DREW & NAPIER

Upcoming amendments to the Personal Data Protection Act 2012 and Personal Data Protection Regulations 2014

12 June 2020

LEGAL UPDATE

In this Update

The Ministry of Communications and Information and the Personal Data Protection Commission conducted a public consultation from 14 to 28 May 2020 to seek feedback on proposed amendments to the Personal Data Protection Act 2012 (No. 26 of 2012). The proposed amendments are set out in the draft Personal Data Protection (Amendment) Bill 2020 ("**draft Bill**") which was released during the public consultation.

Shortly after the public consultation on the draft Bill, on 1 June 2020, the Personal Data Protection Regulations 2014 was amended to permit overseas transfers of personal data to certain organisations which had been certified under the APEC Cross-border Privacy Rules system or Privacy Recognition for Processors system.

We discuss the proposed amendments and their implications for organisations, as well as recent amendments to the Personal Data Protection Regulations 2014 relating to overseas transfers of personal data, in this update.

INTRODUCTION

The Ministry of Communications and Information ("**MCI**") and the Personal Data Protection Commission ("**PDPC**") conducted a public consultation from 14 to 28 May 2020 to seek public feedback on proposed amendments to the Personal Data Protection Act 2012 (No. 26 of 2012) ("**PDPA**"). The proposed amendments are set out in the draft Personal Data Protection (Amendment) Bill 2020 ("**draft Bill**") which was released during the public consultation.

This represents the first comprehensive review of the PDPA since its enactment in 2012 and was preceded by three public consultations conducted by the PDPC from 2017 to 2019 on specific aspects of Singapore's data protection regime.

Shortly after the public consultation on the draft Bill, on 1 June 2020, the Personal Data Protection Regulations 2014 ("**PDP Regulations**") was amended to permit overseas transfers of personal data to certain organisations which had been certified under the APEC cross-border privacy rules ("**CBPR**") system or Privacy Recognition for Processors ("**PRP**") system.

In this Legal Update, we describe some of these amendments and proposed amendments, and their implications on organisations.

KEY PROPOSED AMENDMENTS IN THE DRAFT BILL

1. Expansion of financial penalties and enhanced enforcement powers and options for the PDPC

Increasing financial penalty cap

One of the more significant amendments proposed in the draft Bill is an increase in the maximum financial penalty for contraventions of the PDPA by organisations. Currently, where the PDPC is satisfied that an organisation has breached any of the provisions on data protection in Parts III to VI of the PDPA ("**Data Protection Provisions**"), it is empowered to impose a financial penalty of up to S$1 million or issue other remedial directions to the organisation. Under the draft Bill, the maximum financial penalty will be raised to **the higher of (a) 10% of an organisation's annual turnover or (b) S$1 million**. MCI's public consultation paper clarified that "annual turnover" refers to the organisation's annual gross turnover in Singapore.

Expansion of financial penalty regime

The financial penalty regime in the PDPA will also apply to some new areas under the draft Bill. In particular, it will apply to contraventions of the provisions relating to the Do Not Call registry in Part IX of the PDPA ("**Do Not Call Provisions**") as well as the new provisions against dictionary attacks and use of address-harvesting software in the new Part IXA of the PDPA.

Enhanced enforcement powers and options

The draft Bill also proposes to strengthen the PDPC's enforcement powers and empowers the PDPC to take alternative enforcement options. Some amendments to this effect include:

(a) Enhancing the effectiveness of undertakings by empowering the PDPC to accept statutory undertakings when the PDPC has reasonable grounds to believe that the organisation has been, is, or is likely to be non-compliant with the PDPA; and providing for a range of options for enforcing breaches of undertakings.

(b) Enabling the PDPC to (i) establish or approve one or more mediation schemes; and (ii) direct complaints to resolve disputes via mediation, without the need to secure consent of both parties to the complaint or dispute (although this does not prejudice the individual's right to private action under section 32 of the PDPA).

(c) Providing additional recourse for the PDPC to compel the attendance of witnesses and the provision of documents and information. Non-compliance constitutes an offence under the draft Bill.

2. Changes to strengthen accountability

To reflect the PDPC's increased emphasis on the accountability of organisations, the draft Bill inserts an explicit reference to accountability in Part III of the PDPA. This consolidates the PDPC's position that organisations are accountable for personal data in their possession or under their control, and are expected to be able to demonstrate compliance.

Further, the draft Bill makes increased use of accountability tools such as prescribed assessments (i.e. data protection impact assessments) in certain situations involving the collection and use of personal data without consent (see 'Changes to the Consent Framework' below).

3. Mandatory data breach notification regime

Currently, there is no express requirement in the PDPA for organisations to notify the PDPC or any other party when a data breach has occurred and the PDPC encourages organisations to make voluntary notifications.

