西村あさひ法律事務所
NISHIMURA & ASAHI
Asia Newsletter

SINGAPORE: SUMMARY OF THE PERSONAL DATA PROTECTION (AMENDMENT) ACT 2020 – KEY AMENDMENTS TO THE PERSONAL DATA PROTECTION ACT (NO. 26 OF 2012)

Melissa Tan, Chin Su Xian, Masato Yamanaka, Tomomi Murata

1. Introduction

On 29 January 2021, the Personal Data Protection Commission ("**PDPC**") announced that the Personal Data Protection (Amendment) Act 2020 (No. 40 of 2020) ("**Amendment Act**") will take effect in phases from 1 February 2021 to amend the Personal Data Protection Act (No. 26 of 2012) ("**PDPA**").

The key amendments introduced by the Amendment Act will, amongst others:

(a) expand the current deemed consent framework;
(b) introduce new and revised exceptions to the consent requirement;
(c) introduce a new mechanism for mandatory data breach notification;
(d) introduce new offences for mishandling of personal data;
(e) make changes to the regime governing unsolicited commercial messages;
(f) increase the scope of financial penalties (not yet taken effect as of 1 February 2021); and
(g) introduce a new right to data portability (not yet taken effect as of 1 February 2021).

2. Background

Since the enactment of the PDPA in 2012, a comprehensive review has not been conducted until recently[1]. Together with the PDPC, the Ministry of Communications and Information ("**MCI**") conducted a public consultation in May 2020 to seek feedback from the

[1] The most recent public consultation on the draft Personal Data Protection (Amendment) Bill (prior to the enactment of the PDPA Amendment Act) was conducted from 14 May 2020 to 28 May 2020, being preceded by three public consultations conducted by the PDPC from 2017 to 2019 on specific aspects of Singapore's data protection regime.

public on proposed amendments to the PDPA. These amendments were proposed to address Singapore's evolving digital economy needs and to bring it closer in line with higher global standards.

According to a press release by MCI and PDPC issued on 2 November 2020[2], there has been exponential growth in the amount of data available globally, due to an increased use of social media and online activities. Data has become an integral part of our lives, society, and economy. Consumers today are used to highly personalised services that are achieved through data-driven technology and organisations are expected to be accountable for protecting and using all the different types of data responsibly.

To benefit the citizens and the economy, the PDPA has been amended to:

(a) strengthen consumer trust and protection through organisational accountability;
(b) enhance effectiveness of enforcement;
(c) enhance consumer autonomy; and
(d) enhance data use for innovation.

3. Key Amendments introduced under the Amendment Act

3.1 Expansion of Deemed Consent Framework

The deemed consent framework[3] under the PDPA has been expanded by the addition of two new forms of deemed consent, namely deemed consent by contractual necessity and deemed consent by notification. This expands the circumstances where deemed consent under section 15 of the PDPA would apply to allow organisations to collect, use and disclose personal data, whereby an individual will be deemed to have given consent for:

(a) under deemed consent by contractual necessity: the use and disclosure of personal data if such use and disclosure is reasonably necessary for the conclusion or performance of a contract or transaction between the individual and the organization. This extends to disclosures by such organization to other organizations downstream where the use or disclosure is reasonably necessary to conclude or perform the contract between the individual and the first-mentioned organization;[4] and

(b) under deemed consent by notification: the collection, use and disclosure subject to fulfilling certain conditions, if (i) the organization 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.[5] For an organisation to rely on this exception, an organisation is required to:

    (i) conduct an assessment to determine that the collection, use or disclosure is unlikely to have an adverse effect on the individual;
    (ii) take reasonable steps to ensure that the notification provided to the individual has been adequate; and
    (iii) provide a reasonable opt-out period.

---

2 Please refer to https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/11/amendments-to-the-personal-data-protection-act-and-spam-control-act-passed.

3 Under the deemed consent framework prior to the amendments, section 15 of the PDPA generally 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 organization for that purpose; and (b) it is reasonable that the individual would do so.

