LeadingLines
OCTOBER 2020
JOYCE A TAN & PARTNERS

The Singapore PDPA is being amended – Are you ready?

8 October 2020

Executive Summary

The Personal Data Protection Act 2012 ("**PDPA**"), is being amended via a bill (the "**Bill**"). The Bill was first read in Parliament on 5 October 2020. Taken together, the amendments **will increase the potential for legal corporate regulatory risk,** which can be managed in part by **taking appropriate action to implement or update implemented processes, policies and procedures.**

When passed, the Bill will, among other things, deal with the following key issues:

- Introduce important new mandatory obligations on organisations to report data breaches;
- Add ways to manage data subject consent requirements via an enhanced consent framework obligation;
- Create new rights for data subjects to require organisations to transfer data (also known as "**Data Portability**"); and
- Increase the ceiling on fines and create new criminal offences.

A brief breakdown on some key issues for organisations follows.

Mandatory breach notification

Currently, the reporting of obligation is not explicitly mandatory, but the Bill's amendments will set key parameters where they will be so. Organisations will now need to have in place data breach policies and processes to specifically address mandatory breach obligations.

The Bill is supplemented by guidance on the thresholds for mandatory reporting – these are linked to the concept of "significant harm", which is measured both in terms of whether the breach results or is likely to result in significant harm to the affected individuals; or (ii) is of a significant scale.

Breach policies and processes should be legally designed, and tested operationally. Good design of such processes should be led by a legal review, followed by operational implementation which includes training and simulations where possible.

Enhanced Consent framework

The PDPA is consent-centric (i.e. collection, use or disclosure of personal data is subject to consent being given by the data subject or otherwise permitted by exceptions to the consent requirement). The Bill re-organises how exceptions to consent will be stated, and adds new deemed consent options for organisations.

This includes the following:

- Legitimate interests exception – This could include the purposes of detecting or preventing illegal activities (e.g. fraud and money laundering) or threats to physical safety and security, and ensuring IT and network security, or improve understanding of the organisation of it's customers, etc). The exception requires a balancing of the claimed legitimate interests of the organisation and the benefit to the public against the potential for adverse effect on the individual.

- Business improvement exception – Organisations may use personal data without consent for the purposes of (i) operational efficiency and service improvements; (ii) developing or enhancing products/services; and (iii) knowing the organisation's customers.

- Research exception – Organisations will be allowed to use and disclose personal data without consent for research purposes on condition that (i) the use of personal data or the results of the research will not have an adverse effect on individuals; and (ii) results of the research will not be published in a form which identifies any individual.

- Deemed consent for contractual necessity – The Bill will expand the options for organisations to navigate consent requirements, by allowing a limited form or deemed consent for the collection, use or disclosure of personal data is reasonably necessary to conclude or perform a contract or transaction.

- Deemed consent by notification – The Bill will also introduce options to notify data subjects of certain purposes of intended collection, use or disclosure of personal data and, after giving data subjects a reasonable opportunity to opt-out, to act on these purposes where those individuals have not.

These exceptions and arrangements, if used / relied on correctly, can support or enhance legitimate uses of personal data in areas such as data analytics, R&D, business improvement and product / service development.

Data Portability

With the introduction of a new data portability right for individuals, a data subject can ask an organisation to transmit his / her personal data to another organisation, subject to certain qualifications. The obligation will only apply to:

- User-provided data;

- Requesting individuals with an existing and direct relationship with the organisation; and

- Receiving organisations with a presence in Singapore.

However, personal data that is derived by an organisation ("Derived Data") in the course of business from other personal data is not covered by the portability obligation. The PDPC stated in the public consultation paper that it will work with industry and sector regulators to introduce regulations to improve clarity on the data portability requirement, including:

- A 'whitelist' of data categories to which portability applies.

- Technical and procedural details to ensure the correct data is transmitted safely to the right receiving organisation.

- Relevant data porting request models, for example, a push model where consumers can make the data porting request directly to the porting organisation, or a pull model where consumers make the porting request through the receiving organisation.

- Safeguards for individuals, for example introducing cooling-off periods for certain datasets to provide time for a consumer to change their mind and withdraw a porting request, and the establishment of a blacklist of organisations that porting organisations may justifiably refuse to port data to.

Increased ceiling on fines and the creation of new criminal offences

The Bill will increase the ceiling on fines payable under the PDPA. This will be increased to up to **10% of annual gross turnover in Singapore** (for organisations with more than S$10m in yearly turnover), or SGD 1 million (as at this date approx. €638,000 / USD 736,000), whichever is higher.

There will also be new offences to hold individuals accountable for egregious mishandling of personal data on behalf of an organisation or public agency, which include:

- any unauthorised disclosure of personal data that is carried out knowingly or recklessly;

- any unauthorised use of personal data that is carried out knowingly or recklessly and results in a wrongful gain or a wrongful loss to any person; and

- any unauthorised re-identification of anonymised data that is carried out knowingly or recklessly.

The PDPC will further introduce an offence for a person who fails to comply with an order to appear before the PDPC or an inspector and provide his or her statement in relation to an investigation under the PDPA. It will also be an offence for a person to fail to produce any document specified in a written notice.

A short (but not exhaustive) to-do List

The generic to-do list includes the following measures:

- Implement new or update existing policies and processes – in doing so, means test all policies and processes against the new amendments.

- Create / enhance and test data breach management plans – these are live operational processes, not policy or process documents to be issued "and kept on the shelf".

- Ready your organisation's data for potential portability requirements – part of this will involve sorting your data and ensuring you have sufficient control over how data is used, created and derived and identifying what is Derived Data that should fall outside of the scope of a Data Portability request.

- Prime your individual teams (e.g. HR, IT, procurement, marketing, sales, etc) for the changes, and understand what is required in each case – study / assess the impact and train / implement across functions.

Your readiness to respond depends on where your organisations are in the compliance journey. If you have yet to substantially embark on it or did so years ago but haven't looked back in years, it is important to catch up quickly:

- Whether you are in a legal, IT, ops, or management function, expedite the process by bringing in legal guidance to help guide drive efforts on the operational level.

- Obtain advice to understand what needs to be prioritized and what can be pushed back temporarily to manage the situation.

There has been a long line of sight given to the proposed amendments as the Bill is in largely the same form as published previous versions issued alongside public consultation papers (though some changes are important to note).

For this reason, businesses should understand that preparation for these changes should be underway as soon as possible.

More can be found on the Bill here: https://www.pdpc.gov.sg/news-and-events/announcements/2020/10/closing-note-to-public-consultation-on-personal-data-protection-(amendment)-bill

Jeffrey Lim,
Director, Joyce A. Tan & Partners LLC
jeffrey@joylaw.com
8 October 2020

CONTACT

For more information, please contact us at **all@joylaw.com** or at +65 6333 6383
Joyce A. Tan & Partners LLC
8 Temasek Boulevard
#15-04 Suntec Tower 3
Singapore 038988
www.joylaw.com