Public Consultation on Personal Data Protection Amendment Bill

Submitted by:
AIG Asia Pacific Insurance Pte. Ltd.

Contact Persons: [Redacted]

	Proposed Amendment – extracted from CP (pls read details in CP)	Statement of Interest/Comments
2	Organisations will be required to notify PDPC of a data breach that (i) results in, or is likely to result, in significant harm to the individuals to whom any personal data affected by a data breach relates (the "affected individuals"); or (ii) is of a significant scale. Organisations will also be required to notify affected individuals if the data breach is likely to result in significant harm to them. Notifying PDPC allows organisations to receive guidance from PDPC on post-breach remedial actions (e.g. implementation of data breach management plans) where necessary, and provides PDPC with a better sense of which sectors might need greater support in holding up data protection standards. Notifying affected individuals allows them to take steps, where possible, to protect themselves (e.g. changing passwords, cancelling credit cards, monitoring and reporting scams or fraudulent transactions, etc.). It also ensures that organisations are accountable to individuals for the proper handling and safekeeping of their personal data.	We agree with the PDPC's approach that a balance needs to be found between promoting a secure environment and enabling organisations to collect and use data. To that end, we agree that breach notifications to the PDPC and impacted data subjects may promote the reasonable protection of personal data where the data breach results or may result in significant harm to the individual. However, we believe that: i. Any requirement to notify the PDPC of a breach of a significant scale (ie the proposed section 26B(1)(b)) should only apply where the said breach results in or is likely to result in harm to the impacted individuals based on an objective assessment of all relevant facts. As it stands, there is no harm requirement under the proposed section 26(1)(b). ii. This is inconsistent with the breach notification laws in other jurisdictions where notification applies where there is an element of harm or risk present. iii. A breach notification requirement which does not include an element of harm may result in unwarranted fear amongst data subjects that their data may be misused. As an example, incidents relating to personal data which is sufficiently secured (eg by encryption or multi factor authentication or other similar measures) is unlikely to suffer any harm. iv. This may also discourage organizations from collecting and using personal data as organisations may be wary of reputational costs to their business as well as the need to expend resources in responding to requests for information from the public and/or PDPC even where there is unlikely to be any harm to the data subjects. v. Further, a breach that involves the data of 500 individuals (the proposed threshold) does not equate to there being a systemic risk.
	To provide clarity for organisations to ascertain whether a data breach meets this notification criteria, MCI/PDPC intends to prescribe in Regulations a numerical threshold on what constitutes "a significant scale" in terms of the number of individuals affected in a data breach. Based on its past	Please see above (point 2) in respect of our comments on the proposed section 26B(1)b)

	Proposed Amendment – extracted from CP (pls read details in CP)	Statement of Interest/Comments
	enforcement cases, PDPC notes that data breaches affecting 500 or more individuals would be an appropriate threshold.	An element of harm is required before a data breach becomes reportable to the PDPC.
	MCI/PDPC also intends to prescribe in Regulations categories of personal data which, if compromised in a data breach, will be considered likely to result in significant harm to the individuals. This makes clear the types of data breaches that organisations will be required to notify affected individuals. Several jurisdictions have adopted a similar "whitelist" approach for data breach notification to affected individuals and/or the authorities[1]. Examples of data categories prescribed by other jurisdictions include social security numbers, drivers' licence numbers, state identification numbers, credit/debit card numbers, health insurance information and medical history information.	An assessment on whether an incident would result in or is likely to result in significant harm should be based on an objective assessment of all relevant facts. Besides the type of data, the circumstances under which the breach occurred is an important factor in such an assessment. We believe that it would be better to instead provide guidance on the factors to be taken into account in making the assessment rather than a deeming provision If, however, the PDPC wishes to statutorily provide for categories of personal data which PDPC believes is likely to result in significant harm to an individual if the prescribed data is the subject of a security incident, we recommend that section 26B(2) be worded as a rebuttable presumption instead of a deeming provision, so that other relevant facts and circumstances may be taken into account in assessing significant harm It is important that an objective assessment of all relevant facts be made (and not just the type of data involved) to avoid panic and anxiety to the affected

[1] For instance, various states in the US (such as California and Washington) have prescribed categories of personal data for notification to affected individuals and relevant authorities where a data breach meets the requirements for notification.

