Hogan Lovells Lee&Lee

The next chapter for Singapore data protection

6 July 2020

The story so far

Six years ago, the Personal Data Protection Act 2012 (PDPA) came fully into force – a lifetime in technology terms. That period has seen the development of blockchain technology and the rise of artificial intelligence (AI), and the creation, curation, and consumption of personal data has grown at a staggering rate, with 90 percent of all data in the world being generated in the last two years alone. As both technology and business models develop, personal data permeates all aspects of a person's activities; from the location they dial into their Zoom call, to how they interact with online service providers, to the closed-circuit television images capturing their movements around a city.

Naturally, the evolving digital landscape has brought about a largescale rethink of the ways in which personal data is regulated. The key data privacy development in recent years has been the European Union's implementation of the General Data Protection Regulations (GDPR), which came into force in 2018 and has led to a global shift in mindset by privacy regulators.

In Singapore, the Personal Data Protection Commission (PDPC) and the Singapore Ministry of Communications and Information concluded three public consultations over the past two years. From this, the Personal Data Protection (Amendment) Bill (the Bill) was born, being released for public consultation on 14 May 2020. Given its history, we expect the Bill to be passed in substantially the same form.

The Bill proposes a number of significant changes to the PDPA, being focused on four key themes:

1. Strengthening accountability.
2. Enabling meaningful consent.
3. Increasing consumer autonomy.
4. Increasing deterrence and strengthening enforcement powers.

Theme one: strengthening the accountability of organisations, and individuals

As part of the Bill, the PDPC are taking a number of steps to strengthen the accountability of organizations in respect of their data protection practices. The PDPA does not currently include

express reference to accountability as a key principle. In a move that reflects the increased emphasis on accountability globally and a shift away from "tick box" compliance, the Bill will introduce accountability as a key principle of the PDPA.

Mandatory data breach notification regime

In recent years, many Asia-Pacific countries have moved from voluntary to mandatory data breach reporting. Australia, the Philippines, Korea, and Thailand led the way with mandatory data breach notification regimes, followed by Hong Kong and India. Now Singapore is following suit.

At present, the PDPC adopts a voluntary regime as set out in the latest *Guide to Managing Data Breaches 2.0*. In order to strengthen accountability, the Bill effectively formalizes much of the existing guidance into legislation by introducing a mandatory data breach notification requirement. The regime will cover data breaches which result in, or are likely to result in, significant harm to an affected individual, or which is of a significant scale. The organization concerned will be required to notify the PDPC and, if necessary, affected individuals following a data breach. There are various scenarios in which an organization need not notify the individual, including where sufficient remedial action has been taken, or the data is sufficiently encrypted.

Data breaches that constitute significant harm will be clarified in later regulations but will likely include those which compromise sensitive categories of personal data, such as social security numbers, drivers' licence numbers, credit/debit card numbers, health insurance information, and medical history information. A numerical threshold will be used to determine whether a breach is of a significant scale. The PDPC currently notes that data breaches that affect 500 or more individuals would be an appropriate threshold.

Finally, data intermediaries processing data on behalf of other organizations will be required to notify those organizations, without undue delay, where they have reason to believe that a data breach has occurred.

New offences relating to egregious mishandling of personal data

The PDPC will also move to strengthen the accountability of individuals who handle or have access to personal data through the introduction of three new offences:

1. Knowing or reckless unauthorized disclosure of personal data.
2. Knowing or reckless unauthorized use of personal data for a wrongful gain or a wrongful loss to any person.
3. Knowing or reckless unauthorized re-identification of anonymized data.

Whilst the PDPC will remain focused on holding organizations accountable for data protection, this move to directly criminalize the mishandling of personal data by individuals is an important development in the safeguarding of personal data. Individuals found guilty of an offence will be liable upon conviction to a fine of up toSG$5,000 and/or imprisonment for up to two years. This would include employees who act in contravention of an employer's policies or act outside their scope of employment; as such, the role of the data protection officer, along with staff training and protocols, are likely to be given far more thought by organizations.

Theme two: enabling meaningful consent

It is easy to see the development of personal data regulations across the world as ever-tightening control, particularly following the introduction of the GDPR. But this is not the whole picture. The PDPC has recognized that technological developments are causing significant challenges for

consent-based approaches to data protection. It simply isn't practical for organizations to anticipate the specific purpose for each collection of data at the outset, nor always practical to seek express consent. In practice, the current approach has resulted in very lengthy or broadly worded privacy notices that often do not enable individuals to clearly understand the purpose of the collection such that they can provide meaningful consent.

Extended deemed consent provisions

The PDPC is therefore enhancing the framework for the collection, use, and disclosure of personal data under the PDPA to ensure "meaningful consent" by individuals. Effectively, this can be seen as a "loosening" of the consent requirement under the PDPA. In a move that mirrors developments in Australia, New Zealand, and the EU, the PDPC will expand the concept of deemed consent in two ways – deemed consent by contractual necessity, and deemed consent by notification.