The draft Bill seeks to introduce a mandatory data breach notification obligation which requires organisations to notify the PDPC within the specified timeline in the event of a qualifying data breach. In some cases, organisations are also required to notify the affected individuals.

"Data breach" is defined in the draft Bill as (a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or (b) the loss of any storage medium or device on which personal data is stored in circumstances where such disclosure, copying, modification or disposal is likely to occur.

Organisations are required to notify the PDPC of a data breach that:

(a) **is likely to result in significant harm or impact to the individuals to whom the data relates** (e.g. if it affects any prescribed class of personal data); or

(b) **is of a significant scale** (i.e. if 500 or more individuals are affected).

Where an organisation has reason to believe that a data breach has occurred, it must conduct, in a reasonable and expeditious manner and in accordance with any prescribed requirements, an assessment as to whether it is notifiable.

Organisations must notify the PDPC as soon as practicable, but in any case, no later than three calendar days after determining that the breach meets the notification criteria.

Organisations are required to notify affected individuals if the data breach is likely to result in significant harm or impact to the individuals. However, this is subject to the following exceptions in the draft Bill:

(a) **Remedial action exception:** where the organisation has taken actions in accordance with any prescribed requirements which renders it unlikely that the breach will result in significant harm to affected individuals.

(b) **Technological protection exception:** where the personal data that was compromised by the data breach is subject to technological protection (e.g. encryption) such that the data breach is unlikely to result in significant harm to the affected individuals.

Further, organisations are prohibited from notifying affected individuals if instructed by a prescribed law enforcement agency or directed as such by PDPC, e.g. in circumstances where such notification may compromise investigations or prejudice enforcement efforts.

Where a data breach involves personal data which is being processed by a data intermediary ("**DI**") on behalf and for the purposes of another organisation, the DI must notify that organisation without undue delay.

4. Data portability obligation

The draft Bill introduces a new Data Portability Obligation, which requires an organisation to, at the request of an individual, transmit personal data that is in the organisation's possession or under its control, to another organisation in a commonly used machine-readable format. Nonetheless, the application of the obligation is envisaged to be limited and is subject to certain exceptions and conditions, such as:

(a) The relevant data is limited to **user provided data and user activity data held in electronic form** (which may include business contact information and personal data of third parties, although the provision of the latter is subject to certain safeguards). The obligation also does not apply to derived personal data.

(b) The requesting individual has an **existing, direct relationship with the organisation**.

(c) The **receiving organisation has a presence in Singapore**.

The proposed exceptions to the Data Portability Obligation mirrors those of the Access Obligation under Fifth Schedule (although note that the exceptions with respect to third-party data will be amended to carve out user provided data and user activity data), for instance, data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation.

The PDPC will also have the power to review (a) any refusal to port data; (b) the failure to port data within a reasonable time, and (c) the fees imposed to port data, and to issue related directions.

Furthermore, the draft Bill proposes to have the Data Portability Obligation come into effect with the issuance of regulations, which would prescribe further details such as a whitelist of data categories to which the obligation applies; the technical and process details for the transmission; relevant data porting request models; and certain safeguards for individuals.

5. Changes to the Consent Framework

Introduction of new exceptions to consent

The PDPA is a consent-based regime and requires organisations to obtain consent for the collection, use or disclosure of personal data, subject to the exceptions currently set out in the Second, Third, and Fourth Schedules of the PDPA. The draft Bill provides for two new exceptions to the consent requirement:

(a) '**Legitimate interests' exception:** It enables organisations to collect, use or disclose personal data without consent in circumstances where there is a need to protect legitimate interests that will have economic, social, security or other benefits for the public (or a section thereof). Such benefits to the public must outweigh any adverse impact to the individual, and organisations wishing to rely on this 'legitimate interests' basis must fulfil certain requirements, e.g. conducting a risk and impact assessment as prescribed.

(b) **'Business improvement' exception:** It clarifies that subject to the fulfilment of certain conditions, organisations can use personal data for the purposes of: (i) operational efficiency and service improvements; (ii) product and service development; or (iii) knowing customers better. The proposed business improvement exception only applies to the use of such data, and not to the collection or disclosure of the same.

The draft Bill also proposes to make revisions to using personal data in research without consent, to introduce certain conditions (i.e. requiring the use of personal data to not have an adverse effect on individuals, and that the results of the research not to not be published in a form which identifies any individuals), to ensure appropriate accountability measures are in place when organisations rely on this exception.

Expansion of deemed consent

Currently, section 15 of the PDPA provides that an individual is deemed to consent to the collection, use and disclosure of his personal data for a purpose if: (a) the individual voluntarily provides the personal data to the organisation for that purpose; and (b) it is reasonable that the individual would do so. The draft Bill seeks to expand the circumstances whereby deemed consent would apply to include the following:

(a) **Deemed consent by contractual necessity:** Consent is deemed to have been given for the use and disclosure of personal data where it is reasonably necessary for the conclusion or performance of a contract or transaction between the individual and the organisation.

