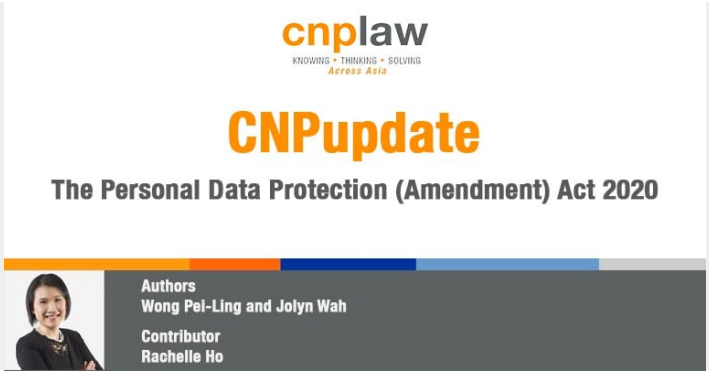
THE PERSONAL DATA PROTECTION (AMENDMENT) ACT 2020

Posted on March 31, 2021



Category: CNPupdates

Authors: Wong Pei-Ling and Jolyn Wah.

Contributor: Rachelle Ho.

The Personal Data Protection (Amendment) Act 2020 (No. 40 of 2020) ("**PDPA Amendments**") was passed by Parliament in November 2020 and came into effect on 1 February 2021. The PDPA Amendments amend the Personal Data Protection Act 2012 (No. 26 of 2012) ("**PDPA**"), which is the primary legislation regulating the collection, use and disclosure of personal data in Singapore.

This article provides an update on the key aspects of the PDPA Amendments, which will be implemented in phases in 2021, beginning 1 February 2021. Several of the key amendments which are now in force are as follows:

Mandatory Data Breach Notification

Effective 1 February 2021	Pre-Amendment under the PDPA	Post-Amendment
Notification of data breach	Breach notification was voluntary, and was recommended by the Personal Data Protection Commission ("**PDPC**") through guidelines issued by the PDPC.	Organisations (i.e. data controllers) must conduct, in a reasonable and expeditious manner, an assessment of whether a data breach affecting personal data in its possession or under its control amounts to a notifiable data breach. Organisations must notify[2] the PDPC as soon as reasonably practicable, but in any case, no later than 3 calendar days after making the assessment that a notifiable data breach has occurred i.e. the breach[3]: (a) results in, or is likely to result in, significant harm to an affected individual[4]; *(i.e. an individual's full name/alias/ID number and prescribed personal data or account identifier and information used to access an individual's account with an organisation are disclosed)*; or (b) is, or is likely to be, of a significant scale, (*i.e. it involves the personal data of 500 or more individuals*[5]). The Personal Data Protection (Notification of Data Breaches) Regulations 2021 provides examples of what amounts to a data breach that is deemed to result in significant harm to an individual[3a.] On or after notifying the PDPC, the organisation must also notify the affected individuals if the notifiable data breach results in, or is likely to result in significant harm to the affected individuals. This is subject to several exceptions. For example, the organisation need not notify an affected individual if the organisation (i) on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual, or (ii) had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual. Where a data intermediary (i.e. a data processor) has reasons to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation, the data intermediary must also notify that other organisation of the occurrence of the data breach without undue delay.[6]

