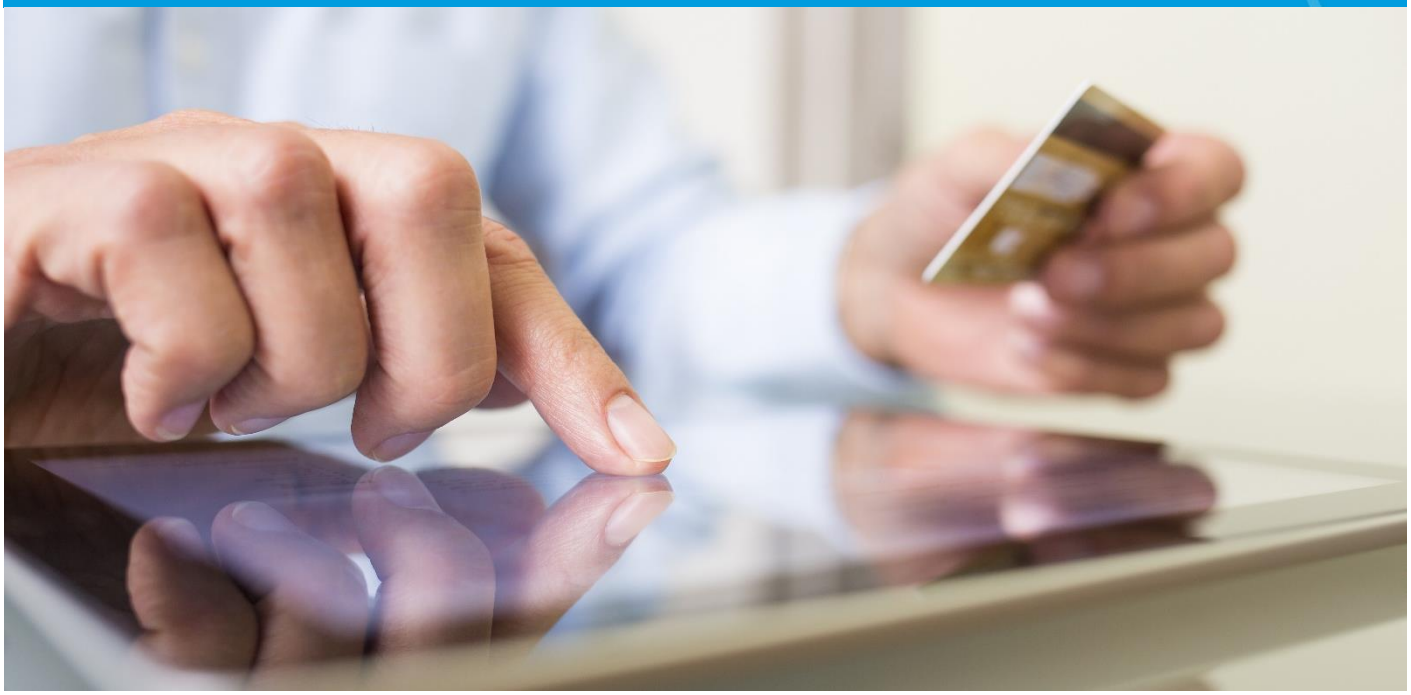
BRIEFINGNOTE

STEPHENSON HARWOOD (SINGAPORE) ALLIANCE

March 2021

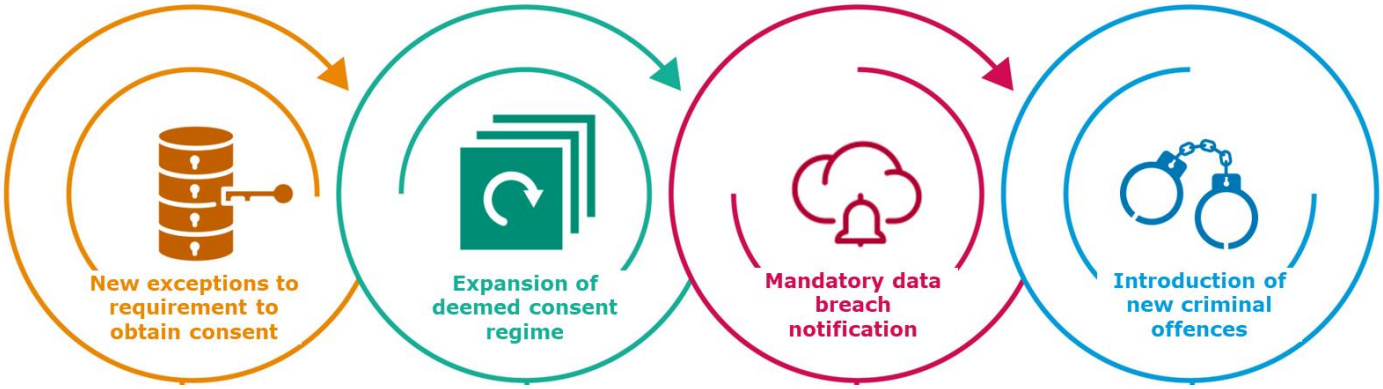
Amendments to Personal Data Protection Act



On 1 February 2021, certain key amendments to the Personal Data Protection Act 2012 ("**PDPA**"), as well as accompanying subsidiary regulations, came into force. This round of amendments will introduce significant change to the existing data protection regime in Singapore, which bring it closer in line with higher global standards.

In this update, we set out the salient changes which organisations in Singapore will need to be cognisant of.

Key updates



1. New exceptions to requirement to obtain consent

Consent need not be obtained from individuals in certain new situations:

(a) Legitimate interests exception

Collection, use and disclosure of personal data without consent is now permitted in the event that this is in the general legitimate interests of the organisation.

To rely on this broad exemption, an organisation must: (1) identify the legitimate interest; (2) conduct an assessment to identify any adverse effect on the individual and implement reasonable measures to reduce any such effects; and (3) disclose reliance on the legitimate interests exception.

- **Identifying the legitimate interests.** Organisations must be able to articulate what the benefits and who the beneficiaries are, as well as demonstrate that the benefits are real. Benefits should not be wholly speculative and should include tangible (e.g. improvements to product, cost savings) and intangible benefits (e.g. improved customer experience).
- **Assessment of adverse effects.** The assessment of whether the proposed actions would give rise to any adverse effects will need to take into account the impact on the individual, the nature and type of personal data, the extent of the proposed processing, as well as prevailing norms and general standards of reasonableness, amongst others. Adverse effects may include, for example, physical harm, harassment, serious alarm or distress to the individual. The Commission has set out a detailed checklist of what to consider when conducting an assessment in **Annex C to the Advisory Guidelines on Key Concepts in the PDPA**.
- **Residual adverse effects.** If it is assessed that there is likely residual adverse effect to the individual after implementing the measures, organisations are required to conduct a balancing test as part of the assessment to determine that the legitimate interests of the organisation or other person (including other organisations) outweigh any likely residual adverse effect to the individual.
- **Disclosure of reliance.** Organisations are required to provide the relevant individuals with reasonable access to information that they are relying on the exception. This can be provided through any reasonable means, e.g. through the firm's public privacy policy or via other means of communication.

(b) Business improvement exception

Organisations may use (note that this does not extend to collection or disclosure) the personal data of individuals without their consent where:

- the use is for any of the following business purposes:
  - improving, enhancing or developing new goods or services;
  - improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;
  - learning or understanding behaviour and preferences of individuals; or
  - identifying goods and services that may be suitable for individuals, or personalising and customising goods and services for such individuals;
- the purpose cannot reasonably be achieved without using the personal data in an identifiable form (i.e. anonymised data would not suffice); and
- the use is one that would reasonably be considered appropriate in the circumstances.

The business improvement exception also applies to sharing of personal data between entities which are related without consent for certain business improvement purposes, provided that the entities are bound by legally enforceable rules which require the recipient entity to implement and maintain appropriate protections for the received personal data.

