Public Consultation on the Draft Personal Data Protection (Amendment) Bill

Response from

Yvonne Wong, MAISP

Associate Director, Data Protection Officer

Association of Information Security Professionals (AiSP)

yvonne.wong@aisp.sg

27 May 2020

Submission in personal capacity as the Data Protection Officer (e: secretariat@aisp.sg), and not on behalf of AiSP as our members are not able to comment before the deadline.

Summary of major points arising from the Personal Data Protection (Amendment) Bill 2020:

1 The inclusion of accountability as a principle may not be appreciated in Singapore's work culture. Companies would need sequential facilitation and specific guidance on how they nurture accountability and ownership of individual processes in their workforce.

2 Some changes in the Bill include specific penalties arising from unauthorised processing of personal data that is managed or controlled by public agencies, arising from the Public Sector Data Security Review Committee's recommendations. There is also some targeted information on technical measures regarding Spam Control Act.

3 However, the changes remain broad-based when it comes to "reasonable and expeditious" notifiable data breach and how organisation assesses whether there would be significant harm to the affected individuals. It can be subjective, and organisations would require detailed guidance on managing their risk assessment.

4 Changes in data portability are fair to consumers. However, it is not certain if efforts and cost involved for organisations to incorporate this implementation to existing systems, work processes and policies will be onerous. If organisations are not able to do so properly, then the changes would not be meaningful.

5 Given the rise in digitalisation and remote working during COVID-19 pandemic, it is useful for amendments to cover automated processes involving personal data including decision-making. More companies would be leveraging AI and machine learning to automate certain processes involving extensive amount and types of personal data. There should be consideration for organisations' accountability on automated decision-making when it impacts lives of people.

Statement of interest

6 AiSP focuses on raising the professional standing of information security personnel in Singapore. Legislation and regulations that shape practices and behaviours on cyber and information security are of interest to us. As our industry focuses on cybersecurity practices and controls in our daily operations, the fact that people remain the weakest link - despite developments in data protection regimes, advancements in digital tools, and greater appreciation for privacy rights. Through our advocacy efforts in cybersecurity awareness since 2018, Singapore SMEs' adoption of the Personal Data Protection Act (PDPA) practices appear to be low after the Act came into effect in 2014. Interest has increased with the increase in penalties for data breaches in Singapore but some companies do not embrace the mindset. Broadly, some changes in the proposed amendments require guidance and some level of handholding from the Personal Data Protection Commission (PDPC) for Singapore companies to be compliant.

7 Since 2019, some data protection practitioners in Singapore are aware that the PDPC has plans to table the amendments in Parliament in 2020, especially on the data breach notification. However, the timing for this public consultation may not be appropriate, considering the current COVID-19 crisis and subsequent economic downturn for many organisations and processers under the PDPA. They are important stakeholders and they are likely not available to respond to this important consultation during such challenging times; some may not even bother to respond.

Comments

8 The inclusion of accountability in the amendments is important but it may not hit home to the users of personal data (organisations, processors) on what they need to do based on Singapore's work culture. The role and primary job scope of a data protection officer in Singapore SMEs is very

different from other larger organisations and in overseas. It cannot be compliance for compliance's sake. In addition, more companies are expected to embark on digitalisation[1], during COVID-19 pandemic and post COVID-19 conditions.

9 On notifiable data breach, organisations need guidance on conducting assessment of data breach in a reasonable and expeditious manner. The concept of expeditious may vary from organisation A to organisation B. Importantly, the objective of risk assessment should be having a proper and robust validation instead of at the expense of speed, when the data breach results in, or is likely to result in, significant harm to the affected individuals. Please elaborate what it means by affect not fewer than the minimum number of affected individuals prescribed.

10 Please clarify if porting organisation refers to organisation or resident in an applicable country, like receiving organisation. It is stated that a porting organisation must not transit any applicable data about an individual if it can reasonably be expected to be contrary to the national interest. Please define if the national interest is applicable to all countries and not just Singapore.

