Credit Bureau Singapore

28 May 2020

Ministry Of Communications And Information
Personal Data Protection Commission
(via email: DataRegulation@mci.gov.sg)

Dear Sir / Madam,

Public Consultation for the PDP (Amendment) Bill

We refer to the above-mentioned Public Consultation dated 14 May 2020 and wish to submit our views on the proposed amendment.

Please find our feedback in the Annex below for your consideration.

Thank you.

Yours sincerely,

Candy Yeap
Data Protection Officer

Encl. Annex

Annex

Feedback on the Public Consultation for the PDP (Amendment) Bill

Paragraph No.	Description of Paragraph	CBS' Comments
16	Notification criteria: "… (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 *(data breaches affecting 500 or more individuals)*. Organisations will also be required to notify affected individuals if the data breach is likely to result in significant harm to them…" Assessment and notification timeframes: "… notify PDPC as soon as practicable, no later than three calendar days after the day the organisation determines that the data breach meets the notification criteria…"	Before the notification / proclaim of a data breach which has occurred, organisation(s) may require long period (e.g. months) to investigate the breach upon detecting any sign of the compromise. As such, it is necessary for PDPC to provide guidance / establish a timeframe for organisation to expedite the assessment of the breach's full impact and determine the eligibility to notify the PDPC. This may then effectively complement the notification criteria stipulated. With respect to notifying the individuals affected by data breach of a significant scale, there may be operational issues involved. Currently, individuals have the option to not provide mobile numbers and/or email to prevent the possibility of receiving marketing materials. Without such personal data, it is onerous to notify these affected individuals via snail mail if a data breach occurs. CBS would like to feedback that the communication mode, speed and cost should be considered to notify such large scale of individuals.
21	Where a data breach is discovered by a data intermediary ("DI") that is processing personal data on behalf of and for the purposes of an organisation, the DI is required to notify the organisation without undue delay from the time it has credible grounds to believe that a data breach has occurred.	Being an approved and controlled data intermediary for the purposes of creating and providing commercial and individual credit reports, CBS relies on data provided by the sources. CBS agrees with the requirement to notify organisation(s) in which CBS processes personal data on behalf of and for the purposes of the organisation(s). However, similar to the above points highlighted, it is important that DI investigates and ascertains the full impact of a breach before notification to organisation(s). Given the scale of

Paragraph No.	Description of Paragraph	CBS' Comments
		personal data currently held by CBS, it is worth noting that long investigation period is reasonably needed.
32	Employees acting in the course of their employment, in accordance with their employer's policies and practices, or whose actions are authorised by their employers, will not run the risk of such criminal sanctions.	CBS agrees that employers are still primarily liable to protect and account for personal data in its possession or under its control. This would mean that employers should enforce awareness and education of data protection within the organisation. Placing a responsibility on each employee, unless acting on behalf of employers, stresses the importance of data protection and that each role within organisation plays a part in protecting personal data collected, accessed, used and disclosed.
35	In line with the PSDSRC's recommendation for such individuals to be held liable for criminal penalties similar to those under the PSGA, 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.	
40	In addition, to cater to situations where there are larger public or systemic benefits where obtaining individuals' consent may not be appropriate, two new exceptions to the consent requirement will be introduced.	CBS has no issue to the introduction of new exceptions to the consent requirement due to the collection, usage and disclosure purposes stipulated for credit bureau under Section 5 Sub-paragraph 6 of First Schedule Part 3. Nevertheless, we have consent and notification established. Also, CBS is already exempted from any withdrawal of consent with regards to personal data of individuals and companies associated with the individual collected. Under the business improvement exception, it will allow CBS to develop more augmented products for banks to make more informed and accurate credit assessment on individuals and companies associated with the individual. It helps to also provide more insightful data analytics to be produced as traditional credit information and alternative data can be combined to strengthen business intelligence for a more proactive, customer-centric approach to account

Paragraph No.	Description of Paragraph	CBS' Comments
		acquisition, relationship management and risk mitigation. Regardless of the alternative data introduce in near future, CBS shall perform strenuous and continuous testing before adoption as it may "contaminate" the existing score attributes which are ascertained to be predictive. The primary data domain i.e. CBS data must be used as a foundation and any introduction of alternative data will be incrementally calibrated for potential use.
47	To provide greater certainty for compliance, the Data Portability Obligation will only come into effect with the issuance of Regulations. The Regulations will prescribe requirements that apply to the porting of specific datasets. PDPC will work with the industry and relevant sector regulators to develop the requirements to be prescribed in the Regulations.	Referring to the proposed Part VIB – Data Portability, CBS would like to clarify on the extent of responsibility by data intermediary on data portability obligations which it is currently omitted in this proposed regulation. In PDPC's response to feedback for 3rd Public Consultation on Data Portability and Data Innovation Provisions issued on 20 Jan 2020, it was mentioned that "the proposed Data Portability Obligation would not apply to a data intermediary in relation to data that it is processing on behalf and for the purposes of another organisation". To recap, our feedback submitted highlighted the potential significant issues arising from data portability requests for a credit bureau. These included a fragmented database, inability to manage data disputes, loss of data, forum shopping by data subjects, and eventually increased cost for end users etc.
74	Currently, organisations are prohibited from providing access to personal data where it reveals the personal data about another individual or it reveals the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to	CBS generally agrees with the proposed criteria to prohibit the provision of access to personal data. However, given the sensitivity of personal data CBS stores as a data intermediary, CBS would like to feedback the detrimental effect of providing access to personal data where it reveals the personal data about another individual or it

Paragraph No.	Description of Paragraph	CBS' Comments
	the disclosure of his/her identity. From PDPC's experience, this has resulted in implementation issues for organisations providing access to personal data (e.g. removing third parties' personal data captured in CCTV footage). To ensure alignment with the Data Portability Obligation and for the reasons provided above in paragraph 46, MCI/PDPC will amend section 21 of the PDPA to reduce the scope of prohibitions to access in relation to user provided and user activity data. The amendment will allow organisations to provide access to such data, regardless of whether providing access could (i) reveal personal data about another individual, or (ii) reveal the identity of an individual who has provided personal data about another individual and that individual does not consent to the disclosure of his/her identity.	reveals the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his/her identity. Currently, CBS only accepts request to access own personal data from the requesting individual (A). Further access to another individual's personal (B) data must be authorised by (B) himself prior to disclosure to (A). This access may not threaten the safety or physical or mental health of an individual other than the individual who made the request; or cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request. But CBS still prudently applies the concept of access and disclosure of own personal data to the requesting individual only. With the amendment to allow CBS to provide access to such data, regardless of revealing about another individual, it may cause requesting individual (A) to identify (B) and able to analyse his behaviour in areas such as credit worthiness and payment background. Example such as clear and visible quality of CCTV footage is easily able to obtain personal data of (B) once provided access to (A).