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

New basis for deemed consent to apply for collection, use and disclosure of personal data		
Effective 1 February 2021	**Pre-Amendment**	**Post-Amendment**
Deemed consent by contractual necessity	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 expressed or deemed only by the individual's conduct.	Deemed consent by contractual necessity[7] is introduced. If an individual gives or is deemed to have given his consent to the disclosure of personal data about that individual to one organisation A with a view to the individual entering into a contract with organisation A, the individual is deemed to consent to the disclosure of the personal data by organisation A to organisation B and the collection, use or disclosure of personal data by organisation B, where disclosure of the personal data is reasonably necessary for the conclusion of a contract entered into between the individual and organisation A. This however, does not affect any obligation under the contract between the individual with the organisation A that restricts the personal data that organisation A may disclose to another organisation.
Deemed consent by notification		Deemed consent by notification[8] is introduced. An individual may be deemed to have consented to the collection, use or disclosure of personal data by an organisation for a purpose that the organisation had taken reasonable steps to bring to his attention, and he has not taken any action to notify the organisation, within a reasonable period provided by the organisation, that he or she does not consent to the organisation's proposed collection, use or disclosure of his or her personal data. Deemed consent by notification does not apply to, amongst other things, the sending of direct marketing messages.[9] An organisation must, before collecting, using or disclosing any personal data about the individual, (a) conduct an assessment to determine that the proposed collection, use or disclosure of personal data is not likely to have an adverse effect on the individual, and (b) take reasonable steps to bring to the attention of the individual: (i) the organisation's intention to collect, use or disclose the personal data, (ii) the purpose for such collection, use or disclosure, and (iii) allow for a reasonable period within which and a reasonable manner by which, the individual may notify the organisation that he or she does not consent to the proposed collection, use or disclosure of the personal data.

New consent exceptions for collection, use and disclosure of personal data		
Effective 1 February 2021	**Pre-Amendment**	**Post-Amendment**
The legitimate interests exception to the consent obligation	Organisations are required to obtain consent for the collection, use and disclosure of personal data, and there are no exceptions for legitimate interests (such as business improvement purposes).	The new First Schedule to the PDPA introduces legitimate interests as an exception to the consent obligation. Legitimate interests generally refer to any lawful interests of an organisation or other person (including other organisations). [10] Under Part 3 of the new First Schedule, there are (i) specific legitimate interests exceptions, (e.g. for evaluative purposes, for any investigation or proceedings, for recovery or payment of debt owed by the individual to the organisation, or to repay to the individual a debt owed by the organisation); and (ii) general legitimate interests exception, which is a broad exception that can be relied on by an organisation, for any other purpose that meet the definition of "legitimate interests". The organisation seeking to rely on the general legitimate interests exception must comply with additional safeguards to ensure that the interests of individuals are protected. In order to rely on the general legitimate interests exception, organisations must conduct an assessment to ensure that the following requirements are satisfied[11]: (a) the collection, use or disclosure of personal data is in the legitimate interests of the organisation or another person; and (b) the legitimate interests of the organisation or other person outweigh any adverse effect on the individual. The organisation's assessment must, amongst other things[12]: (a) identify and articulate the legitimate interests that justify the collection, use or disclosure of personal data of the individual; (b) identify any adverse effect on the individual and identify and implement reasonable measures to eliminate or mitigate the adverse effect, or reduce the likelihood of occurrence of any adverse effect. The assessment must identify any residual adverse effect on any individual after the implementation of the reasonable measures; (c) set out reasons for the organisation's conclusion that the legitimate interests outweigh any adverse effect on the individual. The organisation must also provide the individual with reasonable access to information about the organisation's collection, use or disclosure of personal data under this exception.

The business improvement exception		The "business improvement" exception can be relied on by organisations to use, without consent, personal data that the organisations have collected in accordance with the PDPA, where the use of such personal data falls within the scope of any of the following business improvement purposes [13]: (a) improving, enhancing or developing new goods or services; (b) improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services; (c) learning or understanding behaviour and preferences of individuals (including groups of individuals segmented by profile); or (d) identifying goods or services that may be suitable for individuals (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals. The business improvement exception can also be relied on by related corporations within the same company group to share personal data (*i.e. collection and disclosure*) intra-group, without consent, for the following business improvement purposes [14]: (a) improving, enhancing or developing new goods or services; (b) improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services; (c) learning or understanding behaviour and preferences of existing or prospective customers (including groups of individuals segmented by profile); or (d) identifying goods or services that may be suitable for existing or prospective customers (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals. This exception can only be relied upon[15] if: (a) the business improvement purpose cannot reasonably be achieved without the collection, use or disclosure of personal data in an individually identifiable form; and (b) a reasonable person would consider such collection, use or disclosure of personal data appropriate under the circumstances. For intra-group sharing of personal data, the related corporations within the same company group must also be bound by agreements or binding corporate rules which require the recipient(s) of the personal data to implement and maintain appropriate safeguards for the personal data. Organisations cannot rely on the business improvement exception to send direct marketing messages.