4 Please see paragraph 12.22 of the Advisory Guidelines on Key Concepts in the PDPA issued by the PDPC (revised 1 February 2021) (available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en) ("**Advisory Guidelines**").

5 Please see paragraphs 12.23 to 12.26 of the Advisory Guidelines.

Deemed consent by notification is especially useful for organisations wishing to use or disclose personal data for other purposes where the individual has not consented at the time of collection. Furthermore, the organization will have to retain a copy of the assessment conducted throughout the period the organization relies on the deemed consent by notification.

3.2 New and Revised Exceptions to Consent Requirement

The PDPA requires organisations to obtain consent from individuals for the collection, use or disclosure of personal data subject to exceptions currently set out under the First and Second Schedules of the PDPA (prior to the amendments, under the (old) Second, Third and Fourth Schedules of the PDPA).

The two new exceptions introduced under the Amendment Act are the:

(a) legitimate interests exception: consent for the collection, use or disclosure of personal data does not need to be obtained if there is a need to protect legitimate interests. Such benefits to the public must outweigh any adverse impact to the individual, and organizations wishing to rely on this 'legitimate interests' basis must fulfil certain requirements (e.g. conducting a risk and impact assessment as prescribed);[6] and

(b) business improvement exception: consent for the use of personal data does not need to be obtained if the organization uses the personal data for the purposes of:

(i) improving, enhancing or developing new goods or services;
(ii) improving, enhancing or developing new methods or processes for business operations in relation to the organization's goods and services;
(iii) learning about and understanding the behaviour and preferences of individuals in relation to the goods or services provided by the organisation; or
(iv) identifying goods or services that may be suitable for individuals or personalising or customizing any such goods or services for such individuals;

subject to the fulfilment of certain conditions (i.e. whereby the purpose cannot reasonably be achieved without using the personal data in an individually identifiable form and the organization's use of personal data for such purpose is one that a reasonable person would consider appropriate in the circumstances).[7]

It should be noted that this exception only applies to the use of personal data and does not extend to the collection or disclosure of the same.

Further changes to existing exceptions include:

(a) additional conditions to the existing research exception: that (i) the results of the research will not be used to make any decision that affects the individual, and (ii) in the event that the results of the research are published, the organisation must publish the results in a form that does not identify the individual;[8] and

[6] Please see paragraphs 12.56 to 12.70 of the Advisory Guidelines.

[7] Please see paragraphs 12.71 to 12.77 of the Advisory Guidelines.

[8] Please see paragraphs 12.80 to 12.83 of the Advisory Guidelines.

(b) expanded scope of the business asset transaction[9] exception: to include the disclosure of personal data of independent contractors as well, and that this exception will be extended to include transactions such as mergers and acquisitions, sale of shares, transfer of controlling power or interests, corporate restructuring and reorganisations in cases that involve "an interest in an organisation" or amalgamations with or transfers to related corporations.

3.3 Mandatory Data Breach Notification

This is a new mechanism that has been introduced under the Amendment Act that requires organisations to notify the PDPC of any data breach that:[10]

(a) results in, or is likely to result in, significant harm to affected individuals; or
(b) is of a significant scale.

Organisations are required to conduct assessments of data breaches that are believed to have occurred in a reasonable and expeditious manner, generally within thirty (30) calendar days.[11] Data intermediaries that process the personal data on behalf and for the purposes of another organisation (including a public agency) are also required to notify that other organisation or public agency of a data breach detected without undue delay.

In determining whether a data breach is notifiable:[12]

(a) a data breach is deemed to result in significant harm[13] to an individual if the data breach relates to significant personal information, in particular: (i) an individual's name or alias or identification number, in combination with certain prescribed information relating to, amongst others, identification of vulnerable individuals, insurance information, financial information, specified medical information; or (ii) the individual's account identifier, password, or other access code or data in respect of an account held with a bank or a finance company; or
(b) a data breach is considered to be of a significant scale[14] if five hundred (500) or more individuals have had their data compromised in the breach.

