Public Consultation for Approaches to Managing Personal Data in the Digital Economy

Jul-Sep 2017

Macquarie Response

We welcome the efforts by the Personal Data Protection Commission (***PDPC***) in issuing this consultation paper to review the Personal Data Protection Act (***PDPA***). Macquarie appreciates the opportunity to provide comments on the proposals, specifically in relation to question five, which we set out on the next two pages.

As background, Macquarie Group Limited is a global diversified financial group. It acts primarily as an investment intermediary for institutional, corporate and retail clients and counterparties around the world. We have a strong Asian presence, with 14 offices across 10 countries, including Singapore.

Should you have any questions or wish to discuss our submission, please contact:

Peggy Si
Peggy.Si@macquarie.com
+852 3922 3316

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?*

As drafted, the proposal for breach notification requires notification to regulator and individuals if breach poses "any risk of impact or harm". We note that other markets have imposed much higher thresholds for breach notification. For example:

1. Under the *EU General Data Protection Regulation* (effective, 25 May 2018), notification is only required to individuals when there is "a **high risk** to the rights and freedoms of natural persons"; and
2. Under the *Australian Privacy Act 1988*, as amended by the *Privacy Amendment (Notification Data Breaches) Act 2017* (effective, 22 February 2018), notification is required where the relevant unauthorised loss, access or disclosure would be likely "to result in **serious harm** to any of the individuals".

Given the likelihood of data breaches to traverse multiple jurisdictions, we would recommend that PDPC align the Singapore requirements to these market standards.

In addition, we feel that a low reporting threshold encourages overly conservative reporting, may create an inconsistent standard for international organisations, and can discourage them to operate or be based in Singapore. These include:

- Singapore-based international organisations that regularly process personal data for entities outside Singapore (such as outsourced service providers, call centres); or
- Singapore-based online businesses offering goods and services on a global basis (such as online businesses offering goods and services or monitoring the behaviour of data subjects in the EU[1] or businesses with an 'Australian link'[2]).

We also do not consider the proposed number of 500 affected individuals to be a suitable measure of significance as we consider that the type of breach and the specifics of the information concerned should also be substantive considerations. As such, we feel that the determination on severity of a breach should be done in accordance with similar principles as stipulated in the EU or Australian legislations noted above.

We set out below the hyperlinked sources of the abovementioned provisions.

1. EU regulations 2016/679 (GDPR)

   Article 33(1) (notification to regulator):

   "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural

[1] See Article 3 of the *GDPR* dealing with Territorial scope of the *GDPR*.
[2] See Section 5B of the *Privacy Act 1988*, dealing with the Extra-territorial operation of the Act.

persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

Article 34(1) (notification to the data subject):

"When the personal data breach is likely to result in a **high** risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. 4.5.2016 L 119/52 Official Journal of the European Union EN"

2. Privacy Amendment (Notification Data Breaches) Act 2017

Section 26WE

"….assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in **serious** harm to any of the individuals to whom the information relates;"

Section 26WG then goes on to discuss the relevant factors to be considered in determining the above.