RESPONSE TO PUBLIC CONSULTATION ISSUED BY MINISTRY OF COMMUNICATIONS AND INFORMATION AND THE PERSONAL DATA PROTECTION COMMISSION

FEEDBACK ON THE DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL

FROM

THE AMERICAN CHAMBER OF COMMERCE, SINGAPORE

28 MAY 2020

Contact:
Jessica Cho
Manager, External Affairs
jcho@amcham.com.sg
1 Scotts Road, #23-03/04/05
Shaw Centre Singapore 228208

1 Scotts Road, #23-03 Shaw Centre, Singapore 22820
Tel: (65) 6597 5730 | www.amcham.com.sg
Registration No. ROS 239/73 TAP

28 May 2020

Mr. Tan Kiat How
Personal Data Protection Commission
10 Pasir Panjang Road, #03-01
Business City Singapore 117438

AMCHAM INPUT ON THE PROPOSED AMENDMENTS TO THE PERSONAL DATA PROTECTION ACT

STATEMENT OF INTEREST

The American Chamber of Commerce in Singapore (AmCham) welcomes the opportunity to provide input to the Ministry of Communications and Information and the Personal Data Privacy Commission for the proposed amendments to the Personal Data Protection Act (PDPA).

AmCham is the leading international business association in Singapore, with over 5,000 members representing nearly 600 companies. Many U.S. companies establish their regional headquarters in Singapore before scaling up and expanding in the region. As we celebrate the AmCham's 47th anniversary in 2020, we look forward to further working together with the Singapore Government. Our goal is to meet present and future challenges to the mutual benefit of American business and the people of Singapore.

AmCham's feedback with regards to the proposed amendments to the PDPA is centered on the following areas:

I. Mandatory Data Breach Notification
II. Penalties
III. Data Portability
IV. Exceptions to Consent Requirement
V. Implementation Period

COMMENTS

Mandatory Data Breach Notification

Clarification of Territorial Scope

AmCham would appreciate greater clarity on the territorial scope of Section 26A. Specifically, the definition of 'data breach' and 'affected individual' as defined in Section 26A does not include territorial or jurisdictional limits. For example, in situations where international companies with offices in Singapore are processing international data outside of Singapore, it is unclear whether a data breach in this situation would trigger notification requirements. Expressly providing such limits in this section would assist organizations in better understanding and complying with the notification requirement.

Clarification of Time frame of Notification

AmCham seeks clarification on the timeframe in which an organization must notify the Commission of a breach.

Under Part VIA, *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.*

AmCham encourages PDPC to clarify the timeframe as 'business days', which is a more reasonable approach. Applying the calendar day definition may result in organisations utilizing constrained resources, which leads to a higher risk of an incomplete investigation. For example, if the organisation is aware of a breach on Friday, the organization faces limited resources and manpower over the weekend to launch a full investigation and prepare a report to the authorities. This would leave the organisation only Monday to determine the state and extent of the breach and complete their report. By using 'business days' as the timeframe, PDPC will better equip organisations to conduct accurate investigations.

Time frame of Notification

In regard to the same section mentioned above, AmCham encourages PDPC to amend the timeframe to require notification to all parties within a reasonable time. The required notification time of 3 days will significantly burden both organisations and regulators in two ways. First, once organisations are aware of a breach, they engage in an intense investigative process that encompasses a number and variety of parties (processors, outside computer forensic investigators, outside legal counsel, internal counsel, IT teams). Coordinating these teams to gather an accurate picture of the scope, impact, and extent of the breach may take several weeks, depending on the complexity and severity of the breach. Cyber attacks are increasingly sophisticated in this age of cutting-edge technology, despite the commendable efforts and partnerships of public and private stakeholders. While some breaches may be quickly investigated in a 3 day span, it is likely that a sophisticated breach will necessitate more time for an accurate investigation and subsequent report.

Second, a short notification time diverts attention and resources from the intense process of investigation. Organisations will naturally rush to submit the required notice by expending significant manpower and resources to meet the time requirement. This in turn increases the risk of regulators receiving incomplete or inaccurate reports, which will result in subsequent communications to clarify and/or update the authorities. Requiring notification within a reasonable time will better balance the need for regulators to receive timely *and* accurate reports and the need for organisations to thoroughly investigate and mitigate the breach.

