that has the relationship with the data subject, and would be best situated to communicate with the data subject.

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

Notice obligations, if triggered, should only be "As soon as practicable and without undue delay." To the extent a notice obligation is imposed that references a specific number of hours, it would need to be clear that (1) the obligation is only applicable to the entity that originally collected the personal data (as compared to a service provider of that collecting entity), (2) the obligation is only triggered when that entity has actual knowledge of the breach, and (3) such a time frame should not be imposed on service provider entities, who should simply be obligated to notify " as soon as practicable and without undue delay." When a breach involves multiple entities, each entity should be given reasonable time to notify. For example the contractor may be required to promptly notify the principal, which could then be required to promptly notify affected data subjects.

Furthermore, there needs to be flexibility around communication type/form, specific requirements may impede parties' ability to provide notification quickly. To this end Salesforce supports provisions that allows entities notifying affected parties using whatever channels they normally use to contacts those entities.

Should you require further information regarding this submission, please feel free to contact me at sgrigorian@salesforce.com

Yours sincerely

Sassoon Grigorian
Head of Public Policy ANZ & South East Asia


salesforce