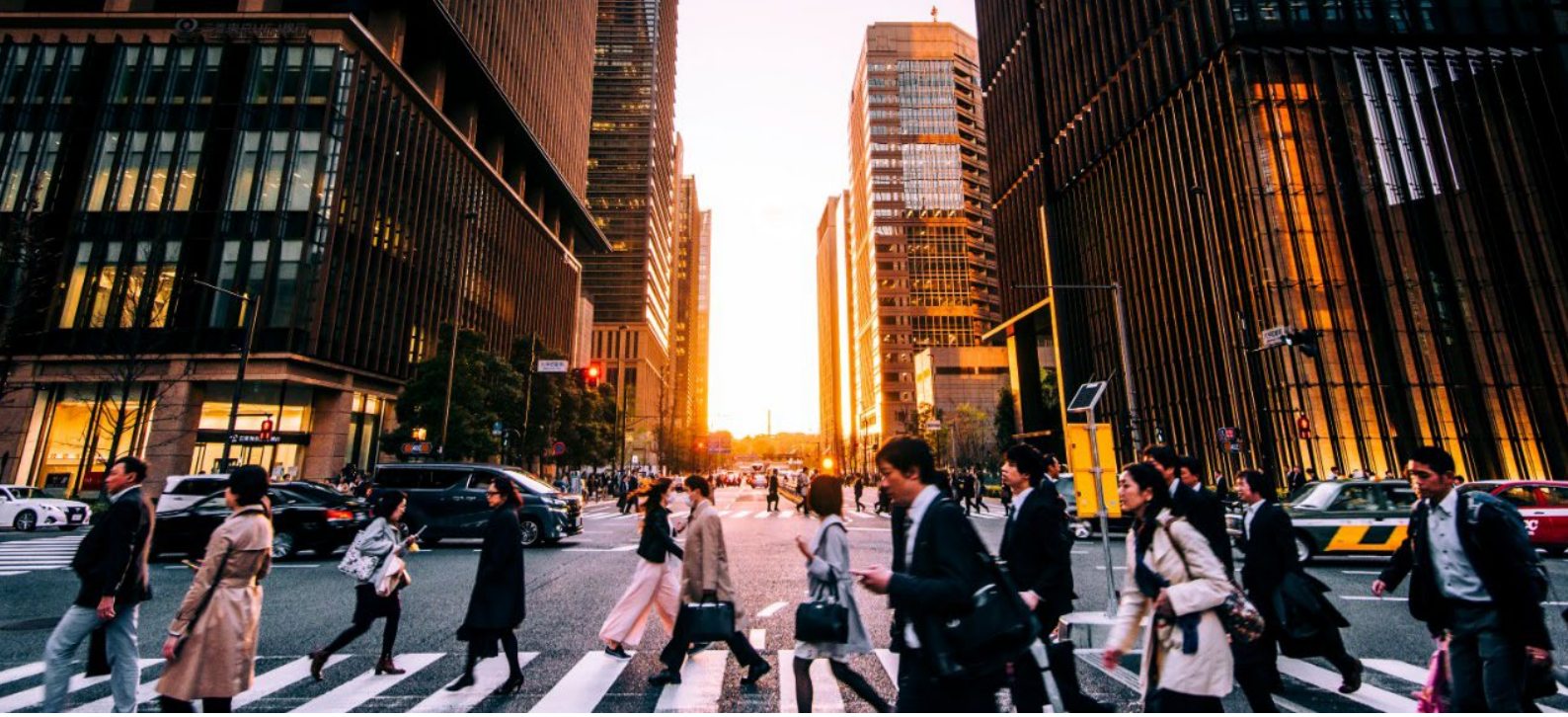

Update on the Personal Data Protection (Amendment) Bill 2020

November 2020

Introduction

Since the enactment of Singapore's Personal Data Protection Act 2012 (the "**PDPA**") on 1 January 2013, Singapore's digital landscape and economy have evolved tremendously and technology have also changed the way data is collected and analysed.

To keep pace with technological advances, the Ministry of Communications and Information (the "**MCI**") and the Personal Data Protection Commission ("**PDPC**") have released the Personal Data Protection (Amendment) Bill 2020 (the "**Bill**") for public consultation earlier this year and the Parliament has passed the Bill on 2 November 2020, though it is not yet clear when the amendments will come into effect. The Bill represents the first comprehensive review of the PDPA since it was enacted.

Below, we discuss four key changes proposed under the Bill, and in particular, the shift of the Singapore regulatory framework towards a risk-based, accountability approach to better protect consumers while balancing the need to provide clear regulations and guidance to promote the continued development of the digital economy and business efficacy in Singapore.