2. Expansion of deemed consent regime

The deemed consent framework has now been expanded significantly such that consent can be deemed in certain additional situations, the key ones being in the event of contractual necessity and by notification.

(a) Deemed consent by contractual necessity

Consent of an individual may be deemed where the individual provides his personal data to an

organisation for the purpose of a transaction, and it is reasonably necessary for the organisation to disclose the personal data to another organisation in order to conclude or perform the transaction. This would also extend to further downstream disclosures to other organisations.

(b) Deemed consent by notification

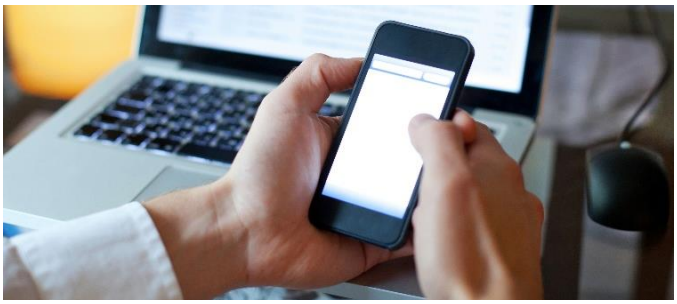
An individual may be deemed to have consented to the collection, use or disclosure of personal data for a purpose he has been notified of if he has not taken any action to opt out of this. This is particularly useful where organisations wish to use personal data for other purposes to which the individual has not previously consented to at the time of collection.

In order to rely on deemed consent by notification, an organisation is required to: (1) conduct an assessment to determine that the proposed collection, consent or disclosure is not likely to have an adverse effect on the individual; (2) take reasonable steps to ensure that the notification provided to the individual is adequate; and (3) provide a reasonable opt-out period.

- **Assessment of adverse effects.** This would be the same assessment as that of the legitimate interests exception, as elaborated above. The Commission has set out a detailed checklist of key considerations when conducting an assessment in **Annex B to the Advisory Guidelines on Key Concepts in the PDPA**.
- **Adequate notification to individual.** In determining whether a notification is adequate, organisations should consider: (1) the usual mode of communication; (2) whether direct communication channels (e.g. mail, email, text message) are available; and (3) the number of individuals to be notified (mass communication channels may be used if so).
- **Reasonable opt-out period.** In determining the length of the opt-out period, organisations should consider: (1) the nature and frequency of interaction; and (2) the communications and opt-out channels used.

  A copy of the assessment conducted will need to be retained by the organisation throughout the period the organisation relies on deemed consent by notification.

3. Mandatory data breach notification



The mandatory data breach notification is a new mechanism that has been introduced. In brief, organisations are now required to:

- conduct assessments of data breaches that are believed to have occurred in a reasonable and expeditious manner (as a general standard, assessments should be conducted within 30 days); and
- notify the Personal Data Protection Commission ("**Commission**") of any breach that:
  - results in, or is likely to result in, significant harm to affected individuals; or
  - is of a significant scale.

  (a) Significant harm and scale

  A data breach is deemed to result in significant harm to an individual if the data breach relates to significant personal information; in particular, where the breach relates to: (1) an individual's name or alias or identification number, in combination with certain prescribed information relating to, amongst others, financial information, identification of vulnerable individuals or insurance information; or (2) in respect of an account held with a bank or a finance company, the individual's account identifier and password or other access code.

  A data breach is deemed to be of significant scale if 500 or more individuals have their data compromised in the breach.

  (b) Timeline for notification

  Once a data breach is assessed to be notifiable, organisations are required to notify the Commission as soon as possible, and no later than 3 calendar days after the breach. Notifications to individuals are also required to be made as soon as practicable, at the same time or after notifying the Commission.

Notifications to individuals need not be made in certain situations, such as where appropriate technological measures have been taken such that the personal data is inaccessible or unintelligible to unauthorised persons.

