5 Further Things You Need to Know About the Personal Data Protection (Amendment) Bill

DENTONS RODYK

November 4, 2020

In our last update, we highlighted five (5) amendments that were proposed to be made to the Personal Data Protection Act (PDPA) (Act 26 of 2012). Parliament has since passed the Personal Data Protection (Amendment) Bill 2020 (Bill No. 37/2020) on 2 November 2020. We do not know when the Amendments will come into force but we expect it to be before the end of the year or in the first quarter of 2021.

This Article highlights five (5) additional amendments to the PDPA that would come into force soon.

1. Increased Penalties for Non-compliance with the PDPA

The maximum financial penalty will be calculated based on the organisation's annual turnover in Singapore.

- It is now clear that the maximum financial penalty for organisations who intentionally or negligently contravene the Data Protection Provisions of the PDPA will be based on the organisation's annual turnover in Singapore. Therefore, if an organisation's annual turnover in Singapore exceeds $10 million, it may face a financial penalty of up to 10% of its annual turnover in Singapore. The Minister has stated that this enhanced penalty cap would come into effect "no earlier than 1 year after the [amendments] come into force".
- There are also harsher punishments for those who send unsolicited messages to telephone numbers obtained through the use of dictionary attacks or address-harvesting software.
- For the purposes of ascertaining the "annual turnover in Singapore" of an organisation or a person, the Bill clarifies that the amount is ascertained from the most recent audited accounts of the organisation / person available at the time the financial penalty is imposed.
- The PDPC will take the following factors into consideration when imposing the financial penalties: (i) the nature, gravity and duration of the non-compliance; (ii) the type and nature of the personal data affected; (iii) whether the organisation / person took any timely and effective mitigating actions; and (iv) the likely impact of the financial penalty on the organisation / person (e.g. the ability of the organisation / person to continue their usual activities).

Organisations and individuals should remain proactive in taking steps to ensure that they do not contravene the PDPA in light of the heavier penalties that can be imposed. Crucially, if organisations and individuals ever find themselves in breach, they should take immediate and effective action to remediate and reduce the impact of the breach. Such actions may serve to reduce the quantum of any financial penalty imposed.

2. Data Portability Obligation

There are exceptions to an organisation's obligation to carry out the individual's data porting request (i.e. Data Portability Obligation).

- The exceptions to the Data Portability Obligation have been clarified.
- Organisations are not required to transmit the individual's data if, for example, (i) the personal data, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organisation; (ii) transmitting the applicable data would unreasonably interfere with organisation's operations because of the repetitious nature of the request; or (iii) the burden or expense of transmitting the data is unreasonable to the organisation.
- Organisations, however, must preserve any applicable data that is specified in the individual's data porting request, regardless of whether the organisation has transmitted the data or not. Such preserved copies of the applicable data must be complete and accurate.
- The Data Portability Obligation would be introduced in phases and not take effect at the same time when the other Amendments take effect.

Organisations should begin to examine their operations and systems now with a view to preparing themselves to transfer data to third parties. System adjustments will take time to test and execute. Last minute system conversion or introduction is usually more expensive (if available) and inherently more risky.

Organisations should develop processes and measures to preserve accurate and complete copies of the data that is specified in the data porting request, for the duration that is be prescribed.

3. New Exceptions to the Collection, Use and Disclosure of an Individual's Personal Data without that Individual's Consent

New exceptions allow an organisation to collect, use and disclose an individual's personal data without their consent.

- In our previous update, we briefly mentioned two new exceptions to the consent requirement: (1) the Legitimate Interest exception; and (2) the Business Improvement exception. We elaborate on these exceptions.
- Legitimate Interest exception: Consent is not required where the collection, use and disclosure of the personal data is (1) in the legitimate interests of the organisation or another person; and (2) this interest outweighs any adverse effect on the individual.
- To rely on the legitimate interest exception, the organisation must (1) articulate what that legitimate interest might be; (2) conduct an assessment to determine whether the legitimate interest outweighs any adverse effect on the individual (and implement reasonable measure to eliminate / mitigate the adverse effect); and (3) provide the

individual with reasonable access to information about the organisation's collection, use or disclosure of the personal data.

