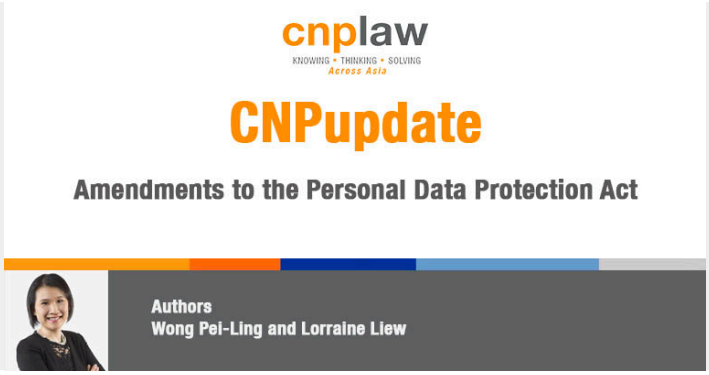
AMENDMENTS TO THE PERSONAL DATA PROTECTION ACT

Posted on January 29, 2021



Category: CNPupdates

Authors: Wong Pei-Ling and Lorraine Liew.

The Personal Data Protection (Amendment) Bill ("**Amendment Bill**") was passed by Parliament on 2 November 2020, the first update to the legislation since the Personal Data Protection Act 2012 ("**PDPA**") came into force in 2014. The effective date of the Amendment Bill has yet to be determined although it is expected to be implemented in phases in 2021.

The amendments to the PDPA sought to strike a balance between consumers and organisations in the collection, use and disclosure of personal data in Singapore. While the Amendment Bill recognizes that consumers must be confident in knowing that their personal data will be kept secure and used responsibly, organisations ought to be allowed to harness personal data for legitimate business and other purposes as long as they comply with the requisite safeguards and maintain accountability.
Several key amendments are as follows:

Mandatory obligation to assess and notify the Personal Data Protection Commission ("Commission") of data breach

The Guide to Managing Data Breaches 2.0 issued by the Commission ("**Guide 2.0**") stipulates that a data breach as "*an incident exposing personal data in an organisation's possession or under its control to the risks of unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks*".

Under the amended PDPA, an organisation that has reason to believe that a data breach affecting personal data in its possession or under its control has occurred must conduct, in a reasonable and expeditious manner, an assessment of the extent and impact of the data breach and whether the data breach is a notifiable data breach. As to what amounts to a notifiable data breach, the current Guide 2.0 recommends that an organisation notifies the Commission and/or affected individuals of a data breach where the breach

is likely to result in significant harm or impact to the individuals to whom the information relates or is of a significant scale (for example, where the data breach involves the personal data of 500 or more individuals). The Commission in the draft Advisory Guidelines on the Key Provisions of the PDPA (Amendment) Bill acknowledges that while there may be varying circumstances that would affect the time taken to establish the facts of a data breach and determine whether it is notifiable, organisations should generally do so within thirty (30) days. An organization must also document all steps taken in assessing the data breach, to demonstrate that "reasonable and expeditious" steps were taken to determine whether the data breach is notifiable.

A data intermediary that possesses personal data on behalf of and for the purposes of another organisation or public agency must, without undue delay, notify the organisation or public agency of the occurrence of a data breach from the time it has credible grounds to believe that the data breach has occurred, to ensure that the organisation is informed of the data breach in a timely way, and is able to decide on the immediate actions to *inter alia*, contain the data breach and conduct an assessment on whether to notify the Commission of the data breach.

Where the organization has determined that the data incident is a notifiable data breach, the organization must report the data breach to the Commission as soon as possible, and in any event no later than **three (3) days** after the assessment is made if the conclusion is that the breach (i) results in, or likely to result in, significant harm to an affected individual or (ii) is, or is likely to be, of a significant scale.

The organisation must also on or after notifying the Commission, notify each affected individual, unless one of the exceptions apply. Exceptions to the data breach notification requirement include but are not limited to cases where the organisation has assessed that it is unlikely that the data breach will result in significant harm to the affected individual, and remedial action has been taken by the organisation to contain the breach or to prevent a repeated occurrence.

Obligation for data portability

In order to give individuals greater autonomy and control over their personal data and to facilitate innovation and more intensive use of applicable data to promote competition between goods and service providers, individuals may give a request to a porting organisation to transmit their personal data to a receiving organisation but this obligation will only apply to certain classes of applicable personal data.

There are excluded types of data and also excluded circumstances specified in the Amendment Bill, and it is specifically stated that a porting organisation must not transmit the requested data if it can reasonably be expected to (i) threaten the safety, or physical or mental health of other individuals; (ii) cause immediate or grave harm to the safety, or physical or mental health, of the individual; or (iii) be contrary to the national interest.

New offences, increased financial penalties and alternative dispute resolution

New offences holding individuals, which may include employees, personally accountable for unauthorised disclosure, improper use or unauthorised re-identification of anonymised information have been introduced. For each of these offences, upon conviction the individual shall be liable to a fine not exceeding $5,000 or imprisonment for up to 2 years, or both.

