RESPONSE TO DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL, INCLUDING RELATED AMENDMENTS TO THE SPAM CONTROL ACT

By
Sunil Prabhakaran
IBM Security
Data Protection and Privacy Lead

Note: This response is drafted is on an Individual capacity as a Data Privacy Practitioner and no way related to my Organization's opinion on the subject.

1. Introduction:

The Ministry of Communications and Information (MCI) and the Personal Data Protection Commission (PDPC) has invited the public to provide feedback on the draft Personal Data Protection (Amendment) Bill, including related amendments to the Spam Control Act (SCA). We understand that the changes are in leu with the technology advancements, digital transformation that organizations are embarking on, sophisticated attacks and cross border data flows (especially in cloud-based business models) in mind. Additionally, the amendments are intended to ensure that the act is in proximity with the changing threat landscape and circumstances.

The following is a summary of some of the welcoming changes that has been proposed in the Singapore Personal Data Protection Bill.

- The first major amendment in PDPA is to **strengthen the accountability** of organizations that collect, store, process and transfer personal data of Individuals. This is done through introduction of the following:
  - ✓ Mandatory **Data Breach notification** for Organizations.
  - ✓ **Removal of exclusion for organizations acting on behalf of public agencies**. The current act has the third parties assisting the public agencies and handling personal data on their behalf being excluded from the application of the Data Protection Provisions of the PDPA.
  - ✓ Offences relating to **egregious mishandling of personal data**.
- The second major amendment in PDPA is to **enable meaningful consent**. This will be brought into practice by means of **Enhanced framework for collection, use and disclosure of personal data.** These amendments are broadly similar to approaches under the data protection frameworks in various other jurisdictions.
- The Third major change is to **increase consumer autonomy.** This has been a topic of discussion for some time and a **new Data Portability Obligation** will be introduced. Like many other major data protection frameworks like EU GDPR, Data Portability will allow Individual to request an organisation to transmit a copy of their personal data to another organisation. In addition to this, the amendment also wants to provide consumers with greater control over the unsolicited marketing messages.

- The final amendment is on **strengthening the effectiveness of Enforcement**. The proposed amendment will have financial penalties for Organizations to be increased to 10% of the turnover in Singapore or 1 Million Singapore Dollars, whichever is higher.

2. Summary of major points and Statement of Interest

The following section will have a summary of all the major amendments in the Personal Data Protection Bill and our point of view on the recommendations provided in the Bill.

2.1. Strengthen the accountability

Summary: According to the current amendment, organizations are supposed to notify the PDPC and affected individual in case of a data breach and in case the data breach meets the notification criteria. The MCI/PDPC has clearly called out the criteria based on which a breach qualifies to be notified to the PDPC and affected Individuals. According to the section **26B.— (1) – Notifiable Data Breaches** of the draft Bill, there are 2 notification criteria for a breach to the Authority and Data Subject. a) in case there is a significant harm to the Individual b) in case of Significant scale.

Points for Consideration	***Statement of Interest***
The draft bill is not clear on what constitutes a significant scale. When read in conjunction with the "PUBLIC CONSULTATION PAPER ISSUED BY THE MINISTRY OF COMMUNICATIONS AND INFORMATION AND THE PERSONAL DATA PROTECTION COMMISSION", it is clarified that data breaches affecting 500 or more individuals would be an appropriate threshold for a significant scale. In addition to this, the type of data compromised could be another notification criteria e.g.: Sensitive Critical data like health data and financial data. However, it is not clear whether PDPC will be coming up with a methodology for assessment of severity of personal data breaches in order to help Organizations to assess the breach for Notification.	*Like other jurisdictions e.g.: EU, it is imperative that PDPC also comes with a* ***Recommendations for a methodology of the assessment of severity of personal data breaches****.* The proposed methodology shall be designed with the following objectives: - To provide Organizations with a quantitative tool (to the extent that this is possible) to assess the severity of data breaches and accordingly notify the authorities as well as the affected individuals. The tool could also serve as a means for organizations to quickly determine the necessary mitigation measures. - To provide the authorities with a tool to assess the severity of the breaches notified by the data controllers.