1. Mandatory data breach notifications

The Bill proposes a new mandatory data breach notification regime which imposes an obligation on organisations to conduct assessments of potential data breaches and notify affected individuals and the PDPC when a data breach has occurred. In this context, a "data breach" is defined as any unauthorised access, collection, use, disclosure, copying, modification, disposal of personal data, or loss of any storage medium or device on which personal data is stored.

When is data breach notifiable?

In all cases, if an organisation has "reason to believe" that a data breach has occurred, it must conduct an assessment on whether the breach is notifiable. A data breach is notifiable under the following circumstances:

(a) it results in, or is likely to result in, "significant harm" to affected individuals; and

(b) it affects more than the prescribed number of individuals. The PDPC has commented that 500 or more individuals would be an appropriate threshold.

The MCI and PDPC have clarified that the classes of data which would be considered likely to cause significant harm if they are the subject of a data breach will be laid out in future regulations. Such classes may include, identification numbers, drivers' licence numbers and credit/debit card numbers.

If the personal data is processed by a data intermediary acting on behalf of the organisation, the data intermediary would have an obligation to notify the organisation "without undue delay" from the time it has credible grounds to believe that a data breach has occurred, but the obligation to conduct an assessment of whether the breach is notifiable remains with the organisation.

Who must be notified?

The PDPC**:** In the event that the criteria for notifying PDPC are met, the organisation must notify the PDPC of the breach as soon as practicable, and no later than 3 calendar days after the day the organisation determines that the data breach meets the notification criteria.

Affected individuals: In addition to notifying the PDPC, organisations must also notify, as soon as practicable, individuals affected by data breaches if the data breach is likely to result in significant harm. However, organisations are not required to notify affected individuals in the following circumstances:

(a) The remedial action exception: If the organisation has taken remedial actions in accordance with the prescribed requirements, such that the data breach is unlikely to result in significant harm to the affected individuals;

(b) The technological protection exception: If the organisation has implemented technological measures (e.g. encryption), such that the data breach is unlikely to result in significant harm to the affected individuals; or

(c) Direction from PDPC / other prescribed authority: The PDPC or any other prescribed authority, may direct the organisation not to notify an affected individual. This is intended to cater to circumstances where notification to affected individuals may compromise any investigations or prejudice any enforcement efforts under the law.

2. Expanded scope of situations where consent is deemed to have been given

Obtaining consent was one of the key principles that underpinned the data protection rules in the PDPA when it was initially enacted in Singapore. However, MCI and PDPC have stated that they believe it is now necessary to recalibrate the balance between the organisational accountability to harness data for appropriate and legitimate purposes and the individual's consent. The Bill updates the framework for obtaining consent under the PDPA, with the aim of ensuring meaningful consent by individuals, while still safeguarding their interests by introducing new accountability measures for organisations.

2 new categories of deemed consent

Currently under the PDPA, an individual's consent is deemed to have been given for a particular purpose when he / she has voluntarily provided the personal data and it is reasonable that the individual would do so. The Bill introduces two more situations where consent will be deemed to have been given:

(a) Consent may be deemed by contractual necessity: If the individual provides personal data to an organisation with a view of entering into a contract with them, the individual is deemed to also have consented to the collection, use or disclosure which are "reasonably necessary" to conclude or perform the contract;

(b) Consent may also be deemed by notification: If the organisation determines that their proposed use for an individual's personal data is not likely to have an adverse effect on the individual following measures implemented to eliminate, reduce the likelihood of or mitigate the identified adverse effect to the individual, and the individual has been notified of the intention and purpose for the collection, use or disclosure of his/her personal data, the individual is deemed to have consented to the collection, use or disclosure of the personal data, provided that the individual has not notified the organisation of his / her intention to opt-out.

2 new exceptions to the consent requirement

The Bill also introduces two new exceptions to the consent requirement: the legitimate interests and business improvement exceptions.

"Legitimate interests" exception

The "legitimate interests" exception applies to the collection, use, and disclosure of personal data when:

(a) it is in the "legitimate interests" of the organisation; and

(b) the benefit to the public (or any section thereof) is greater than any adverse effect on the individual.

To rely on this exception, an organisation must conduct an assessment of whether the above requirements have been satisfied and inform individuals' of its reliance on the exception to collect, use, or disclose personal data without obtaining consent.

"Business improvement" exception

The "business improvement" exception only applies to the use of personal data. Under this exception, consent is not required when personal data is used for:

(a) operational efficiency and service improvements;

(b) developing and enhancing products or services; and

(c) knowing the organisation's customers.

Following feedback received by the public, the MCI and the PDPC have clarified that the business improvement exception shall also apply to the collection, use and disclosure of personal data by related corporations within a group, with additional safeguards, so as to allow companies to leverage data for business improvement purposes within a group.

