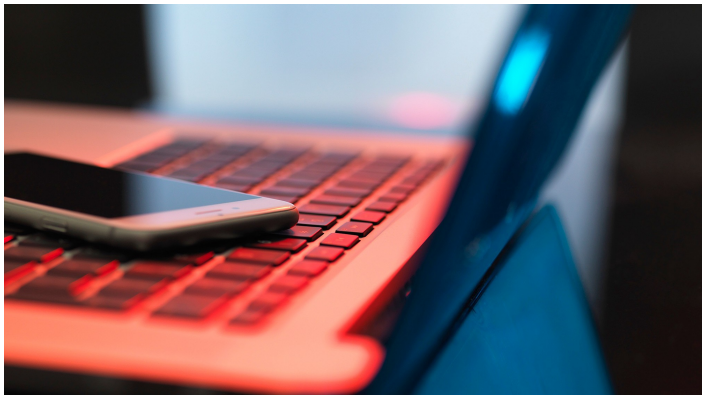
Personal Data Protection (Amendment) Act 2020 in Singapore: Effects on your business

04 NOVEMBER 2020

CATEGORY:
ARTICLE



The Personal Data Protection Act 2012 ("PDPA") has not been amended since it was first enacted in 2012, with its Data Protection Provisions and its Do Not Call ("DNC") Provisions coming into effect on 2 January 2014 and 2 July 2014 respectively.

With accelerating growth in data-centric technologies such as Internet of Things, artificial intelligence and gig economy, there is an exponential increase in the volume of personal data generated, collected and processed around the world and in Singapore. The new Personal Data Protection (Amendment) Bill 2020 just passed on 2 November 2020 seeks to strengthen the accountability of organisations, to recalibrate the balance between individual's consent and organisational accountability to harness data for appropriate and legitimate purposes, to grant greater consumer autonomy over their own personal data, and to strengthen the effectiveness of enforcement efforts by the Personal Data Protection Commission ("PDPC").

The amendments to the PDPA are timely in the fast-changing landscape of the digital economy, and bring Singapore's personal data protection laws up to date and aligned with international standards, such as the GDPR.

Notwithstanding the potential increase in operating costs for companies (especially SMEs) in order to comply with the new obligations, the investment spent in being digitally secure far outweighs the cost of a data breach, as reputational damage cannot be quantified and it will take more time and effort to restore consumer or business confidence in a company which is publicly fined for failing in its data protection obligations.

This article explores some of the new obligations introduced and their potential effects on your business.

New mandatory data breach notification requirement

Subject to prescribed exceptions, organisations are now required to notify (i) PDPC of any data breach that results in, or is likely to result in, significant harm to the individuals to whom any personal data affected by a data breach relates ("affected individuals"), or is of a significant scale (i.e. involving 500 or more individuals), and (ii) affected individuals if the data breach results in, is likely to result in, significant harm to them.

In the event of a data breach, the PDPC must be notified as soon as practicable and no later than three days after the data breach is assessed to fall within the above notification criteria, and affected individuals must be notified as soon as practicable.

In order to comply with the data breach notification requirement within the prescribed timeline, organisations should put in place cross-disciplinary data breach management policies and procedures, if they have not already done so, to manage data breach incidents effectively.

Penalties for data breach incidents have also been raised, with organisations whose annual turnover in Singapore exceed S$10 million exposed to the risk of fines up to 10% of the organisation's annual turnover in Singapore. The maximum fine was previously S$1 million.

In view of the tighter timelines and higher penalties on data breach incidents, organisations may consider purchasing cybersecurity insurance to insure themselves against the costs arising from data breach incidents, such as the costs of engaging external IT forensic experts to investigate the incident and engaging lawyers, if necessary, to manage the reporting of the data breach to the PDPC and the affected individuals.

New data portability obligation

A new data portability obligation has also been introduced to enable easy switching of service providers (e.g. telecommunication services), to

provide consumers with greater autonomy and control over their personal data, and to facilitate the innovative and more intensive use of specified personal data in the possession or under the control of organisations to support the development, enhancement and refinement of products and services provided by other organisations located or operating in Singapore or elsewhere.

An individual may request (data porting request) an organisation (porting organisation) to transmit applicable data specified in the request to another organisation (receiving organisation). Save under prescribed exceptions, the porting organisation must transmit the requesting individual's personal data that is in the porting organisation's possession or control to the receiving organisation, so long as (i) the data porting request satisfies the requirements prescribed in the regulations, (ii) the porting organisation, at the time it receives the data porting request, has an ongoing relationship with the individual, and (iii) the receiving organisation has a presence in Singapore, regardless of the storage location of the data.

The new data portability obligation will only come into effect when the regulations are issued. In a separate article, we will be sharing our insights from the European perspective on their equivalent Right to Data Portability.

Expanded scope of "deemed consent"

Organisations now enjoy enhanced ease in disclosure of personal data to other organisations, as the meaning of "deemed consent" has been expanded.

An organisation may now disclose personal data of an individual to another organisation without expressly obtaining the individual's consent, in the following expanded circumstances relating to contractual necessity, subject to any express terms to the contrary in the contract between the organisation and the individual.

Subject to prescribed exceptions (e.g. marketing messages), an organisation may also rely on notification to obtain deemed consent from individuals, so long as:

• The organisation takes reasonable steps to provide appropriate notification to inform the individual about (i) the organisation's intention to collect, use or disclose the personal data, (ii) the purpose of such collection, use or disclosure, and (iii) 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;

• The organisation conducts an assessment to determine that the proposed collection, use or disclosure is not likely to have an adverse effect on the individual, with such assessment identifying any such adverse effect and identifying and implementing reasonable measures to eliminate, reduce the likelihood of, or mitigate such adverse effect; and

• The individual does not notify the organisation, before the expiry of the above period, that he or she does not consent to the proposed collection, use or disclosure

New consent exceptions: legitimate interests exception and business improvement exception

In order to cater to situations where there are larger public or systemic benefits where obtaining individuals' consent may not be appropriate, two new exceptions have been added to the Consent Obligation: legitimate interests exception and business improvement exceptions.