Points for Consideration	*Statement of Interest*
	- To support the authorities in the process of performing detailed analyses and statistics concerning the reported personal data breaches. - To contribute to the harmonization of the severity assessment of personal data breaches in Singapore, by proposing a common methodology and severity scoring. In addition to this, as per the draft bill capping the data breaches affecting 500 or more individuals would be an appropriate threshold for a significant scale shall be re-looked and Authorities may propose that it has to follow the methodology to arrive at a conclusion on whether the data breach has to be notified. For e.g.: (1) In case there is a data breach and if the breach has resulted in compromised of 450 records and those records have Personally Identifiable Information (not SPII) of high-profile individuals within Singapore like name, telephone number and house address. This does not qualify to be notified according to the proposed criteria. However, if it based on a risk-based approach then this could potentially be notified to the authority considering the details of high-profile individuals. (2) A breach affecting 500 individuals may be large for a small Organization viz a via a large multinational. Instead the Authority may consider providing percentage of data compromised against the total volume of data the organization possess. This will also urge Organizations to understand what data they have in their possession.

Summary : According to **Section 26D.— (1) - Duty to notify occurrence of notifiable data breach**, Once the organisation has credible grounds to believe that a data breach has occurred, the timelines for the notification is defined as 3 days (72 hours) from the time the notification assessment has been performed. When read in conjunction with the "PUBLIC CONSULTATION PAPER ISSUED BY THE MINISTRY OF COMMUNICATIONS AND

INFORMATION AND THE PERSONAL DATA PROTECTION COMMISSION" it is specified that PDPC must be notified before or at the same time as affected individuals are notified, to allow PDPC to assist affected individuals who contact PDPC once they are notified.

According to **Section 26C.— 2.a and b - Duty to conduct assessment of data breach**, In case the breach is discovered by the "data intermediary" – entity that processes data on behalf of another Organization, the data intermediary is required to notify the Organization on whose behalf they process the personal data without undue delay.

Clarification	**Statement of Interest**
Undue delay for notification by data intermediary is open ended and could be left to the Interpretation of the Organization. Additionally, are the data intermediaries supposed to notify the parent Organization once there is an Incident or once it qualifies it to be a breach?	Organizations shall re-look at the contracts with their Data Intermediaries in order to cater to the new requirement of 72 Hours for notification. It is recommended that in case the data intermediaries identify a security incident and it affects the PII in their possession, the data intermediaries shall immediately notify the Organization instead of waiting to qualify it as a breach. Advantages of doing this could be that there are more than one party involved to see whether the incident qualifies to be a breach.

Summary: MCI and PDPC has proposed for exceptions to the requirement to notify affected individuals. This includes a) organization has taken remedial action to reduce the significant harm. b) have technological protection (e.g. encryption, masking) that is of a reasonable security standard.

Clarification (2): The above point needs clarification on whether the same could apply for the PDPC as well or will apply for notification to individuals only. An explicit statement on whether to notify the PDPC in this case would be helpful for Organizations.

Summary: According to **Section 26D.— 6 - Duty to conduct assessment of data breach**, organizations must not notify any affected individual if instructed by a prescribed law enforcement agency or directed by PDPC. However, this is in contradiction with the point PDPC must be notified before or at the same time as affected individuals are notified, to allow PDPC to assist affected individuals who contact PDPC once they are notified.

Clarification	**Statement of Interest**
what happens if both authority and individual is notified simultaneously and If PDPC takes a call to not notify the Individual?	The bill shall consider the above point on both authority and individual being notified simultaneously and If PDPC takes a call to not notify the Individual. The process shall be

Clarification	Statement of Interest
	streamlined to first notify the authorities and then notify the Individuals. This will avoid issue in case the authorities do not want the Organization to notify the Individuals.

The Draft bill has also made it very clear that the data breach notification requirements under the amended PDPA do not affect any data breach notification requirements organizations have under any other laws. If there is a requirement that has to be notified to any other public agencies or authorities, the same has to be done as per the requirement.

