PUBLIC CONSULTATION ON THE DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL 2020

SUBMISSION BY SINGAPORE EXCHANGE LIMITED

27 May 2020

Submitted by: Singapore Exchange Limited
2 Shenton Way, #02-02
SGX Centre 1
Singapore 068804

Contacts: Jeth Lee
Head, Compliance
+65 6236 8513
jeth.lee@sgx.com

SUMMARY OF MAJOR POINTS

- The remedial action and technological protection exceptions to the requirement to notify affected individuals should similarly apply to the "significant harm" limb of the requirement to notify the PDPC.

- The wording of the draft Bill should clarify that the new maximum financial penalty is in respect of an organisation's annual turnover in Singapore (as expressed in the Consultation Paper).

- Alternative mechanisms should be explored in preserving personal data pending exhaustion of an individual's request or appeal processes. In particular, onus should be placed on the individual to notify an organisation of the status of, or intention to file, a request or appeal. This is given that the organisation may not have the unilateral means of ascertaining this.

- Individuals who have obtained derived personal data from an organisation by exercising their access rights should be prohibited from sharing such data with other organisations for commercial gain. This is to protect business innovation and investments by organisations.

STATEMENT OF INTEREST

The respondent, Singapore Exchange Limited ("SGX"), operates a vertically integrated group of companies that provides listing, trading, clearing, settlement, depository and data services across various asset classes. The proposed changes may impact the services that SGX provides to individuals.

COMMENTS

No.	Reference to the Consultation Paper and draft PDP (Amendment) Bill (emphasis ours)	SGX's Comments
1.	Paragraph 22 of the Consultation Paper and Clause 12 of the draft PDP (Amendment) Bill. *"Duty to conduct assessment of data breach* *26C.—(1) Subject to subsection (2), where an organisation has reason to believe that a data breach has occurred affecting personal data in its possession or under its control, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach.* *… …* *(3) The organisation must carry out the assessment mentioned in subsection (1) in accordance with any prescribed requirements.* *Duty to notify occurrence of notifiable data breach* *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.* *(2) Subject to subsections (4), (6) and (7), the organization must also notify, on or after notifying the Commission under subsection (1), each affected individual to whom significant harm results or is likely to result from a notifiable data breach in any manner that is reasonable in the circumstances.* *… …* *(4) Subsection (2) does not apply to an organisation in relation to an affected individual if the organisation takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.* *(5) Without limiting subsection (4), subsection (2) does not apply to an organisation in relation to an affected individual if the organisation had implemented, prior to the occurrence of the notifiable data breach, any technological measure*	We note that the remedial action and technological protection exceptions ("**Relevant Exceptions**") apply to the requirement to notify affected individuals under Section 26D(2) and (4), Clause 12 of the draft Bill. As the Relevant Exceptions are afforded on the basis that the remedial action and technological protection taken and implemented by the organisation will render it unlikely that the data breach will result in significant harm to the affected individual, the Relevant Exceptions should similarly apply to the requirement to notify the PDPC. This could be provided for in Section 26C(3), Clause 12 of the draft Bill.

No.	Reference to the Consultation Paper and draft PDP (Amendment) Bill (emphasis ours)	SGX's Comments
	that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual. *… …"*	
2.	Paragraph 38b of the Consultation Paper and Clause 7 of the draft PDP (Amendment) Bill. *"Deemed consent by notification* *15A.—(1) Subject to subsection (2), an individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation if —* *(a) the organisation satisfies the requirements in subsection (3); and* *… …* *(3) For the purposes of subsection (1)(a), the organization must, before collecting, using or disclosing any personal data about the individual —* *… …* *(b) take reasonable steps to bring the following information to the attention of the individual:* *(i) the organisation's intention to collect, use or disclose the personal data;* *(ii) the purpose for which the personal data will be collected, used or disclosed;* *(iii) a reasonable period within which, and a reasonable manner by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure of the personal data.* *… …*	With reference to Section 15A, Clause 7 of the draft Bill, we would be grateful if the PDPC could provide guidance (e.g. in the advisory guidelines) on the following matters proposed in the draft Bill: - What would be deemed reasonable steps to be taken by an organisation in bringing the stipulated information to a relevant individual? - What would be considered a reasonable period within which, and a reasonable manner by which, an individual may notify the organisation that the individual does not consent to the organisation's proposed personal data processing?
3.	Paragraph 58 of the Consultation Paper. *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 <u>in Singapore</u>; or (ii) S$1 million, whichever is higher.* Clause 17 of the draft PDP (Amendment) Bill.	We note that paragraph 58 of the Consultation Paper states, *inter alia*, that the maximum financial penalty will be increased to up to 10% of an organisation's annual gross turnover <u>in Singapore</u>. The limitation to Singapore-based turnover should be reflected in Section (2A), Clause 17 of the draft Bill.