Organisations are required to notify the PDPC as soon as practicable, and no later than three (3) calendar days once the data breach is assessed to be notifiable. Notifications to affected individuals (where required) are also required to be made as soon as practicable, at the same time or after notifying the PDPC.

Notwithstanding the above, organisations are not required to notify affected individuals (but still must notify the PDPC) where either of the following exceptions[15] apply, rendering it unlikely that the data breach will result in significant harm to the affected individual:

(a) remedial action exception: timely remedial actions have been taken by the organisation or its data intermediary, on or

---

9 Under the PDPA prior to the amendments, an organisation which is undertaking a "business asset transaction", defined as the purchase, sale, lease, merger or amalgamation or any other acquisition, disposal or financing of an organisation or a portion of an organisation, may disclose personal data of its employees, customers, directors, officers or shareholders without obtaining such individuals' consents.

10 "Data Breach" is defined under the new section 26A of the PDPA 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.

11 Please see paragraphs 20.3 to 20.5 of the Advisory Guidelines.

12 Please see sections 3 and 4 of the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (available at: https://sso.agc.gov.sg/SL-Supp/S64-2021/Published/20210129?DocDate=20210129).

13 Please see paragraphs 20.13 to 20.18 of the Advisory Guidelines.

14 Please see paragraphs 20.19 to 20.21 of the Advisory Guidelines.

15 Please see section 26D(5) of the PDPA and paragraphs 20.26 to 20.31 of the Advisory Guidelines.

after assessing that the data breach is a notifiable data breach, in accordance with any prescribed requirements; or

(b) technological protection exception: appropriate technological measures (e.g. encryption, password-protection, etc) have been taken, prior to the occurrence of the notifiable data breach, such that the personal data is unintelligible or inaccessible to unauthorised persons.

3.4 New Offences for Mishandling of Personal Data

Three new offences have been introduced under the Amendment Act that target actions by individuals for egregious mishandling of personal data in the possession of or under the control of an organisation (including a public agency).[16] These include offences for:

(a) knowing or reckless unauthorised disclosure of personal data;
(b) knowing or reckless improper use of personal data for wrongful gain or causing wrongful loss to any person; and
(c) 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 two (2) years.

3.5. Changes to the regime governing unsolicited commercial messages

Amendments have also been made to the regime governing unsolicited commercial messages under the PDPA and the Spam Control Act (Cap. 311A) ("**SCA**"). These include:

(a) the prohibition of sending specified messages to telephone numbers obtained through the use of dictionary attacks and address harvesting software;
(b) imposing a new obligation on third-party Do Not Call ("**DNC**') checkers to communicate accurate DNC register query results to organisations on whose behalf they are checking; and
(c) extending the scope of the SCA to cover messages sent to instant messaging (**"IM**') accounts via IM platforms, such as Telegram and WeChat.

3.6 Increased Financial Penalties

These have not yet taken effect as of 1 February 2021 but are expected to come into effect in the near future.

The financial penalties which may be imposed on organisations which are in breach of the PDPA will be increased significantly. Currently, the existing maximum fine is S$1 million. After the provisions take effect, the penalty will be a maximum penalty of S$1 million or ten per cent (10%) of the organisation's annual turnover in Singapore, whichever is higher. These revised penalties are expected to take effect no later than 1 February 2022; and

3.7 Right to Data Portability[17]

As of 1 February 2021, this has yet to take effect but is expected to come into effect in the near future.

[16] Please see Part IXB of the PDPA and paragraphs 22 to 23 of the Advisory Guidelines.

[17] This will be covered under a new Part VIB (to be inserted as new sections 26F to 26J) of the PDPA.

Individuals will be granted a new right to data portability meaning that an individual will be able to request that an organisation transmit the individual's personal data held by that organisation to another organisation in a commonly used machine-readable format. However, this obligation to transmit personal data is subject to the following conditions:

(a) the relevant data must be user provided data and user activity data held in electronic form;
(b) the obligation does not apply to derived personal data;
(c) the requesting individual must have an existing, direct relationship with the organization; and
(d) the receiving organization must have a presence in Singapore.