- Business Improvement exception: Consent is not required if the organisation uses the personal data for a 'relevant purpose'. Broadly, a 'relevant purpose' includes: (i) improving any goods or services provided, or developing new goods or services, by the organisation; (ii) improving the methods or processes for the operations of the organisation; (iii) learning about and understanding the behaviour or preferences of the individual in relation to the goods / services provided by the organisation; or (iv) personalising or customising the goods / services for the individual.
- The business improvement exception applies only if (i) a reasonable person would consider the use of the personal data for the 'relevant purpose' to be appropriate in the circumstance; and (ii) the 'relevant purpose' cannot be achieved without using the personal data in an individually identifiable form.
- The business improvement exception can also apply to a group of companies (e.g. if the data is collected by an organisation from a related corporation for a 'relevant purpose') but the recipient of the data needs to implement and maintain appropriate safeguards for the personal data.

Organisations may now rely on these expanded exceptions to collect, use or disclose personal data. However, before the organisations are able to do so, they should conduct the appropriate assessment as required by the amendments introduced to the PDPA.

4. Updates to the Mandatory Breach Notification Requirement

Clarifications to the Mandatory Breach Notification Requirement

- A new deeming provision has been included; unauthorised access, collection, use, disclosure, copying or modification of personal data only within an organisation is deemed not to be a notifiable data breach.
- Data intermediaries that process personal data on behalf of or for the purposes of a public agency are now required under the Amendments to notify the public agency of the occurrence of a data breach when it has reason to believe that a data breach has occurred.
- The wording of when a data breach is a notifiable data breach has been amended from if the data breach "affects not fewer than the minimum number of affected individuals prescribed" (in the draft Bill) to "is, or is likely to be, of a significant scale". We expect that there would be guidance issued later as to what constitutes "significant scale".
- It has also been clarified that organisations must notify the PDPC of any notifiable data breach no later than 3 calendar days (as opposed to simply "3 days" in the draft Bill) after the organisation has made the assessment that a notifiable data breach has occurred.

Data intermediaries, regardless of whether they are processing personal data on behalf of public agencies or other organisations, must inform the public agency / organisation without undue delay when it has reason to believe that a data breach has occurred.

5. Additional Enforcement Measures Available

PDPC may now direct parties to mediate and has powers to review an organisation's refusal to comply with any access, correction or data porting request. Organisations can give voluntary undertakings to the PDPC.

- The PDPC may now refer any complaint made by an individual against an organisation to mediation even if the parties do not want to, if the PDPC is of the opinion that the complaint is more appropriately resolved by mediation. The PDPC may also direct the individual and the organisation to attempt to resolve the complaint in a manner directed by the PDPC.
- The PDPC is granted wide powers of review under the new Section 48H. The PDPC may review, for example: (i) an organisation's refusal to provide the individual with access to their personal data; (ii) a refusal by the organisation to correct the individual's personal data in accordance with a correction request; or (iii) a refusal by the organisation to transmit any applicable data pursuant to a data porting request or a failure to do within a reasonable time.
- Organisations may give written voluntary undertakings to the PDPC when the PDPC has reasonable grounds to believe that the organisation has not complied with the provisions of the PDPA. The undertaking can be in relation to the organisation taking a course of action within a specified time or to publicise the voluntary undertaking itself.
- The directions or written notices of the PDPC can now be registered in the District Court and the District Court is empowered to make a court order to enforce the PDPC's directions and written directions.

With these new measures, individuals, organisations and the PDPC have a wider variety of options available to them to enable compliance with the PDPA.

Organisations should be aware of the possibility of mediation, giving voluntary undertakings to the PDPC and the PDPC's powers of review if the organisation chooses to refuse an individual's correction, access or data porting requests.

If you have any questions regarding this article, please contact Gilbert Leong.

Dentons Rodyk thanks and acknowledges Senior Associate Desmond Chew, Associate Sherman Poon, and Practice Trainee Jonathan Soh for their contributions to this article.

Your Key Contacts

Gilbert Leong
Senior Partner, Singapore
D +65 6885 3638
gilbert.leong@dentons.com