The research exception		The research exception is intended to enable organisations to conduct broader research and development that may not have any immediate application to their products, services, business operations or market. The PDPA Amendments now allow organisations to use personal data for a research purpose (including historical or statistical research), subject to compliance with the following new conditions[16]: (a) the research purpose cannot reasonably be accomplished unless the personal data is used in an individually identifiable form; (b) there is a clear public benefit to using the personal data for research purpose; (c) the results of the research will not be used to make any decision that affects the individual; and (d) in the event that the results of the research are published, the organisation publishes the results in a form that does not identify the individual. If the organisation wishes to rely on the research exception to disclose personal data for a research purpose, the above conditions must be complied with, and it must be impracticable for the organisation to seek the consent of the individual for the disclosure.

Proposed amendments that have not come into force

Obligation for data portability

Not in Force Yet	Pre-Amendment	Proposed Post-Amendment
Rights to data portability	No such right to request that a porting organisation transmit their personal data to a receiving organisation. Organisations only had an Access Obligation[4], which is intended to allow individuals to access and verify their personal data in an organisation's possession or under its control, and how their personal data has been used by the organisation.	An individual who has an ongoing relationship with an organisation will have a right to data portability. The purpose of this right is to: (a) provide individuals with greater autonomy over their personal data; and (b) boost development, enhancement and refinement of goods and services provided by organisations given that the transmission of data will be facilitated. Save for certain excluded categories of data and in certain excluded circumstances, organisations which possess or control the personal data of an individual (i.e. the "porting organisation") will, upon receiving a data porting request by the individual, have to transmit the applicable data about the individual specified in the request to another organisation (i.e. the "receiving organisation") in accordance with the prescribed requirements in the PDPA, such as requirements relating to technical, user experience and consumer protection matters. This obligation only applies if the receiving organisation is formed or recognised under the laws of Singapore or a prescribed foreign country or territory (i.e. an applicable country), or is resident or has an office or a place of business in Singapore or an applicable country.[17] The excluded types of data and circumstances are specified in the Personal Data Protection (Amendment) Bill, and it is specifically stated that a porting organisation must not transmit the requested data about an individual if, amongst others, the transmission can reasonably be expected to: (a) threaten the safety, or physical or mental health of any other individual; (b) cause immediate or grave harm to the safety, or physical or mental health, of the individual; or (c) be contrary to the national interest.

New offences and increased financial penalties

Not in Force Yet	Pre-Amendment	Proposed Post-Amendment
New offences for individuals who egregiously mishandle personal data	No equivalent offences to hold individuals accountable for egregious mishandling of personal data.	New offences[18] will be introduced where an individual may be found personally liable in respect of (a) unauthorised disclosure of personal data; (b) improper use of personal data that results in personal gain for the offender or another person, or harm or loss to another person; or (c) unauthorised re-identification of anonymised information. Organisations shall remain liable for the actions of their employees in the course of their employment with the organisations. These offences are to criminalise egregious misconduct by individuals whose actions had not been authorised by the organisation.
Increased financial penalties	The maximum financial penalties were capped at S$1 million.	The maximum financial penalty imposed on organisations for breaches of certain key obligations under Parts III to VI of the PDPA (the main data protection obligations) and the new Parts VIA (notification of data breaches) and VIB (data portability) of the PDPA will be increased to 10% of an organisation's annual turnover in Singapore in the case of a contravention on or after 1 February 2021, or one million Singapore dollars (SGD $1milion) [19] in other cases.