The 2 welcoming points and positive points with respect to accountability is as follows:

- **Removal of exclusion for organizations acting on behalf of public agencies.** As per PSDSRC recommendations, the PDPA will be amended to remove the exclusion for organizations that act on behalf of a public agency in relation to the collection, use or disclosure of personal data.
- **Offences relating to egregious mishandling of personal data.** New offences under the PDPA to hold individuals accountable for egregious mishandling of personal data in the possession of or under the control of an organisation or a public agency. Individuals found guilty of each offence will be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding two years, or both. This ensures that the offences and penalties are aligned for public officers and other individuals.

2.2. Increasing consumer autonomy

2.2.1. Data Portability

Summary: Very similar to the EU GDPR requirements, the Draft bill has a new data potability obligation which provides consumer the right to request an organisation to transmit a copy of their personal data to another organisation. O in a commonly used machine-readable format. The Data Portability Obligation will be scoped to ***User provided data, User Activity Data created as a part of the user consuming the product or services of the Organization***. In addition to this, the user needs to have an existing relationship or contract with the Organization in order to request for porting the data.

PDPC may also extend data portability to like-minded jurisdictions with comparable protection and reciprocal arrangements. However, it is not clear what would be these jurisdictions.

Since it allows the direct transmission of personal data from one organization to another, the right to data portability is also an important tool that will support the free flow of personal data and foster competition between Organizations. It will facilitate switching between different service providers and will therefore foster the development of new services in the context of the digital single market strategy.

Clarification	**Statement of Interest**
Does the Organization answering a data portability request have any specific obligation to check and verify the quality of the data before transmitting it?	Organizations answering a data portability request shall not have any specific obligation to check and verify the quality of the data before transmitting it. These data should already be accurate, and up to date, according to the other requirements of PDPA. Moreover, data portability does not impose an obligation on the organization to retain personal data for longer than is necessary or beyond any specified retention period. Importantly, there is no additional requirement to retain data beyond the otherwise applicable retention periods, simply to serve any potential future data portability request.

Summary: The Data Portability Obligation will only come into effect with the issuance of Regulations. This essentially means that the data portability will be applicable in a prospective manner and will not apply retrospectively for Organizations. The authorities have also clearly mentioned in the draft bill that it intends to provide the following details:

- **'whitelist' of data categories** – The data on which the Data Portability Obligation applies.
- **technical and process details** – To ensure that the correct set of data is transmitted to the receiving Organization. *However, it is not very clear that whether the Organization answering a data portability request have any specific obligation to check and verify the quality of the data before transmitting.*
- **relevant data porting request models** – Whether the request can be made to the porting organization or through the receiving organization and what will be the process for the same.
- **Safeguards for individuals** - measures to protect consumers and measures to reduce risks to the ecosystem.

Based on the various inputs from the previous consultation paper on Data Portability, the draft bill covers Exceptions to the Data Portability Obligation will be provided. When read in conjunction with the "PUBLIC CONSULTATION PAPER ISSUED BY THE MINISTRY OF COMMUNICATIONS AND INFORMATION AND THE PERSONAL DATA PROTECTION COMMISSION", personal data about an individual that is derived by an organisation in the course of business from other personal data (referred to as "derived personal data") will not be covered by the Data Portability Obligation.

Clarification	**Statement of Interest**
The authorities should provide a guidance to Organizations on what could be called as a derived data.	Derived data are created by the organizations on the basis of the data "provided by the data subject". As per the inputs from EU GDPR WP 29 – Example of derived data could be the outcome of an assessment regarding the health of a user or

Clarification	Statement of Interest
	the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules) cannot in themselves be considered as "provided by" the data subject. Even though such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject (through his actions for example), these data will typically not be considered as "provided by the data subject" and thus will not be within scope of this new right
what is the time limit imposed to answer a portability request? After undertaking a request, what is the timeline to respond with action taken?	According to some of the other regulations like GDPR, the Organization shall provide "information on action taken" to the data subject "without undue delay" and in any event "within one month of receipt of the request". This one-month period can be extended to a maximum of three months for complex cases, provided that the individual has been informed about the reasons for such delay within one month of the original request.

2.2.2. Controls for unsolicited messages

According to our understanding, The PDPA's DNC Provisions and the SCA's Spam Control Provisions will address consumer annoyance and provide consumers to decide on what messages they receive. This is a welcoming move considering the fact that there are a number of unsolicited messages that residents of Singapore receive on a daily basis. The SCA will also cover commercial text messages sent to IM accounts. Additionally, DNC Provisions will prohibit the sending of specified messages to telephone numbers obtained through the use of dictionary attacks and address harvesting software. The draft bill also talks about Introduce of obligation and liability on third-party checkers who check the DNC registry on behalf on other organizations.