Threshold for Notification

In regard to Section 26B(1)(b), *A data breach is a notifiable data breach if the data breach - affects not fewer than the minimum number of affected individuals prescribed*, AmCham recommends PDPC include risk of significant harm to trigger the notification requirement to the relevant parties. This will ease the volume of reports sent and filter out breaches that are not likely to result in harm, such as cases where personal data is secured by encryption.

AmCham also encourages PDPC to raise the threshold of data subjects from 500 to 1000. Most databases far exceed 500 subjects and having such a low threshold may overwhelm authorities with a flood of notices and result in 'notice fatigue'.

Penalties

AmCham strongly encourages PDPC to reconsider criminal penalties under this act and continue to impose fines, or provide clear guidance on the rare occasions where criminal liability are applied. If criminal penalties are necessary, AmCham recommends they be added to the criminal code rather than the PDPA.

AmCham encourages additional consultations on the financial penalty under Part VIB, 29(2)(d), *based on 10% of annual turnover in Singapore, or in any other case, $1 million*. This penalty is particularly onerous to startups and small and medium enterprises, and may dissuade those who are looking to use Singapore as a hub for commercial activities where data may be processed. AmCham recommends PDPC lower the potential fines so that it is proportionate to the harm caused or prescribe clear situations where the fines would be lower, such as a showing of good faith of compliance.

Data Portability

Exemption of Data Intermediaries

AmCham supports exempting data intermediaries (data processors) from the Data Portability Obligation. The party that is ultimately responsible for the personal data (data controllers) will already have contractually conditioned such requirements on its affiliates. Moreover, data controllers are in the better position to process data portability requests. Data intermediaries generally do not have direct relationships with requesting individuals and do not provide services directly to the requesting individuals, therefore they are unable to effectively respond to portability requests.

User Activity Data vs. Derived Personal Data

In regard to Amendment of Section 2, AmCham would appreciate greater clarity regarding the definition and scope of 'user activity data': *"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*.

"Derived personal data" 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 does not include personal data derived by the organisation using any prescribed means or method.

AmCham recommends this amendment should expressly apply to user activity data that is organised or structured by the business regarding each user. Many organisations gather aggregate data that make it very difficult and/or impracticable to sort and attribute to an individual. For example, cyber security firms gather unstructured aggregate information for threat analysis. Requiring organisations to include such data in portability requests may result in unintended disclosures of information that should not be disclosed to the requesting individual.

AmCham would also appreciate greater clarity on the distinction and scope of derived personal data and user activity data. There is no international standard for what constitutes user activity data, so clearer guidance on what types of data falls under user activity data and derived personal data would increase compliance of this provision, and reduce the risks of under or over reporting during porting exercises. The definition of user activity data includes the word 'created', which leads to confusion on whether data created as a result of an individual's use of a product or service provided by an organisation is user activity data or derived user data. Additionally, too broad of scope for user activity data may result in the disclosure of proprietary data used to provide or improve services, which can impact fair competition and hinder innovation.

AmCham strongly encourages future discussions with industry on data portability to ensure the act is calibrated to the ever-changing data landscape.

Exceptions to Consent Requirement

In regard to the new Second Schedule (Amendment Bill, p. 43) AmCham supports the three exceptions to the consent requirement: legitimate interests, business improvement, and research. AmCham recommends PDPC to include an explicit exception for information security and sending communications to existing customers about new products and services under legitimate interests.

Implementation Period

AmCham recommends PDPC to allow for a two-year implementation period for the law and for all subsequent rulemaking, which should also allow for notice and comment.

CONCLUSION

Data is a critical factor in securing Singapore's position as a hub for technology, innovation, and business competitiveness. AmCham greatly appreciates the efforts of MCI and PDPC in facilitating open discussions with industry on Singapore's personal data protection regime. We look forward to working closely together with Government on advancing Singapore as a global center of innovation.

Yours Sincerely,

Dr. Hsien-Hsien Lei
Chief Executive Officer