No.	Reference to the Consultation Paper and draft PDP (Amendment) Bill (emphasis ours)	SGX's Comments
	"(2A) For the purposes of subsection (2)(*d*), the amount of the financial penalty must not exceed — (*a*) where the direction is given to an organisation or a person with an annual turnover exceeding $10 million (as ascertained from the most recent audited accounts of the organisation or person available at the time the direction is given), and the failure to comply that is the subject of the direction occurs on or after the date of commencement of section [17] of the Personal Data Protection (Amendment) Act 2020 — 10% of the annual turnover; or (*b*) in any other case — $1 million.".	
4.	Paragraph 72 of the Consultation Paper and Clause 19 of the draft PDP (Amendment) Bill. *"MCI/PDPC will introduce a requirement for organisations to preserve personal data requested pursuant to an access request (or a copy) for a prescribed period of (a) at least 30 calendar days after rejection of the request, or (b) until the individual has exhausted his/her right to apply for a reconsideration request to PDPC or appeal to the Data Protection Appeal Committee, High Court or Court of Appeal, whichever is later. This will help to preserve the availability of a meaningful remedy should the individual succeed in his/her application. MCI/PDPC will similarly require preservation of personal data requested pursuant to a data porting request. "*	The draft Bill introduces a requirement for organisations to preserve personal data requested pursuant to an access request for a prescribed period after rejection of the request, or until the individual has exhausted his/her right to apply for a reconsideration request to PDPC or appeal to the Data Protection Appeal Committee, High Court or Court of Appeal ("**Request/Appeal**"), whichever is later. As an organisation may not have the unilateral means of ascertaining if a Request/Appeal is pending or if the individual intends to seek a further Request/Appeal, we propose that the onus be placed on the individual to notify the organisation of the status of the Request/Appeal. In line with our proposal above, we also propose the following mechanisms for MCI/PDPC's consideration: - After an organisation has been notified by the individual of a Request/Appeal, the organisation could be required to extend the preservation period for a prescribed period of time (e.g. 180 days). - If the individual notifies the organisation, prior to the expiration of the prescribed period, of the pendency of the

No.	Reference to the Consultation Paper and draft PDP (Amendment) Bill (emphasis ours)	SGX's Comments
		Request/Appeal or the intent to commence a fresh Request/Appeal, the prescribed period (e.g. 180 days) would be refreshed. - If the individual fails to notify the organisation prior to the expiration of the prescribed period, the organisation should be entitled to destroy the personal data in accordance with its usual data retention policies.
5.	Paragraph 76 of the Consultation Paper. *"For the reasons provided above in paragraphs 48 and 49, MCI/PDPC will provide an exception for "derived personal data" to the Correction Obligation. "Derived personal data" will also be excluded from the Data Portability Obligation. To ensure organisations remain accountable for personal data in their possession or under their control, organisations will still be required to provide individuals with access to derived personal data. Organisations are to also provide the individual with information about the ways in which the derived personal data has been or may have been used or disclosed by the organisation within a year before the date of the request."*	We note that paragraph 49 of the Consultation Paper states that derived personal data will not be subject to the Data Portability Obligation, in a bid to protect business innovation and investments by organisations. We are in support of this. Paragraph 76 of the Consultation Paper further states that organisations will be required to provide individuals with access to derived personal data. We understand the underlying accountability rationale. However, we propose that individuals be prohibited from abusing this access right. In particular, individuals should be prohibited from subsequently sharing such data with other organisations for commercial gain. This is in line with the objective of protecting business innovation and investments by organisations.
6.	Clause 6 of the draft PDP (Amendment) Bill. *"Amendment of section 15* *6. Section 15 of the principal Act is amended by inserting, immediately after subsection (2), the following subsections:* *"(3) Without limiting subsection (2) and subject to subsection (5), an individual (P) who provides personal data to an organisation (A) with a view to P entering into a contract with A is deemed to consent to the following:*	We propose that the wording of Clauses 6 and 13 of the draft Bill be clarified such that they read conjunctively (i.e. "and").

No.	Reference to the Consultation Paper and draft PDP (Amendment) Bill (emphasis ours)	SGX's Comments
	(a) the disclosure of that personal data by A to another organisation (B), where the disclosure is reasonably necessary for the conclusion of the contract between P and A; *(b) the collection and use of that personal data by B, where the collection and use is reasonably necessary for the conclusion of the contract between P and A;* *(c) the disclosure of that personal data by B to another organisation where the disclosure is reasonably necessary for the conclusion of the contract between P and A."* Clause 13 of the draft PDP (Amendment) Bill. *"… …* *Porting of applicable data* *26G.—* *… …* *(3) Subsection (2) applies only if the following are satisfied:* *(a) the data porting request satisfies any requirements prescribed;* *(b) the porting organisation, at the time it receives the data porting request, has an ongoing relationship with the individual.* *… …"*	

CONCLUSION

SGX is generally supportive of these proposed legislative changes and the purposes to which they relate. We express our thanks to MCI/PDPC for the opportunity to comment on this Consultation Paper.