Under the legitimate interests exception, subject to prescribed exceptions (e.g. marketing messages), an organisation may collect, use or disclose an individual's personal data without consent if (i) such collection, use or disclosure is in the legitimate interests of the organisation and (ii) the benefit to the public (or any section thereof) is greater than any adverse effect on the individual. Before availing itself of this exception, an organisation must:

• Conduct an assessment to determine whether conditions (i) and (ii) above are satisfied, with such assessment identifying any such adverse effect on the individual and identifying and implementing measures to eliminate, reduce the likelihood of, or mitigate such adverse effect; and

• Inform the individual, in any reasonable manner, that the organisation is collecting, using or disclosing personal data under the legitimate interests exception.

Separately, an organisation may rely on the business improvement exception to use personal data without consent for the following business improvement purposes:

• To improve, enhance or develop goods or services provided by the organisation, or methods or processes for the operations of the organisation;

• To learn about and understand the behavior and preferences of customers in relation to the goods services provided by the organisation or to identify goods or services provided by the organisation that may be suitable for the organisation's customers other than individual customers.

The business improvement exception can be used only if these purposes cannot reasonably be achieved without the use of personal data in individual identifiable form and the use of the personal data by the organisation does not have any adverse effect on the individual.

Access and porting requests: preservation obligation

To ensure that an individual will have meaningful recourse in the event an organisation refuses his / her access or porting request under the PDPA, the organisation is now required to preserve, a complete and accurate copy of the personal data concerned, for the prescribed period. According to the Public Consultation Paper, the prescribed period will be set out in the regulations, and will be (a) at least 30 calendar days after rejection of the request, or (b) until the individual has exhausted his / her right to apply for a reconsideration request to PDPC or appeal to the Data Protection Appeal Committee, the High Court or Court of Appeal, whichever is later.

Organisations should amend their privacy policies and prepare record retention schedules to ensure that customer data is not accidentally or intentionally deleted or removed just because the customer's access or porting request has been refused by the organisation.

Access request: wider scope of disclosure

Organisations, which previously may have difficulty acceding to access requests for personal data that may contain personal data about another individual, will now be able to provide access to personal data that reveal personal data about another individual, or reveal the identity of the individual who provided the personal data about another individual even if the individual providing the personal data does not consent to the disclosure of his / her identity, as long as the personal data concerned is user activity data about, or user-provided data from, the individual who made the request.

Personal liability for offences relating to egregious mishandling of personal data

While organisations are still liable for the conduct of their employees in the course of their employment with the organisations, three new offences have been introduced to hold individuals accountable for egregious mishandling of personal data by:

- Unauthorised disclosure;
- Improper use; and/or
- Unauthorised re-identification of anonymised information.

The above offences are punishable on conviction by a fine not exceeding S$5,000 or to imprisonment not exceeding 2 years or both.

The possibility of personal liability for failing to act in accordance with the company's data protection policies and procedures, and social media polices, if any, should be highlighted by employers when conducting PDPA training for their employees.

DNC Provisions: ongoing relationship exemption

The PDPA now in clearer wording sets out an exemption from the obligation to check the DNC Register(s) for organisations with an ongoing relationship with recipients of the message.

DNC Provisions: new obligation on third-party checkers

A piece of good news for organisations who have been relying on third-party checkers to check the DNC Register is that the onus and liability will now be reallocated to third-party checkers.

An organisation will now be deemed to have complied with the duty to check the DNC Register(s) under section 43 of the PDPA if, before sending the message, it has been informed by the third-party checker that the Singapore telephone number is not listed in the DNC Register(s), and it has no reason to believe that, and is not reckless as to whether, the information provided by the third-party checker is false or inaccurate.

On the other hand, a third-party checker now has an obligation under the PDPA, to accurately communicate the DNC Register results to the organisation engaging its services.

Nevertheless, in any event, organisations should still ensure that in their service agreements with third-party checkers, there is an undertaking by the third-party checkers that they will accurately communicate the DNC Register results to the organisations, accompanied by an indemnity that the third-party checkers will indemnify the organisations for any costs, damages, fines or administrative penalties arising from any breach of the undertaking.

DNC Provisions: dictionary attacks and address-harvesting software

It is now prohibited for anyone to send any message that has a Singapore link (e.g. the sender or recipient is in Singapore or has an office in Singapore) to any telephone number generated or obtained through the use of a dictionary attack or address-harvesting software.

Organisations which have been utilising such software should make alternative arrangements and cease sending unsolicited commercial advertisements or messages to such telephone numbers.

Conclusion

Since the enactment of the PDPA in 2012, organisations in Singapore have gradually implemented privacy policies and procedures, and it has become the prevailing norm for personal data-related issues to be considered in business processes and as part of legal compliance.

We have no doubt that companies in Singapore will similarly adjust to the new obligations and with greater automation come to see them as a responsibility that they have over the personal data that they are handling. This would stand them in good stead as companies that take data protection seriously.

Authors

Gretchen Su

PARTNER | SINGAPORE

Intellectual property and technology

+65 6238 3068

gretchensu@witherskhattarwong.com

Magdalene Tan

SENIOR ASSOCIATE | SINGAPORE

Intellectual property

+65 6238 3378

magdalenetan@witherskhattarwong.com