Revisions to existing exceptions to the consent requirement

"Research" exception

Under the existing provisions of the PDPA, an organisation may use or disclose personal data about an individual without express consent where the personal data is generally used or disclosed for a research purpose, subject to certain safeguards. The Bill proposes to remove certain restrictions on the *use* of personal data for research purposes so that the organisation may carry out research for purposes beyond improving business products or services (such as scientific research and developments) but the *disclosure* of personal data will continue to be subject to the stringent condition of impracticality and an additional condition that the benefits to be derived from the disclosure are clearly in the public interest.

"Business asset transaction" exception

Under the existing provisions of the PDPA, an organisation which is undertaking a "business asset transaction", defined as the purchase, sale, lease, merger or amalgamation or any other acquisition, disposal or financing of an organisation or a portion of an organisation, may disclose personal data of its employees, customers, directors, officers or shareholders without obtaining consents from the individuals.

This exception will be amended to include the disclosure of personal data of independent contractors as well, and the Bill has further clarified that this exception will be extended to include transactions such as mergers and acquisitions, sale of shares, transfer of controlling power or interests, corporate restructuring and reorganisations in cases that involves "an interest in an organisation" or amalgamations with or transfers to related corporations.

3. Increased financial penalties and new offences affecting individuals

Increased financial penalties and scope of PDPC's power to give directions

Currently, the PDPC may give any or all of four directions to an organisation which has failed to comply with any provision related to data protection, including a direction to pay a financial penalty not exceeding $1 million. Under the Bill, the maximum financial penalty has been increased to either 10% of the company's annual turnover in Singapore, if its annual turnover exceeds $10 million; or $1 million, whichever is higher.

Additionally, the PDPC will be given expanded powers to give directions for a failure to comply with the Do-Not-Call ("**DNC**") Registry provisions and the new Data Portability provisions. The PDPC intends to have tiered financial penalty caps for breaches of the DNC provisions, aligned with the egregiousness of the breach.

New offences affecting individuals

Three new offences relating to acts committed by individuals have also been introduced under the Bill 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. These offences may apply when an individual either knowingly or recklessly:

(a) make an unauthorised disclosure of personal data;

(b) make an unauthorised use of personal data for a wrongful gain or a wrongful harm or loss to any person; or

(c) make an unauthorised re-identification of anonymised information.

Individuals found guilty of any of these offences face a maximum sentence of a fine not exceeding $5,000 or imprisonment for a term not exceeding 2 years or both.

4. New data portability obligation for organisations

The Bill also introduces a data portability obligation for organisations with the intention for consumers to be provided greater autonomy over their personal data.

Under the new obligation, individuals may request organisations to transmit or "port" their personal data to other organisations in a commonly used machine-readable format, and organisations receiving such requests must abide by

them. Where an organisation refuses a data porting request, it must inform the individual of the reason of the refusal within a reasonable time, which will be subject to the PDPC's review.

However, certain requirements must be met before the organisation's obligation to port data arises – chiefly, the request must relate to the individual's "user activity data or user-provided data" held in electronic form, the receiving organisation must have a presence in Singapore, and the 'porting' organisation must have an ongoing relationship with the individual.

The MCI and PDPC intend for exceptions to this obligation to be laid out in future Regulations, including prescribing a 'whitelist', technical and process details, the relevant data porting request models, and safeguards for individuals.

Takeaways

The major changes summarised in this article will represent key changes to the PDPA since its enactment in 2012, particularly as Singapore seeks to recover from the economic impact from the COVID-19 pandemic.

Therefore, it was comforting to note from the Closing Note to Public Consultation that the MCI and PDPC have recognised that the prevailing global economic situation means that any substantial fines under the revised data protection framework may result in even greater financial hardships for organisations. They have also clarified that notwithstanding the higher penalty caps, PDPC will continue to be circumspect and be guided by the specific facts of each case before deciding on a financial penalty that will be proportionate to the level of seriousness of the breach and the level of culpability of the organisation.

Nevertheless, organisations should note that the Bill has been passed by the Parliament, though it is not yet clear when the amendments will come into effect. In view of the upcoming changes to the PDPA, organisations should start actively getting ahead of the curve and consider reviewing their existing data protection policies and data breach management and response plans to ensure that they are compliant with the proposed changes to the PDPA.

Contact Details

If you should have any queries, please do not hesitate to contact any of us:

Rachel Eng
Managing Director
+65 6597 3343
rachel.eng@mail.engandcollc.com

Vincent Tan
Associate Director
+65 6597 3334
vincent.tan@mail.engandcollc.com

Andrew Heng
Associate Director
+65 6597 3348
andrew.heng@mail.engandcollc.com