28 May 2020

Ministry of Communications and Information
140 Hill Street #01-01A, Old Hill Street Police Station
Singapore 179369

Personal Data Protection Commission
10 Pasir Panjang Road, #03-01 Mapletree Business City
Singapore 117438

Email: DataRegulation@mci.gov.sg
cc Email: YEONG_Zee_Kin@pdpc.gov.sg

Dear sir/madam,

RE: PUBLIC CONSULTATION FOR THE PDP (AMENDMENT) BILL

Salesforce[1] commends the Ministry of Communications and Information (MCI) and the Personal Data Protection Commission (PDPC) on the ***Singapore Personal Data Protection (Amendment) Bill*** (PDP Bill) public consultation, and appreciates the need to further strengthen Singapore's data protection enforcement and implementation.

Attached is a list of Salesforce's suggestions to the proposed PDP Bill for your easy reference, review, and kind consideration. Please do not hesitate to reach out to me by email at bmok@salesforce.com or by mobile phone at +65 9067 2189 should you and / or your team have further questions. Salesforce would be pleased to discuss further with MCI / PDPC in person.

Once again thank you so much for the opportunity to provide input.

Your faithfully

Boon Poh MOK
Head of Government Affairs & Public Policy
Southeast Asia & Greater China Regions

[1] Salesforce is the global leader in Customer Relationship Management (CRM), bringing companies closer to their customers in the digital age. Founded in 1999, Salesforce enables companies of every size and industry to take advantage of powerful technologies—cloud, mobile, social, internet of things, artificial intelligence, voice and blockchain—to create a 360° view of their customers. For more information about Salesforce (NYSE: CRM), visit: www.salesforce.com.

5 Temasek Boulevard
#13-01, Suntec Tower Five
Singapore 038985
salesforce.com
/salesforce
@salesforce

Amendment of Section 2(1)

*"**derived personal data**"*

*(a) means personal data about an individual that is **derived** by an organisation in the course of business from other personal data about the individual or another individual in the possession or under the control of the organisation; but*

*(b) does not include personal data **derived** by the organisation using any prescribed means or method;*

*"**user activity data**", in relation to an organisation, means personal data about an individual that is **created** in the course or as a result of the individual's use of any product or service provided by the organisation;*

Salesforce's input:

The word "**created**" covers too broadly under the definition of "user activity data", which could potentially overlap with the definition of "**derived** personal data" and cause confusion.

Salesforce suggests narrowing and simplifying both definitions to ensure clear exclusivity between "derived personal data" and "user activity data".

Amendment of section 21

(3A) Subsection (3)(c) and (d) does not apply to any user activity data about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual.

Salesforce's input:

The intention of the proposed amendment is unclear whether it is meant to exclude user-provided data and user activity data from the exception, even if it contains information about a third-party individual? If so, it would be a concern because organizations often do not know whether an individual has the right to provide third-party information.

In case the organization has to "return" this data to the individual that had provided the data, the potential breach of the third-party individual's privacy would only be perpetuated. Furthermore, the information that was provided to the organization by the individual is likely to be complemented with other information regarding this third person.

It is not feasible to 'split' a data set and only provide the information that was initially received. In addition, providing data relating to a third-party individual with respect to user activity data could potentially cause damage to the third-party individual's privacy and result in substantial negative impact. For example, this would mean that a spouse can obtain the 'web surfing behaviour' of the other spouse.

Salesforce suggests that Article 3(A) to be repealed.

5 Temasek Boulevard
#13-01, Suntec Tower Five
Singapore 038985
salesforce.com
/salesforce
@salesforce

Amendment to Section 26D

(1) Where an organisation assesses, in accordance with section 26C, that a data breach is a notifiable data breach, the organisation must notify the Commission as soon as is practicable, but in any case, no later than 3 days after the day the organisation makes that assessment.

Salesforce's input:

A 'honey pot' for malicious actors can happen in case the incident becomes public while the organisation has not been able to resolve the root cause within the three-day notification period.

Salesforce suggests including a provision to mandate notification be kept confidential to protect the data from further breaches.

