3 June 2020

DATA PROTECTION

Proposed Amendments to the Personal Data Protection Act

The Personal Data Protection Act 2012 ("**PDPA 2012**") governs the collection, use and disclosure of personal data by organisations in Singapore. Between 2017 and 2019, the Singapore Ministry of Communications and Information ("**MCI**") and Personal Data Protection Commission of Singapore ("**PDPC**") conducted three public consultations to canvass views regarding potential amendments to the PDPA 2012 and to assess ways to ensure the relevancy of the PDPC 2012 in Singapore's evolving digital landscape and economy.

Having consolidated feedback from these consultations, the MCI and PDPC published a draft Personal Data Protection (Amendment) Bill ("**Draft Bill**") for public consultation in May 2020. Given that the Draft Bill is a culmination of several public consultations covering similar subject matter, it is likely to be passed in substantially the same form. In this briefing note, we explore the following key amendments in the Draft Bill:

- New mandatory data breach notification;
- New offences relating to the mishandling of personal data;
- Expansion of categories of deemed consent;
- New exceptions to the consent requirement;
- New data portability obligation;
- Increased financial penalty cap for breaches;
- Expansion of the Spam Control Act (Cap. 311A) to cover instant messaging platforms.

Mandatory Data Breach Notification

Under the existing data protection regime, organisations are encouraged, but not legally obliged, to notify affected parties when a data breach occurs. The PDPC has issued guidance on managing data breaches, which includes guidelines on the circumstances warranting a notification, and timelines for making such a notification.

The Draft Bill proposes to formalise much of the existing guidance into legislation. In particular, the proposed amendments will require organisations to notify **(a)** the PDPC and **(b)** individuals whose personal data has been affected by the data breach, if either:

(i) the data breach results in or is likely to result in *significant harm* to the affected individuals; or
(ii) the data breach *affects* at least a *certain number of individuals* (PDPC's suggested number: 500).

What constitutes "significant harm" has not been specified in the Draft Bill, but is expected to be addressed in subsidiary legislation; it is likely to include situations involving sensitive personal data such as personal identification numbers, certain financial and medical information, and minors' personal data.

Where an organisation has determined that a data breach is required to be notified, it must notify **(a)** the PDPC within 3 calendar days and **(b)** affected individuals (as the case may be) as soon as practicable.

There are two general exceptions proposed to the requirement to notify affected individuals:

1. **Remedial action exception**: where the organisation takes any remedial actions to reduce the likely harm or impact to the affected individuals such that the data breach is unlikely to result in significant harm to the affected individuals; and

2. **Technological protection exception**: where the organisation had implemented, prior to the occurrence of the data breach, any technological measure (e.g. encryption or technological protection that is of a reasonable security standard) that renders it unlikely that the data breach will result in significant harm to the affected individuals.

In addition, the PDPC or a law enforcement agency may direct the organisation not to notify all or certain affected individuals.

New Offences Relating to the Mishandling of Personal Data

The Draft Bill introduces new offences to hold individuals accountable for egregious mishandling of personal data in the possession or under the control of an organisation. These are:

1. knowing or reckless unauthorised disclosure of personal data;
2. knowing or reckless unauthorised use of personal data for a wrongful gain or a wrongful loss to any person; and
3. knowing or reckless unauthorised re-identification of anonymised data.

The proposed penalty for any of the aforementioned offences is a fine not exceeding S$5,000 or imprisonment for a term not exceeding 2 years, or both.

Expanded Categories of Deemed Consent

Under the PDPA 2012, consent is the primary basis for collecting, using and disclosing personal data. The PDPA 2012 also provides for deemed consent where an individual voluntarily provides his/her personal data to an organisation for the purpose for which such data is being collected, used or disclosed, and it is reasonable that the individual would do so.

The Draft Bill proposes to expand the categories of deemed consent to include the following:

1. **Deemed consent by contractual necessity**: Consent may be deemed for the organisation's disclosure to and use of the personal data by third-party organisations, where it is reasonably necessary for the conclusion or performance of a contract or transaction between an individual and an organisation; and

2. **Deemed consent by notification**: Consent may be deemed if **(a)** the organisation provides appropriate notification to inform the individual of the purpose of the intended collection, use or disclosure of his/her personal data, with a reasonable period for the individual to opt out; and **(b)** the individual did not opt out within that period. This approach is not intended to be available for direct marketing purposes.

   To rely on deemed consent by notification, organisations will be required to assess and ascertain that the intended collection, use or disclosure of personal data for the purpose is not likely to have an adverse effect on the individual after taking into account any measures implemented to eliminate, reduce or mitigate such adverse effect.

New Exceptions to the Consent Requirement

Two new exceptions to the consent requirement are proposed in the Draft Bill. These are intended to cater to situations where there are larger public or systemic benefits and obtaining individuals' consent may not be appropriate:

1. **Legitimate interests exception**: This exception allows organisations to collect, use or disclose personal data without consent, where it is in the legitimate interests of the organisation to do so and the benefit to the public is greater than any adverse effect on the individual, e.g. for purposes of detecting or preventing illegal activities such as fraud and money laundering, or threats to physical safety and security.