	Proposed Amendment – extracted from CP (pls read details in CP)	Statement of Interest/Comments
		individual(s) especially when an organization has taken all reasonable steps to contain the breach.
	Exceptions to requirement to notify affected individuals a) Remedial action exception: where organisations have taken remedial actions to reduce the likely harm or impact to the affected individuals such that the data breach is unlikely to result in significant harm to the affected individuals. b) Technological protection exception: where the personal data that was compromised by the data breach is subject to technological protection (e.g. encryption) that is of a reasonable security standard, such that the data breach is unlikely to result in significant harm to the affected individuals. Organisations must not notify any affected individual if instructed by a prescribed law enforcement agency or directed by PDPC. PDPC will have the power to exempt organisations from notifying affected individuals.	Given that there may be cases where a prescribed law enforcement agency or PDPC may direct organizations not to notify an affected individual, we would recommend that individuals should only be notified after notifying PDPC and PDPC has agreed that the organization may notify the individuals
	MCI/PDPC will introduce the following 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: a) Knowing or reckless unauthorised disclosure of personal data; b) Knowing or reckless unauthorised use of personal data for a wrongful gain or a wrongful loss to any person; and c) Knowing or reckless unauthorised re-identification of anonymized data. Organisations remain liable for the actions of their employees in the course of their employment with the organisations. Employees acting in the course of their employment, in accordance with their employer's policies and	We believe that inadvertent human errors should not amount to "knowing" unauthorized disclosure or re-identification. We also believe that (a) and (c) should also be conditional upon the disclosure or re-identification of anonymized data for "a wrongful gain or wrongful loss to any person". We will be grateful if PDPC could provide examples of reckless unauthorized disclosure of personal data would entail

	Proposed Amendment – extracted from CP (pls read details in CP)	Statement of Interest/Comments
	practices, or whose actions are authorized by their employers, will not run the risk of such criminal sanctions. In addition, MCI/PDPC does not intend for these offences to apply in situations where the conduct is in the nature of a private dispute for which there is recourse under private law (e.g. ex-employee taking an organisation's customer list when joining a competitor). Such private disputes should continue to be settled through civil suits or other forms of dispute resolution. The amendments provide for defences, such as where the information is publicly available; where the conduct is permitted or required under other laws; or where the conduct is authorised or required by an order of the court or in the reasonable belief that the individual has the legal right to do so.	
	MCI/PDPC will expand deemed consent under section 15 of the PDPA to include: a) Deemed consent by contractual necessity - where it is reasonably necessary for the conclusion or performance of a contract or transaction between an individual and an organisation. b) Deemed consent by notification - if (i) the organisation provides appropriate notification 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	We support this to include situations where the organization cannot provide a service if there is no consent. In our context, an example would be when a policyholder wants to withdraw consent totally for collection, use and disclosure of personal data (as opposed to just withdrawing consent to marketing). In such cases, it would be impossible for an insurer to continue with the policy since it will not be able to process, service or administer it. It would be helpful for organisations if the PDPC could provide guidance on: i. What amounts to a reasonable period ii. The factors to be considered in assessing the existence of any "adverse effects" that is likely to have on an individual iii. The form the assessment ought to take. We propose that this should be expanded to allow for deemed consent where organization may engage third party to perform the services. In the current business environment, outsourcing is very common and the expectation is that some activities will be performed by third party and customers PII will be shared with the third party service provider.

	Proposed Amendment – extracted from CP (pls read details in CP)	Statement of Interest/Comments
	disclosure of his/her personal data for that purpose; and (ii) the individual did not opt-out within that period. In order to rely on deemed consent by notification, organisations are required to assess and ascertain that the intended collection, use or disclosure of personal data for the purpose is not likely to have any adverse effect on the individual after implementing measures to eliminate, reduce the likelihood of or mitigate the identified adverse effect to the individual. Organisations also may not rely on this approach to obtain consent to send direct marketing messages to the individuals. Individuals will also be able to withdraw their consent to the collection, use or disclosure of their personal data. Please refer to clause 7 of the draft PDP (Amendment) Bill.	
	To ensure that the compliance burden is reasonable for organisations, the Data Portability Obligation will be scoped to the following: a) User provided data (i.e. data that is provided to the organisation, such as name, contact information, credit card details, delivery address) and user activity data (i.e. data about the individual that is created in the course of or as a result of the individual's use of any product or service, such as transactions, data collected by wearables and sensors) held in electronic form, including business contact information; b) Requesting individuals who have an existing, direct relationship with the organisation; and c) Receiving organisations that have a presence in Singapore. PDPC may also extend data portability to like-minded jurisdictions with comparable protection and reciprocal arrangements.	We recommend that the PDPC considers the following in implementing any data portability requirements: i. The costs and investment in implementing data portability requirements are likely to be significant ii. Cybersecurity risks are likely to increase given the increase in applications accessing the subject data and/or databases storing the subject data and the additional transfer of subject data; iii. Financial institutions are subject to stringent client confidentiality obligations; Given the foregoing, we recommend: i. Data portability obligations may not be appropriate with respect to organisations in sectors which are regulated and which have strict client confidentiality obligations and which handle data that may be sensitive. ii. A better approach may be to encourage organisations in such sectors to share data through industry driven efforts. This could include industry-driven data pooling and sharing through the General Insurance Association and the Association of Singapore Banks. Such associations are likely to be able to pool together a larger pool of relevant data in a structured format for use within the sector or across sectors