The maximum penalty for data breaches has been raised for large organisations with annual turnovers exceeding S$10 million. For example, in the case of a contravention of section 24 of the PDPA (the obligation to protect personal data by making reasonable security arrangements) by an organisation whose annual turnover in Singapore exceeds $S10 million under the amended PDPA shall be 10% of the organisation's annual turnover in Singapore (as compared to a maximum of S$1 million).

The Commission may accept written voluntary undertakings from an organisation in breach, if the organisation provides them. Such undertakings may include taking specified action within a specified time, refraining from taking specified actions and publicizing the undertaking.

In cases where the Commission is of the opinion that a complaint by an individual may be more appropriately resolved by mediation, the Commission may refer the matter to mediation without the consent of the parties.

Changes to "deemed consent" and enhanced exceptions to the consent requirement

Under the current PDPA, an individual has not given consent unless he has been notified of the purposes for which his personal data will be collected, used or disclosed, and the individual has provided his consent for those purposes. Consent may be express or deemed.
The Amendment Bill introduces two new forms of "*deemed consent*":

Consent may now be deemed by contractual necessity
The amendment will provide greater leeway for disclosure of personal data by one organisation to another organisation in order to complete a contract with a customer. Deemed consent under the new section 15(3) extends to a situation where an individual provides his personal data to one organisation ("**A Co**") for a transaction, and it is reasonably necessary for A Co to disclose his personal data to another organization ("**B Co**") for the performance of the contract between A Co and the individual. Deemed consent by contractual necessity now extends the disclosure to another downstream organization ("**C Co**") where the disclosure (and collection) is reasonably necessary to fulfil the contract between A Co and the individual. However, the amended PDPA requires that the organisation (in this case A Co), before collecting, using or disclosing any personal data, conduct an assessment to determine that such collection, use or disclosure is not likely to have an adverse effect on the individual and 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; and (iii) a reasonable period within which, and a reasonable manner by which, the individual may notify the organisation that he does not consent to the proposed collection, use or disclosure.

Consent may also be deemed by notification:

An individual may be deemed to have consented to the collection, use or disclosure of personal data for a purpose that he has been notified of, and he has not taken any action to opt out of the collection, use or disclosure of his personal data, thus allowing an organisation (who wishes to use or disclose existing data for a secondary purpose that is different from the primary purpose for which the organisation had originally collected the personal data), to use the personal data for the organisation's secondary purpose. However, this is subject the organisation assessing and determining that certain conditions have been met - for example, conducting an assessment to determine if the proposed collection, use or disclosure of personal data is not likely to have an adverse effect on the individual, taking into consideration the method of notification and measures to eliminate, reduce or mitigate identified adverse effects. An organisation must also ensure that the notification provided to the individual is adequate and allow for a reasonable period within which the individual can opt out of the collection, use or disclosure of his personal data. The Commission recognises that there are various ways of implementing the opt-out method and will consider the circumstances and facts of each case in determining whether the conditions for relying on deemed consent by notification have been met.

Enhanced Exceptions

An individual's consent need not be obtained for collection, use and disclosure in certain cases where it is in the "*legitimate interests*" of the organisation or another person, subject to restrictions and conditions as stated in the amended PDPA, such as conducting an assessment to eliminate or reduce risks associated with the collection, use or disclosure of personal data. An organisation that relies on the "*legitimate interests*" exception to collect, use or disclose personal data must make it known to the affected individuals that the organisation is relying on this exception to collect, use and disclose their personal data. One example provided by the Commission was in the context of the collection and use of personal data on company-issued devices to prevent data loss by the installation by the organisation of a data loss prevention software to detect any unauthorized data leakage, disclosure or loss of the organisation's information.

An organisation may also rely on the "*business improvement*" exception to use personal data that it has collected in accordance with the PDPA, to increase operational efficiency, develop new products, improve or enhance its services. However, this exception may only be relied upon for such purposes that a reasonable person may consider appropriate in the circumstances and where such purposes cannot be achieved without use of the personal data. The "*business improvement*" exception also applies to the sharing of personal data between entities within a group. For example, personal data is shared to enable the learning or understanding of behaviour and preferences of existing or prospective customers (including groups segmented by profiles) or identifying, personalizing or customizing goods or services that may be suitable for existing or prospective customers.

Other changes and what organisations should strive for

In addition to the amendments highlighted above, the Amendment Bill introduced other changes including

the removal of the exclusion from the PDPA for agents of the Government and updates to strengthen the "Do Not Call" regime.

Whilst several of the new amendments have previously been introduced in the form of advisory guidelines issued by the Commission, in light of the changes to the PDPA (including increased financial penalties), organisations should be prepared to review their current privacy policies and processes for compliance with the amended PDPA, if they have not already done so. This would include reviewing and enhancing their IT security system and processes to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal of personal information. It will also be necessary to review current consent collection and notification procedures, and SOPs for data breach incident management, remediation and notification.

Update (4 February 2021): It has been announced by the PDPC that the above amendments to the PDPA will take effect in phases, beginning from 1 February 2021. Read the updated version here.