   In order to rely on this exception, organisations will need to: **(a)** assess any likely adverse effect to the individuals and implement measures to eliminate, reduce or mitigate such identified adverse effect; **(b)** determine that the benefit to the public outweighs any likely residual adverse effect to the individual; and **(c)** disclose their reliance on legitimate interests to the individual to collect, use or disclose personal data.

2. **Business improvement exception**: This exception allows organisations to use personal data without consent for the following business improvement purposes:

   (a) operational efficiency and service improvements;
   (b) developing or enhancing products/services; and
   (c) knowing the organisation's customers.

   The use of personal data for business improvement must be what a reasonable person would consider appropriate in the circumstances, and the data must not be used to make a decision that is likely to have an adverse effect on an individual.

The Draft Bill also proposes to revise the research exception under the PDPA 2012 (which permits use and disclosure of personal data without consent for research purposes), such that less stringent restrictions are now imposed on organisations that rely on this exception.

New Data Portability Obligation

The Draft Bill introduces a new obligation on an organisation to transmit an individual's personal data to another organisation if requested by that individual. This is intended to provide individuals with greater autonomy over their personal data, and facilitate smoother switching between service providers.

To reduce the burden on organisations fulfilling this obligation, the Draft Bill proposes limiting the obligation to specific categories of data and specific stakeholders. In particular, the data porting obligation is envisaged to be limited to:

1. **User provided data** (*i.e.* data that is provided to the organisation, such as name, contact information, credit card details, delivery address) and **user activity data** (*i.e.* data about the individual that is created in the course of or as a result of the individual's use of any product or service, such as transactions, data collected by wearables and sensors) **held in electronic form**, including business contact information;
2. Requesting individuals who have an **existing, direct relationship with the organisation**; and
3. Receiving organisations that have a **presence in Singapore**.

There will be exceptions: for instance, an organisation will not be required to transmit certain data to another organisation, such as data which could reveal confidential commercial information that could harm the competitive position of the organisation, or derived personal data (*i.e.* personal data about an individual that is derived by an organisation from other personal data in the course of business).

Increased Financial Penalty Cap for Breaches

Under the PDPA 2012, the PDPC may impose a financial penalty of up to S$1 million for data breaches. The Draft Bill proposes revising this to **(a)** up to 10% of an organisation's annual gross turnover in Singapore or **(b)** S$1 million, whichever is higher.

Expansion of the Spam Control Act to Cover Instant Messaging Platforms

The Spam Control Act (Cap. 311A) imposes obligations on those who would send unsolicited bulk marketing messages. Currently, it governs only messages sent to e-mail addresses and mobile telephone numbers. The Draft Bill proposes expanding its coverage to instant messaging accounts – this would include accounts on platforms like Telegram, WeChat, or Facebook Messenger, on which messages can be sent without targeting e-mail addresses or mobile numbers.

Comments

The proposed amendments contained in the Draft Bill reflect Singapore's commitment to promoting greater business use of personal data, with a corresponding focus on accountability and responsibility.

Notably, the expansion of categories of deemed consent and the introduction of new exceptions to the consent requirement are aimed at reducing compliance costs and providing organisations more flexibility to use personal data for business purposes. Businesses will have wider latitude to make their own risk-benefit assessments

and to act accordingly; they will also have greater freedom and incentive to use personal data to improve service quality.

At the same time, organisational and individual responsibility will need to keep pace: the introduction of new offences to hold individuals accountable for offences relating to the mishandling of personal data, the mandatory data breach notification, as well as the increased financial penalties, all seek to enhance deterrence and strengthen accountability. Organisations should keep in mind that despite the new offences directed at individuals, organisations remain primarily accountable for data protection and are liable for the actions of their employees in the course of employment.

The introduction of the new data portability obligation represents a significant step forward in improving consumers' autonomy over their personal data and aligning Singapore laws on data portability with those in other jurisdictions. As data portability reduces friction involved in moving data, it would make it easier and less costly for individuals to change service providers. Incumbent organisations may face increased compliance costs, while new entrants will find lower barriers to entry. Overall, consumers are likely to benefit from the greater competition.

On the whole, the proposed amendments to the PDPA 2012 indicate a shift from a more prescriptive, consent-based approach to a more flexible, risk- and accountability-based approach. This, crucially, keeps our data protection regime relevant as countries around the world adapt to technological advances with increasing velocity – unexpectedly aided, in part, by the Covid-19 pandemic – and as technological developments present greater challenges to strict actual-consent-based approaches to data protection. A flexible approach, however, requires organisations to appreciate deeply the risks of intensive personal data usage and the wide-ranging concerns of individuals, and to make sincere efforts to observe the spirit of the legislation. We have seen awareness of data protection in Singapore grow in the years since the PDPA 2012 came into force; it is hoped that this first major amendment to the Act will result in greater engagement and understanding for both users and providers of personal data.

For queries or more information, please contact:

Wilson Wong
Director
wilson.wong@amicalaw.com
(65) 6303 6213

Anna Toh
Associate Director
anna.toh@amicalaw.com
(65) 6303 6234

Geraldine Tan
Director
geraldine.tan@amicalaw.com
(65) 6303 6231

Nicholas Tong
Senior Legal Associate
nicholas.tong@amicalaw.com
(65) 6303 8397

This article is intended to provide general information only and should not be relied upon as an exhaustive or comprehensive statement of law. Should you have any specific questions, please speak with one of our above contacts, or your usual contact at Amica Law LLC.