Organizations will be required to preserve a copy of the personal data requested pursuant to a porting or access request for a prescribed period (i.e. at least thirty (30) calendar days)[18] after the rejection of the request or until the individual has exhausted the right to reconsider or appeal, whichever is later.

4. Key Takeaways

Following these changes, it is vital for organisations to review their existing data protection policies and consent provisions for compliance with existing provisions and review their current collection, use and disclosure of personal data in light of the revised framework.

It is recommended for organisations to put in place a robust data breach protection and assessment framework and ensure adequate protections and response procedures are in place in case of data breach incidents. Moreover, organisations should provide regular internal training sessions to introduce amendments to policies and procedures so that employees are familiar with the updated regime.

The amendments demonstrate PDPC's ability to recognise and respond to the advancements in technology in the course of business and commerce and hence, developments to the PDPA are expected to keep up with practical realities.

[18] Please note that this will be covered under the new section 22A of the PDPA. Please also see section 8 of the Personal Data Protection Regulations 2021 (effective as of 1 February 2021) (available at: https://sso.agc.gov.sg/SL/PDPA2012-S63-2021?DocDate=20210129&Timeline=On#pr8-) and paragraph 15.42 of the Advisory Guidelines issued by the PDPC.

Melissa Tan
Bayfront Law LLC (formal law alliance with Nishimura & Asahi Singapore Office)
Director
melissa.tan@bayfrontlaw.sg

Melissa Tan's practice area is non-contentious corporate law and commercial law, specializing in domestic and cross-border mergers and acquisitions.

Her practice encompasses negotiating and drafting documentation for commercial matters as well as regulatory and compliance advisory work for private companies in Singapore.

Melissa graduated from the National University of Singapore and is called to the Singapore bar.

Chin Su Xian
Bayfront Law LLC (formal law alliance with Nishimura & Asahi Singapore Office)
Attorney-at-Law (Admitted in Singapore)
suxian.chin@bayfrontlaw.sg

Su Xian is a Senior Associate and works with the corporate team. Her work focuses on mergers and acquisitions, corporate finance, corporate governance, compliance, and employment matters.

She graduated from University of Tasmania and is called to the Singapore Bar in 2014.

Masato Yamanaka
Nishimura & Asahi Singapore Office Co-representative Partner
m.yamanaka@nishimura.com

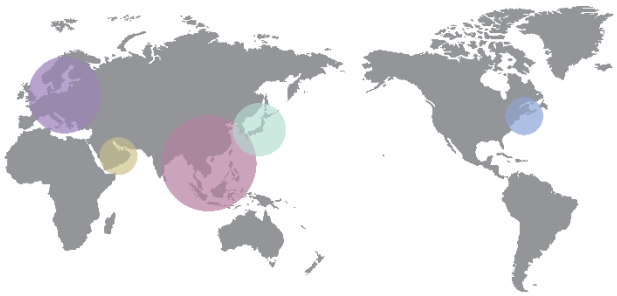
Masato Yamanaka graduated from Keio University (LL.B.) in 2000 and qualified as a lawyer in Japan in 2002.

He has been based in Singapore since 2012 to provide support for Japanese clients with businesses in Singapore, Malaysia and Indonesia as well as non-Japanese clients seeking investment opportunities in the Japanese market.

Tomomi Murata
Nishimura & Asahi Singapore Office Attorney-at-Law
t.murata@nishimura.com

Tomomi Murata was admitted to practice in Japan in 2010. She worked for N&A Hanoi Office from 2016 to 2017, and started working for Singapore Office from April 2019. She has been involved in many M&A transactions and handled a variety of issues especially faced by Japanese companies in southeast Asia. She also focuses on international construction.