Under the first limb, consent will be deemed to have been given where data has been disclosed to, and used by, a third party organization and it is reasonably necessary to conclude or perform a contract or transaction between the individual and the disclosing organization.

Under the second limb, consent will be deemed to have been given where individuals have been notified of the purpose of the intended collection, given a reasonable opportunity to opt-out, and have not opted out.

Exceptions to the consent requirement

The Bill will also introduce two entirely new exceptions to the consent requirement, covering situations where there are substantial public or systemic benefits and where obtaining individuals' consent may not be appropriate.

Legitimate interests exception

A legitimate interests exception will be introduced to enable organizations to collect, use, or disclose personal data where it is in the legitimate interest of the organization and where the benefit to the public outweighs any adverse effect to the individual. This is very similar to the legitimate interest concept enshrined in the GDPR and will work to ensure information technology and network security, as well as prevent illegal activities such as fraud and money laundering.

Business improvement exception

In a pragmatic move, businesses will be able to use personal data without having to obtain consent for business improvement purposes. This broad criteria includes ensuring better operational efficiency, improved services, for product or service developments, and to better get to know customers.

These exceptions will be welcomed by businesses operating in Singapore, as well as by in-house counsels advising product teams who may benefit from these innovative provisions.

Theme three: increasing consumer autonomy

As part of the data protection package, a number of measures are being introduced to provide consumers with greater autonomy in respect of their personal data.

Data portability obligation

The Bill will introduce a new data portability obligation aimed at making it easier for consumers to switch service providers and avoid being "locked in" with a single provider. At an individual's request, an organization will be obliged to transmit all data about the individual that is in their

possession to another organization in a commonly used machine-readable format. This measure will facilitate movement of consumer data from one service provider to another in order to improve competition.

The scope of data covered by the data portability obligation includes all user provided data and data generated by the individual's activities in using the product or service. The data portability obligation will come into effect with the issuance of regulations which will institute a "white list" of data categories to which the obligation will apply.

A number of exceptions to the data portability obligation will also be introduced. These will mirror the exceptions to the Access Obligation under Schedule Five to the PDPA. One of the important exceptions will relate to data which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organization.

Improved controls for unsolicited commercial messages

The Do Not Call (DNC) provisions in the PDPA and the somewhat overlapping provisions of the Spam Control Act (SCA) will be amended to provide consumers with greater protection against, and control over, unsolicited marketing messages. The following measures will be introduced:

- The SCA will be extended to cover messages sent to instant messaging account platforms.
- The DNC provisions will be expanded to prohibit the sending of unsolicited messages to numbers obtained through the use of dictionary attacks and harvesting software.
- Obligations and liabilities will be imposed on third-party checkers.

Theme four: Iicreasing deterrence and strengthening enforcement

The first half of 2018 saw a 72 percent increase in data records lost, stolen, or compromized worldwide, compared to the same period the previous year. Data breaches have therefore become a primary concern for businesses and individuals alike. In response to this growing threat, the PDPA will be enhanced to ensure better deterrence and effectiveness of enforcement.

Increased financial penalties

The maximum financial penalty under the PDPA will be increased to the greater of 10 percent of an organization's annual gross turnover in Singapore, or SG$1 million. These penalties are significant, although it should be noted that they are still comparatively low compared to some other regimes. The maximum penalty under the GDPR, for example, is the greater of four percent of worldwide turnover or €20 million.

Statutory undertakings

The implementation of a data breach management plan can be the subject of a statutory undertaking. This will enable the PDPC to have a more effective system for monitoring, internal reporting, and management of data breaches, aligning the regime with Australia, Canada, and the UK. The PDPC will be able to investigate the underlying breach if the organization fails to comply with a statutory undertaking. When coupled with the mandatory data breach notification, statutory undertakings will further encourage organizations to adopt accountable practices.

Referrals to mediation

Finally, the PDPC will be afforded the power to make referrals to mediation, without both parties having to consent. This will enable the PDPC to manage the increase in data protection complaints in a sustainable manner.

Onwards and upwards

The data privacy landscape is constantly shifting, with technological advances and the monetization of new business models pushing the boundaries of legal regulations. The amendments introduced by the Bill reflect the complexity of this landscape, having to balance the rights of the individual with the innovation and flexibility of business. The proposed amendments reflect Singapore's commitment to promoting greater business use of personal data, with a corresponding focus on accountability and responsibility, allowing businesses to make their own risk-based assessments to a greater extent than previously.

Contacts

Stephanie Keen
Asia-Pacific Head of Corporate & Finance, Singapore
T +65 6302 2553
stephanie.keen@hoganlovells.com

Matthew Bousfield
Counsel, Singapore
T +65 6302 2565
matthew.bousfield@hoganlovells.com