4. Introduction of new criminal offences

New offences which target actions by individuals have been introduced. These include offences for: (1) knowing or reckless unauthorised disclosure of personal data; (2) knowing or reckless improper use of personal data for wrongful gain or causing wrongful loss to any person; and (3) knowing or reckless unauthorised re-identification of anonymised information.

Individuals found guilty of any of these offences will be liable on conviction to a fine of up to S$5,000 and/or imprisonment for a term of up to 2 years.

What's next

The remaining provisions of the Personal Data Protection (Amendment) Act 2020 are expected to come into effect in the near future. Of note are the following updates:

- **Increased financial penalties.** The financial penalties which may be imposed on organisations for breach of provisions of the PDPA will be increased significantly, from the existing maximum fine of S$1 million to a maximum penalty of S$1 million or 10% of the organisation's annual turnover in Singapore, whichever is higher. The revised financial penalties are expected to take effect no earlier than 1 February 2022.
- **Right to data portability.** Individuals will be granted a new right to data portability. This means that an individual will be able to request that an organisation transmit the individual's personal data held by that organisation to another organisation.

What should organisations do?

In light of the extensive amendments to Singapore's data protection regime, we would recommend that organisations take the following steps:

- review their existing collection, use and disclosure activities in light of the revised consent framework, and determine if this can be streamlined further in reliance on the new exemptions to consent and the expanded scope of deemed consent;
- put in place a robust data breach detection and assessment framework and ensure that the relevant persons are familiar with response plans in accordance with the mandatory data breach assessment and notification requirements;
- review existing privacy policies and consent provisions for compliance with the existing provisions; and
- ensure that employees are familiar with the updated regime by providing appropriate internal training.

How can we help?

We are well-versed with the workings of Singapore's data protection regime and have advised numerous organisations on their data protection obligations. We have also conducted complete data protection audits on various international companies, through which we identify, assess and address gaps in their compliance regime.

If you are an organisation, we can assist with ensuring your company is fully compliant with all its obligations under the amended PDPA. Our capabilities include assisting with:

- conducting compliance reviews and audits to identify gaps in compliance and proposing appropriate measures to remedy gaps and streamline processes;
- drafting bespoke data protection policies (e.g. employee data policies and website policies) and standard operating procedures to address your organisation's obligations based on your business operations; and
- providing in-house training sessions to ensure your employees are fully cognisant of the practical steps they will need to take to maintain a robust data protection practices within the company.

This article was written by Virtus Law LLP (a member of the Stephenson Harwood (Singapore) Alliance). For more information, please do not hesitate to contact any of the team at Stephenson Harwood (Singapore) Alliance. We remain committed to assisting our clients during this challenging period.

Get in touch

Sheetal Sandhu
Partner, Singapore
T: +65 6661 6523
E: sheetal.sandhu@shlegalworld.com

Tom Platts
Partner, Singapore
T: +65 6622 9641
E: tom.platts@shlegal.com

Naomi Leach
Partner, London
T: +44 20 7809 2960
E: naomi.leach@shlegal.com

Ben Sigler
Partner, London
T: +44 20 7809 2919
E: ben.sigler@shlegal.com

Stephenson Harwood is a law firm of over 1100 people worldwide, including 180 partners. Our people are committed to achieving the goals of our clients – listed and private companies, institutions and individuals.

Our headquarters are in London, with nine offices across Asia, Europe and the Middle East. In addition, we have forged close ties with other high quality law firms. This diverse mix of expertise and culture results in a combination of deep local insight and the capability to provide a seamless international service.

The Stephenson Harwood (Singapore) Alliance (the "**Alliance**") is part of the Stephenson Harwood network and offers clients an integrated service in multi-jurisdictional matters involving permitted areas of Singapore law. The Alliance is comprised of Stephenson Harwood LLP and Virtus Law LLP. Court litigation services in Singapore are provided by the Singapore law firm, Virtus Law LLP.

STEPHENSON HARWOOD (SINGAPORE) ALLIANCE