(3) The notification under subsection (1) or (2) must —
(a) contain all the information that is prescribed for this purpose; and
(b) be made in the form and submitted in the manner required by the Commission.

Salesforce's input:

Salesforce suggests adding the following after the word "purpose" in Section 26D(3)(a): "to the extent the organisation has reasonable access to the information."

Data Privacy Rules, such as GDPR, allow for a staged notification, i.e., a first notification can be made containing the information known at that time, and after further investigation, a follow-up notification can be submitted with additional detail once they are available and can be shared without causing any additional security risks.

Amendment to Section 26G

(2) Subject to subsections (3), (5) and (6), the porting organisation must, upon receiving the data porting request, transmit the applicable data specified in the data porting request to the receiving organisation in accordance with any requirements prescribed.

Salesforce's input:

Salesforce strongly suggested that the time and scope of this provision should be limited. In the EU, several abuses under such EU GDPR's provision occurred in the past when individuals submitted multiple onerous requests within a short timeframe that created operations burden that negatively impacted businesses. It is very costly to respond to such a request, especially given the rather broad scope of this right, and this right should thus be limited "with reasonable intervals."

(3) Subsection (2) applies only if the following are satisfied:
(a) the data porting request satisfies any requirements prescribed;
(b) the porting organisation, at the time it receives the data porting request, has an ongoing relationship with the individual.

Salesforce's input:

Salesforce suggests following the GDPR's portability provision because a broad data portability right proposed in this amendment could be problematic for various reasons. For example, it could lead to an organization exposing Intellectual Property / confidential information, as well as third-party individual's information in case the data was provided by a third-party individual.

Organizations are usually unable to identify a particular individual in its user activity data sets. They may not know the individual's IP address and thus would not be able to distil the individual's data out of the larger data set. Even if this is possible, it could expose confidential information related to other individuals which could have grave consequences.

For example, if an organization is using an IP address, they are unable to identify who else is using the same IP address. If the organization provides the individual with a list of all user activities related to the said IP address, then they are likely to expose third-party confidential and sensitive information.

GPPR and some other laws restrict the right to data portability to data provided by the individual to the organization and such right does thus not cover generated / user activity data, or data provided by third parties.

(6) A porting organisation must not transmit any applicable data about an individual under subsection (2) if —
(a) the transmission of the applicable data can reasonably be expected to —
(i) threaten the safety, or physical or mental health, of an individual other than the individual to whom the applicable data relates;
(ii) cause immediate or grave harm to the safety, or physical or mental health, of the individual to whom the applicable data relates; or
(iii) be contrary to the national interest;

Salesforce's input:

Salesforce suggests adding the following clause after 6(a)(iii): "(iv) cause a breach of the organisation's or a third-party's intellectual property rights or confidential information."

Amendment to Section 26H

(2) A porting organisation may disclose personal data about T to a receiving organisation without T's consent only if the data porting request —
(a) is made in P's personal or domestic capacity; and
(b) relates to P's user activity data or user-provided data.

Salesforce's input:

Similar to Salesforce's input for Amendment to Section 26G(6), this could cause a serious breach of the third-person's privacy. For example, this would mean that a spouse of an individual may obtain the "web surfing behaviour" of the spouse of another individual.

Salesforce suggests adding the following clause after 2(b): "(c) cause a breach of the organisation's or a third-party's intellectual property rights or confidential information."

Amendment to Section 35B

(1) If
(c) the individual does so —
(i) knowing that the disclosure is not authorised by the organisation or public agency, as the case may be; or
(ii) reckless as to whether the disclosure is or is not authorised by the organisation or public agency, as the case may be, the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both.

Salesforce's input:

An employee of an organization cannot always be expected to assess whether or not a disclosure is authorized. If their employer orders them to share data, the individual should not be held liable for simply doing their job as instructed by their employer which is expected to only give instructions that are in line with applicable law, unless it should be obvious to the employee that the latter is not the case. This applies to all similar sections related to offence throughout the PDPA.

Salesforce suggests that organisation's and employee's penalty clauses to be clearly and narrowly defined based on the respective obligations under the PDPA. An employee should only be penalised if, and only if, the disclosure is done intentionally by the employee without authorisation from the organisation or public agency.

***