LES BRÈVES - LEGAL INFORMATION

PROPOSED BY DS GROUP

February 24th 2021

Singapore – Personal Data Protection (Amendment) Act 2020

With a view to bringing Singapore's personal data protection landscape up to date and in line with international standards, Singapore passed the Personal Data Protection (Amendment) Act 2020 on 2 November 2020 ("**PDPA Amendment**").

The PDPA Amendment brings the most significant changes to the Personal Data Protection Act 2012 ("**PDPA**") since the PDPA first came into force on 1 July 2014.

The PDPA Amendment will take effect in phases. The following key changes took effect on **1 February 2021**:

➢ **New mandatory data breach notification (new Part VIA)**

Subject to prescribed exceptions, organisations are now required to notify:

(i) the Personal Data Protection Commission (**PDPC**) of any data breach that:
   a. results in, or is likely to result in, significant harm to an affected individual, or
   b. is of a significant scale (i.e. involving 500 or more individuals)

(ii) affected individuals if the data breach results in, is likely to result in, significant harm to them.

Personal data resulting in significant harm: The Personal Data Protection (Notification of Data Breaches) Regulations 2021 (Regulations on Notification of Data Breaches) ("**2021 Data Breach Regulations**") provides in its schedule a list of personal data or circumstances deemed to result in significant harm to affected individuals if compromised in a data breach.

Timeline: according to the new section 26D of the PDPA, where an organisation assesses that a data breach is a notifiable data breach, it must notify:

(i) PDPC as soon as is practicable, but in any case no later than 3 calendar days after the day the organisation makes such assessment;
(ii) the affected individual(s) as soon as practicable, at the same time or after notifying the PDPC.

Content of notification: sections 5 and 6 of the 2021 Data Breach Notification list the information that the notification must contain.

Enhanced penalties: penalties for data breach incidents have been raised as follows:

- for organisations having annual turnover in Singapore exceeding S$10 million: up to 10% of the organisation's annual turnover in Singapore.
- any other case: S$1 million.

It is however to be noted that according to the PDPC Advisory Guidelines on Enforcement of Data Protection Provisions (as updated on 1 February 2021), the increased financial penalties will take effect on a further date to be notified, and no earlier than **1 February 2022**.

- **New offences concerning mishandling of personal data**

Under new sections 48D, 48E and 48F of the PDPA, individuals may be held accountable for:

(i) unauthorised disclosure of personal data;
(ii) improper use of personal data for a wrongful gain or a wrongful loss to any person; and
(iii) unauthorised re-identification of anonymised data.

The prescribed penalty for these offences, which may be imposed on individuals, is a fine not exceeding S$5,000 or imprisonment for a term not exceeding 2 years or both.

- **Changes to the consent framework**

The meaning of deemed consent has been expanded.

The PDPA Amendment introduces the concept of deemed consent by contractual necessity (section 15 of the PDPA) and deemed consent by notification (new section 15A of the PDPA) to allow organisations to collect, use and disclose personal data without expressly obtaining the individual's consent subject to certain conditions.

Echoing the General Data Protection Regulation 2016/279, the PDPA Amendment also introduces "Legitimate Interests" and "business improvement" as an additional basis of processing personal data, or as an exception to the consent obligation to cater to situations where there are larger public or systemic benefits where obtaining individuals' consent may not be appropriate.

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) he legitimate interests of the organisation outweigh any adverse effect on the individual. Before availing itself of this exception, an organisation must (a) conduct an assessment, before collecting, using or disclosing the personal data (as the case may be), to determine whether conditions (i) and (ii) are satisfied; and (b) provide the individual with reasonable access to information about the organisation's collection, use or disclosure of personal data (as the case may be).

Under the business improvement exception, an organisation may collect, use or disclose an individual's personal data without consent to:

(i) improve or enhance any goods or services provided, or develop new goods or services to be provided, by the organisation;
(ii) improve or enhance the methods or processes, or develop new methods or processes, for the operations of the organisation;
(iii) learn about and understand the behaviour and preferences of an individual in relation to the goods or services provided by the organisation;
(iv) identify any goods or services provided by the organisation that may be suitable for an individual, or personalise any such goods or services for the individual.

- **PDPA Amendment Regulations**

In addition to the 2021 Data Breach Regulations, a set of regulations made under the PDPA Amendment also came into force on 1 February 2021:

- The Personal Data Protection Regulations 2021,
- The Personal Data Protection (Enforcement) Regulations 2021;
- The Personal Data Protection (Composition of Offences) Regulations 2021.

- **Right to data portability**

A new data portability obligation has been introduced to provide individuals with greater autonomy and control over their personal data and facilitate the innovative and more intensive use of applicable data in the possession or under the control of organisations to support the development, enhancement and refinement of goods and services provided by other organisations located or operating in Singapore or elsewhere.
An individual may request a 'porting organisation' through 'data porting request' to transmit to a 'receiving organisation' the applicable data about the individual specified in the data porting request. Save under prescribed exceptions, the porting organisation must, upon receiving the data porting request, transmit the applicable data specified in the data porting request to the receiving organisation, subject to:

(i) the data porting request satisfying the prescribed requirements; and
(ii) the porting organisation having an ongoing relationship with the individual at the time it receives the data porting request.

This new data portability obligation is expected to take effect in the coming months when the regulations are issued.

Conclusion:
Organisations should review their personal data protection policies to ensure that they are in line with the PDPA Amendment and that they are adequately prepared to handle data breach incidents.

For any additional information, contact Lisbeth Lanvers-Shah or Olivier Monange.