2.3. Enabling Meaningful Consent

According to the **Amendment of section 15 in the draft bill**, MCI/PDPC has proposed to enhance the framework for the collection, use and disclosure of personal data under the PDPA to ensure meaningful consent by individuals, complemented by accountability requirements to safeguard individuals' interests. This would include deemed consent by contractual necessity, deemed consent by notification.

Just to elaborate a bit more on the understanding on deemed consent by contractual necessity, this will come into picture when there is a reasonable necessity for the conclusion or performance of a contract or transaction between

an individual and an organisation. If an organization seeks to process personal data that are necessary for the performance of a contract, there is no need to use another lawful basis such as consent.

An example could be when a user makes an online purchase, an Organization processes the address of the user in order to deliver the goods. This is necessary in order to perform the contract. However, the profiling of a user's interests and preferences based on items purchased is not necessary for the performance of the contract and the controller cannot rely on this as the lawful basis for this processing. Even if this type of targeted advertising is a useful part of your user relationship and is a necessary part of your business model, it is not necessary to perform the contract itself.

Like EU GDPR, the imbalance of power between the Organization and the data subject shall also be taken into consideration.

Deemed consent by notification could come into picture in case appropriate notification has been provided to inform the individual of the purpose of the intended collection, use or disclosure of his/her personal data, with a reasonable period for the individual to opt-out of the collection, use or disclosure of his/her personal data for that purpose; and (ii) the individual did not opt-out within that period. Organizations shall ensure that there is no adverse effect to the individual due to deemed consent by notification.

In addition to the above, there are two new exceptions to the consent requirement that will be introduced when the bill comes into effect:

- **Legitimate Interest Exception**
- **Business Improvement Exception**

Taking the same example under deemed consent by contractual necessity, when a user makes an online purchase, an Organization processes the address of the user in order to deliver the goods. This is necessary in order to perform the contract. However, the profiling of a user's interests and preferences based on items purchased is not necessary for the performance of the contract and the controller cannot rely on this as the lawful basis for this processing. Even if this type of targeted advertising is a useful part of your user relationship and is a necessary part of your business model, it is not necessary to perform the contract itself.

However, the above example could be an idea example for Business Improvement exception. This could be for any of the three reason as mentioned below.

- operational efficiency and service improvements;
- developing or enhancing products/services; and
- knowing the organization's customers.

Note: Legitimate Interest Exception could come handy for organizations while doing business. Legitimate interests as other regulations like GDPR mentions, is the most flexible lawful basis for processing, but cannot assume it to be the most appropriate. Organizations should identify a legitimate interest; show that the processing is necessary to achieve it; and

balance it against the individual's interests, rights and freedoms. What most of the Organizations should keep in mind is that If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply. The same shall be documented and made justifiable. PDPC like other regulatory body could give guidance to Organizations on how to evaluate whether individual's interests override the legitimate interest.

2.4. Strengthening effectiveness of enforcement

In order to enforce data protection practices to organizations and in order to increase the importance of having a data protection framework to be Implemented and practices within the Organization, The amendments will increase the maximum financial penalty to up to 10% of an organization's annual gross turnover in Singapore; or S$1 million, whichever is higher. This is very similar to penalties imposed by other geos.

3. Conclusion

Singaporean Authorities-MCI and PDPC have taken the right step at the right time to make updates considering that Data Security and Privacy are all increasingly at risk and also more important and intertwined in our data-driven economy. The points especially regarding Data Portability, Increased fines and accountability for Organization in form of notifying the data breach are welcoming and has put Individual rights at utmost importance. We presume that these positives will be well accepted by Organizations in case the authorities come with the right set of guidance to support the Implementation of the requirements on ground. To summarize some of them are as follows:

- Recommendations for a methodology of the assessment of severity of personal data breaches.
- Breach Notification Guidance with timelines
- Guidance on what could be called as a derived data

Note: Please note that there are references obtained from some other countries' regulations such as EU GDPR. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052