Swiss Re

Damen How
Compliance Officer

Personal Data Protection Commission
(PDPC) Singapore

Swiss Reinsurance Company Ltd
Singapore Branch
12 Marina View #16-01
Asia Square Tower 2
Singapore 018961
damen_how@swissre.com

Your Reference Public consultation issued on 27 July 2017
Our Reference S0DH5V

September 15, 2017

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

Dear Sir or Madam

We refer to the above subject matter relating to PDPC's Public Consultation on Approaches to Managing Personal Data in the Digital Economy issued on 27 July 2017.

We would like to provide our comments as follow:

With regards to the proposed enhanced framework for the collection, use and disclosure of personal data framework, we would appreciate if there are more clarity and guidance on the following:

- Decisions that might be taken to not obtain consent ie, what are the expectations for documenting such decisions so that this documentation can be used to demonstrate compliance?
- The definition of "impractical", "adverse impact or risks", "benefits to the public".
- Who should conduct the risk and impact assessment? Is it the data controller or data processor or data intermediary or all? Will it be self-assessment and done by third party?
- The scope and extent of the risk and impact assessment.

With regards to the mandatory data breach notification framework, we would appreciate if there are more clarity and guidance on the following:

- The definition of "risk of impact or harm".

- Whether the threshold of 500 individuals consists of (1) those individuals from Singapore only or (2) individuals from countries where the group entity operates.

In addition, we would also like to comment that definitions are needed for what constitutes a notifiable breach. If there isn't a clear threshold (e.g. on number of impacted individuals or severity of damage) it would lead to the notification of hundreds if not thousands of breaches by each organization. The loss of one personal record or one email that was sent to the wrong recipient with an attachment might be a breach of the law but if the damage is limited or the email was recovered and no impact to the affected individuals can be expected, notifying it within 72 hours would not be necessary.

Notifying unqualified breaches would actually have a contrary effect to what the notification is supposed to achieve. Notifications should be one measure that should lead to better protection (e.g. alerting individuals that they should change their passwords) and to prevent further harm (e.g. investigating or prosecuting the attacker via government authorities and alerting individuals so that they keep an eye on their online bank accounts or wherever the breach happened).

Only if it cannot be ruled out that further damage could happen (e.g. it is not known who got the data) and a larger number of individuals are potentially impacted, fast notifications makes sense and can reduce the impact or any further damage from materializing.

Thank you

Yours sincerely,
Damen How
Compliance Officer
Swiss Reinsurance Company Ltd
Singapore Branch