Nishimura & Asahi has 18 offices throughout Japan and in the markets that matter, with Asia as the starting point.



Tokyo
Otemon Tower, 1-1-2 Otemachi, Chiyoda-ku, Tokyo 100-8124 Japan
Tel +81-3-6250-6200 +81-3-6250-7210 (Nishimura & Asahi LPC Principal Office)

Nagoya
Tel +81-52-533-2590
LPC Partner Hiroki Fujii

Osaka
Tel +81-6-6366-3013
LPC Partners Hiromune Usuki
Taisuke Igaki
Yuichiro Hirota
Masanori Ban

Fukuoka
Tel +81-92-717-7300
LPC Partners Tsuneyasu Ozaki
Kengo Takaki
Yasuko Maita

New York
Nishimura & Asahi NY LLP
Tel +1-212-830-1600
E-mail info_ny@nishimura.com
Managing Partner Katsuyuki Yamaguchi
Vice Managing Partner Megumi Shimizu
Partners Kaoru Tatsumi
Yusuke Urano

Dubai
Tel +971-4-386-3456
E-mail info_dubai@nishimura.com
Counsel Masao Morishita

Frankfurt (main office)
Nishimura & Asahi Europe
Rechtsanwaltsgesellschaft mbH
Tel +49-(0)69-870-077-620

Düsseldorf (branch office)
Nishimura & Asahi Europe
Rechtsanwaltsgesellschaft mbH
Tel +49-(0)211-5403-9512

E-mail info_europe@eml.nishimura.com
Co-representatives Noriya Ishikawa
Dominik Kruse

Bangkok
Tel +66-2-126-9100
E-mail info_bangkok@nishimura.com
Co-representatives Chavalit Uttasart
Hideshi Obara
Jirapong Sriwat

Jakarta*1
Walalangi & Partners
Tel +62-21-5080-8600
E-mail info@wplaws.com
Representative Luky Walalangi

Rosetini & Partners Law Firm
Tel +62-21-2933-3617
E-mail info_jakarta@nishimura.com
Partner Noriaki Machida

Yangon
Tel +95-1-8382632
E-mail info_yangon@nishimura.com
Representative Yusuke Yukawa
Vice Representative Isamu Imaizumi

Beijing
Tel +86-10-8588-8600
E-mail info_beijing@nishimura.com
Chief Representative Azusa Nakashima
Representative Masashi Shiga

Shanghai
Tel +86-21-6171-3748
E-mail info_shanghai@nishimura.com
Chief Representative Takashi Nomura
Representatives Satoshi Tojo
Seita Kinoshita

Singapore
Tel +65-6922-7670
E-mail info_singapore@nishimura.com
Co-representatives Masato Yamanaka
Shintaro Uno
Partners Masataka Sato
Yuji Senda
Ikang Dharyanto

Note: We are in formal law alliance with Bayfront Law LLC, a Singapore law practice, under name of Nishimura & Asahi-Bayfront Law Alliance.

Okada Law Firm (Hong Kong)*2
Tel +852-2336-8586
E-mail s.okada@nishimura.com
Representative Saori Okada

Hanoi
Tel +84-24-3946-0870
E-mail info_hanoi@nishimura.com
Partner for Vietnam offices Hikaru Oguchi
Representative Akira Hiramatsu

Ho Chi Minh City
Tel +84-28-3821-4432
E-mail info_hcmc@nishimura.com
Partner for Vietnam offices Hikaru Oguchi
Representative Partners Kazuhide Ohya
Vu Le Bang
Ha Hoang Loc

Taipei
Nishimura & Asahi Taiwan
Tel +886-2-8729-7900
E-mail info_taipei@nishimura.com
Co-Representatives Ing-Chian Sun
Sheng-Chieh Chang

*1 Associate office *2 Affiliate office

Public Relations Section, Nishimura & Asahi
Otemon Tower, 1-1-2 Otemachi, Chiyoda-ku, Tokyo 100-8124, JAPAN
URL: https://www.nishimura.com/en