11 On transmission of personal data under data porting request, the relationship between individuals *P* and *T* should be based on legal relations if *T*'s consent is not required – if the data porting request is made in *P*'s personal or domestic capacity, or relates to P's user activity data or user-provided data. It is not clear why *T*'s consent is required and the basis for this.

12 Please elaborate the need to specify that the financial penalty must not exceed 10% of annual turnover for organisation's or individual's annual turnover exceeding $10 million, since the cap of $1 million remains the same in current Act.

13 Specific penalties for an individual who discloses, or the individual's conduct causes disclosure of, personal data in the possession or under the control of an organisation or a public agency to another person, underscores the seriousness of such offence. Please clarify the need to exclude consultant or agent of the Monetary Authority of Singapore (MAS) under unauthorised disclosure or improper use or unauthorised re-dentification of anonymised information of personal data. In addition, please clarify the difference between an officer and an employer of MAS.

14 The staggering amount of data collected and shared by people and devices worldwide, are growing exponentially with technological progress. Besides data portability, there is no mention on how the PDPA can raise the level of accountability on companies in using data analytics and automated processes that track, monitor and profile individuals. In my opinion, I was expecting the amendments to be more forward-looking. More companies – large organisations and startups, are using algorithm and AI to improve customers' purchasing experience, especially on online platform during COVID-19 pandemic. There should be more emphasis on this as part of the amendments.

1) The rise of telemedicine is also an emerging concern as prognosis may be automated based on sensitive personal data. This is important in our ageing population and how our healthcare infrastructure is evolving.
2) There are new developments in processing personal data for insurance application overseas, and one dimension is based on the individual's lifestyle choices and risk appetite. As a hub for 'deep-tech' startups, it is likely that Singapore companies may want to focus on this as business proposition.

[1] Sources: https://www.singaporebudget.gov.sg/budget_2020/fortitude-budget/fortitude-budget-statement, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-covid-19-recovery-will-be-digital-a-plan-for-the-first-90-days.

3) Increasingly, companies are using automated processes to filter job applicants' submission and the process may not be fair to some candidates if the algorithm has inherent biases in place. Some recruitment companies also conducted due diligence on applicants' social media activities as well. It will be a great leap forward if we can consider Singapore's take on automated decision-making when personal data is being processed for decision-making that has significant impact to people's lives.

15 It will help the responsible users of the PDPA to understand the Act and their roles and obligations better if our language and expression are easier to understand and have clear interpretation. I understand some organisations rely on lawyers to interpret the Act for them as the non-legal personnel do not understand clearly on what is required. This may not be viable for freelancers who are considered organisations under the PDPA; and there would be more freelancers in Singapore with companies' cost-cutting measures or closure. I believe the PDPC put in significant resources and efforts to develop the advisory guidelines and materials to equip better appreciation of the Act. It could be more practical and productive if our Act is worded for the laymen, for instance, how the General Data Protection Regulation is articulated.

16 From the perspective of cyber threat landscape in Singapore, there has been an increase in e-commerce fraud, phishing, and attacks since COVID-19 pandemic; it is likely to persist with large-scale telecommuting and home-based learning. Given our open economy and interconnectivity with other regional markets and ecosystems, the impact of a minor gap in personal data protection by one organisation can have repercussions to other stakeholders in the chain. It is important that the key principle of accountability is complement with organisation's security and protective measures that cut across people, processes, and technology. This would be one of my key narratives I would share with AiSP members, their organisations and industry players in Singapore's cybersecurity ecosystem.

Conclusion

17 Based on current COVID-19 conditions and economic aftermath, it is probable to see exponential use and sharing of personal data from diverse stakeholders and possibly, cross border. I hope future amendments can take this into consideration so that the accountability principle can be observed in a more holistic manner. Personally, I hope to see clarity on protection for sensitive personal data and minors' privacy rights. As it takes a lot of resources and efforts to amend an Act, we should consider if the intended outcomes could be meaningfully realised based on the current constraints faced by organisations.

(end)