	Proposed Amendment – extracted from CP (pls read details in CP)	Statement of Interest/Comments
		iii. It should be made clear that the data porting organization bears no liability in verifying if the recipient organization is a legitimate business or whether the data subject provided the correct details of the recipient organization. Such information is entirely within the knowledge of the data subject and/or the receiving organization and porting organisations should not be required to expend further resources to verify the said information. We will be happy to provide further comments when details are clearer <u>Definition of Derived Personal Data</u> Data about an individual may be derived from a combination of personal data and aggregated or anonymised data. The proposed definition of derived data does not clearly cover such circumstances. We recommend that the definition of derived personal data be amended to cover personal data that is derived from any other data elements and not limited to personal data derived only from other personal data.
	User provided and user activity data may include personal data of third parties. Organisations need not obtain consent from the third party whose personal data is to be ported as a result of an individual's data porting request. However, organisations may only port such third party's personal data where the data porting request is made in the requesting individual's personal or domestic capacity.	Since third party's personal data may be ported to the receiving organization, it may contain personal data of an EU resident. What then would be the obligation of the receiving organization viz a viz the EU resident data?
	The Data Portability Obligation will only come into effect with the issuance of Regulations. PDPC intends to prescribe the following in the Regulations: a) A 'whitelist' of data categories to which the Data Portability Obligation applies. b) The technical and process details to ensure the correct data is transmitted safely to the right receiving organisation, and in a usable form.	We welcome this. There should be an industry/sector agreement and coordination (e.g., General Insurance Association) to ensure data portability obligation can be managed effectively and efficiently within the industry, e.g., data format, how data will be sent and received.

	Proposed Amendment – extracted from CP (pls read details in CP)	Statement of Interest/Comments
	c) The relevant data porting request models. d) Safeguards for individuals, tailored to the risks associated with the white-listed dataset.	
	Exceptions to the Data Portability Obligation will be provided. One such exception relates to data which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organisation.	This exception is welcome.
	Organisations will also be prohibited from porting data where it is contrary to national interest; threatens the safety or physical or mental health of an individual other than the individual who made the request; or causes immediate or grave harm to the safety or to the physical or mental health of the individual who made the request.	It is burdensome to put the obligation on the organization to decide whether it can port the data as this involves due diligence by the porting organization on whether the prohibition in the law applies.
	Increased financial penalty cap Under section 29(2)(d) of the PDPA, PDPC may impose a financial penalty of up to S$1 million for data breaches under the PDPA. The amendments will increase the maximum financial penalty to (i) up to 10% of an organisation's annual gross turnover in Singapore; or (ii) S$1 million, whichever is higher.	The financial penalty of up to 10% of an organization's annual gross turnover in Singapore is too high a cap. and that the $1 million fine is sufficiently high to deter non-compliance
	Statutory undertakings Statutory undertakings allow a regulator to apply more flexible and individually tailored approaches to enforcement. From PDPC's experience, organisations that have in place a data protection management plan will have an effective system for monitoring, internal reporting, and management of data breaches. The implementation of the data breach management plan can be the subject of a statutory undertaking. When coupled with mandatory breach notification, statutory undertakings will further encourage organisations to adopt accountable practices. PDPC may investigate the underlying breach if the organisation fails to comply with the statutory undertaking. Alternatively, a breach of a statutory undertaking will be enforceable by PDPC directly through the issuance of directions. If the organisation fails to comply with these directions, PDPC may apply for the directions to be registered by the District Court under	Please clarify that an organization which has been placed under a statutory undertaking will not be subject to a financial penalty under the proposed Section 29(9)) (2d). We believe that further guidance (similar to the Guide on Active Enforcement issued by the PDPC) on the factors which PDPC will take into account in accepting statutory undertakings would be helpful.

	Proposed Amendment – extracted from CP (pls read details in CP)	Statement of Interest/Comments
	section 30 of the PDPA. Please refer to clause 18 of the draft PDP (Amendment) Bill.	
	<u>Referrals to mediation</u> To enable PDPC to manage the increase in data protection complaints in a sustainable manner, MCI/PDPC will amend section 27 of the PDPA to provide PDPC with the power to (i) establish or approve one or more mediation schemes; and (ii) direct complainants to resolve disputes via mediation, without the need to secure consent of both parties to the complaint or dispute. Where individuals seek PDPC's assistance on a complaint or dispute under the PDPA, all parties to the complaint or dispute will be required to participate in the mediation scheme when directed by PDPC, and must comply with such terms and conditions of participation in the scheme as may be prescribed. If an individual does not agree to the terms and conditions of the scheme, he/she may attempt to resolve the matter on his/her own, either through exercising his/her right of private action under section 32 of the PDPA, or by other forms of alternate dispute resolution outside of the PDPA. Please refer to clause 15 of the draft PDP (Amendment) Bill.	Which statutory body will administer and conduct the mediation? We would be grateful for guidance on which party will bear the costs of mediation and whether parties may be represented by lawyers.