(b) **Deemed consent by notification:** Subject to fulfilling certain conditions, consent is deemed to have been given if: (i) the organisation provides appropriate notification as to the purpose of such processing, with a reasonable period for the individual to opt-out; and (ii) the individual did not opt-out within the period.

6. Removal of exemption for public agencies

Currently, under section 4 the PDPA, certain categories of organisations are carved out of the application of the Data Protection Provisions, such as employees acting in the course of their employment with an organisation; and organisations acting on behalf of a public agency in relation to the collection, use or disclosure of personal data.

The draft Bill removes the exemption for such organisations acting on behalf of public agencies in relation to the collection, use or disclosure of personal data, and introduces, subject to various defences and safeguards, certain new offences under the PDPA to hold individuals (who may be employees) accountable for the knowing or reckless unauthorised handling (e.g. use, disclosure) of personal data.

7. Other amendments in the draft Bill

Requirements to preserve personal data following access and porting requests

Under the draft Bill, organisations will be required to preserve a copy of the personal data requested pursuant to an access request for a prescribed period (i.e. at least 30 calendar days) after the rejection of the request or until the individual has exhausted the right to reconsider or appeal, whichever is later.

Amendments to the Do Not Call Provisions and the Spam Control Act

The draft Bill intends to make various changes to the regime governing unsolicited commercial messages under the PDPA and the Spam Control Act (Cap. 311A) ("**SCA**"). These changes include:

(a) Inserting a new Part IXA into the PDPA with provisions prohibiting the sending of specified messages to telephone numbers obtained through the use of dictionary attacks and address harvesting software.

(b) Imposing a new obligation on third-party checkers to communicate accurate Do Not Call register query results to organisations on whose behalf they are checking the register.

(c) Amending the SCA to cover messages sent to Instant Messaging ("**IM**") accounts via IM platforms, including platforms such as Telegram and WeChat.

8. Transfers of personal data to APEC CBPR- and PRP-certified organisations under the PDP Regulations

Singapore became the sixth APEC economy to participate in the CBPR system and the second APEC economy to participate in the PRP system in 2018. Since then, PDPC has been active in promoting measures for organisation to certify their compliance with the PDPA, including a Data Protection Trustmark regime which was introduced in 2019.

On 1 June 2020, the PDPC amended the PDP Regulations to permit overseas transfers of personal data to organisations which are APEC CBPR- or PRP-certified.

By way of background, section 26 of the PDPA, commonly referred to as the Transfer Limitation Obligation, provides that an organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDP Regulations to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA.

Under the PDP Regulations, organisations are generally permitted to transfer personal data overseas if they have taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations to provide the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.

Under the amended PDP Regulations, an overseas recipient of personal data will now be considered to be legally bound to provide comparable protection for the transferred personal data if it holds an APEC CBPR or PRP certification that is granted or recognised under the laws of the country or territory to which the personal data is transferred.

This is a welcome addition as it would allow organisations in Singapore to transfer personal data overseas to CBPR- or PRP-certified organisations more easily without meeting additional requirements. However, organisations that are seeking to rely on this provision should still ensure that they carry out the necessary due diligence to determine that the overseas recipient is indeed CBPR- or PRP-certified under the laws of the country or territory in question.

CONCLUSION

The proposed amendments to the PDPA, as set out in the draft Bill, as well as the amendments to the PDP Regulations, demonstrate the PDPC's shift towards a risk-based, accountability approach to data protection. They broadly signify that organisations should similarly adapt or change their approach to PDPA compliance and data protection in general to meet the changing needs and expectations of individuals, regulators and society at large.

For questions or comments, please contact:

Lim Chong Kin
Managing Director, Corporate & Finance
Co-Head, Data Protection, Privacy & Cybersecurity Practice
T: +65 6531 4110
E: chongkin.lim@drewnapier.com

David N. Alfred
Director, Corporate & Finance
Co-Head, Data Protection, Privacy & Cybersecurity Practice
T: +65 6531 2342
E: david.alfred@drewnapier.com

Benjamin Gaw
Director, Healthcare & Life Sciences
T: +65 6531 2393
E: benjamin.gaw@drewnapier.com

Albert Pichlmaier
Senior Cyber-Security Engineer
T: +65 6531 4108
E: albert.pichlmaier@drewnapier.com

Janice Lee
Associate Director, Corporate & Finance
T: +65 6531 2323
E: janice.lee@drewnapier.com

Charis Seow
Associate Director, Corporate & Finance
T: +65 6531 2713
E: charis.seow@drewnapier.com

Drew & Napier LLC

10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com

T : +65 6535 0733
T : +65 9726 0573 (After Hours)
E : mail@drewnapier.com

DREW & NAPIER