Significant Changes Ahead for the Personal Data Protection Act

Overview

Following a series of public consultations over the past three years, the Singapore Parliament has passed amendments to the Personal Data Protection Act ("**PDPA**") on 2 November 2020. The amendments are extensive and take into account technological advances, new business models and global developments in data protection legislation. The key amendments are further discussed below:

(a) Strengthening Accountability

Explicit reference to storage mediums/devices

Under existing guidelines, a data breach refers to an incident exposing personal data in an organisation's possession or control to the risks of unauthorised access, collection, use, disclosure, copying, modification, disposal or other similar risks. The amendments will incorporate the concept of a data breach into the PDPA and will expand the definition to cover the loss of any storage medium or device on which personal data is stored in circumstances where unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

The protection obligation under section 24 of the PDPA will similarly be amended to require organisations to make reasonable security arrangements to prevent the loss of any storage medium or device on which personal data in their possession or under their control is stored.

Mandatory data breach notification requirement

It will become *mandatory* for organisations to:

- conduct an assessment of whether a data breach is notifiable in accordance with prescribed requirements; and
- notify the Personal Data Protection Commission ("**PDPC**"), no later than 3 calendar days after the day of determination that a data breach is notifiable, if the:

Significant Harm	• Data breach results in, or is likely to result in, significant harm to individuals to whom any personal data relates to ("**affected individuals**"). To this end, a data breach is deemed to result in significant harm to an individual if the data breach is in relation to any prescribed personal data or class of personal data relating to the individual or in any other prescribed circumstances.
Significant Scale	• Data breach is, or is likely to be, of a significant scale. In this regard, a data breach is deemed to be of a significant scale if the data breach affects not fewer than the prescribed number of affected individuals (stated to be 500 or more in the public consultation) or in other prescribed circumstances.

Organisations will also be required to notify the affected individuals if the data breach is likely to result in significant harm to them, unless a specified exception applies.

New "egregious mishandling" offences

Individuals can now be prosecuted for the "egregious mishandling" of personal data. Criminal offences will be introduced for the knowing or reckless: (1) unauthorised disclosure of personal data; (2) unauthorised use of personal data for a gain for the individual or another person or causing harm / loss to another individual / person; and (3) unauthorised re-identification of personal data.

The penalties for each of the abovementioned offences is a fine not exceeding SGD 5,000 or imprisonment for a term not exceeding 2 years or both. The PDPC has also stated that it intends to clarify in advisory guidelines, the situations which the new offences are not intended to cover.

(b) Enabling Meaningful Consent

Expanded concept of deemed consent

While the PDPA previously provided only for deemed consent by conduct, the amendments will expand the concept of deemed consent to cover the following:

- **deemed consent by contractual necessity**, where the collection, use or disclosure of personal data is reasonably necessary to conclude or perform a contract or transaction between the individual and organisation; and
- **deemed consent by notification**, where individuals have been notified of the purpose of the intended collection, use or disclosure of personal data, and given a reasonable opportunity to opt-out, and have not opted out.

However, organisations seeking to rely on the expanded concepts of deemed consent may be required to fulfil certain requirements, such as the taking of reasonable steps to bring certain information to the individual's attention before the organisation is able to rely on deemed consent by notification. Accordingly, organisations should review existing data protection policies and processes to account for the prescribed requirements.

New exceptions to the consent obligation – legitimate interests and business improvement

There will be two new exceptions to the consent obligation, namely:

Legitimate Interests Exception	• Subject to certain requirements, an organisation will be able to collect, use or disclose personal data where it is for the legitimate interests of the organisation or another person and the legitimate interests of the organisation or other person outweigh any adverse effect on the individual. • An organisation relying on this exception will have to provide individuals with reasonable access to information about the organisation's collection, use or disclosure of personal data (e.g., in its public data protection policies).

Business Improvement Exception	• Organisations may use personal data properly collected for prescribed business improvement purposes, which include: (a) improving, enhancing or developing new goods or services/new methods or processes for business operations in relation to the organisations' goods and services; (b) learning or understanding behaviour and preferences of individuals; and (c) identifying goods or services that may be suitable for individuals. • In addition, where groups of companies are concerned, an organisation (X) may collect from a related corporation (Y) and use, and Y may disclose to X, personal data about an individual without consent for any of the specified business improvement purposes, provided that the specified conditions are met.

These exceptions may be of particular interest to organisations and corporate groups wishing to utilise personal data for the purposes of data analytics, product and service development and enhancing customer experience.

(c) Improving Consumer Autonomy and Rights

Data portability

It will be *mandatory* for organisations to transmit, at an individual's request, his or her personal data that is in the organisation's possession or under its control, to another organisation in a commonly used machine-readable format. It is intended that the new data portability obligation will apply to applicable data that is the subject of a data porting request regardless of whether the applicable data is stored or processed in, or transmitted from, Singapore or a foreign country or territory. In particular:

- **Scope of Transmission**: Organisations will only be required to transmit data to other organisations that have a presence in Singapore (i.e., formed/recognised, or resident/having, an office or place of business in Singapore or an applicable country).

- **Scope of Data**: The data portability obligation will only apply to applicable data that is in electronic form on the date of the porting request, and which was collected or created by the porting organisation within the prescribed period.

- **Exceptions**: The exceptions to the data portability obligation will be similar to the exceptions to the access obligation under section 21 of the PDPA. Notably, the data portability obligation will also exclude "derived personal data", i.e., personal data derived by an organisation in the course of business from other personal data.

The remaining details (e.g., class of organisations and data to which this obligation applies/format of transmission) will be prescribed in the relevant regulations. It is expected that sector-specific codes of practice and/or other regulatory instruments will be developed to provide implementation clarity for organisations required to comply with this obligation.

Expanded protection from unsolicited messages

To further deter spammers using technology to indiscriminately send unsolicited commercial messages, there will be new prohibitions against sending of messages with a "Singapore link" to any telephone numbers generated or obtained through the use of:

- **Dictionary Attacks**: method by which the telephone number of a recipient is obtained using automated means that generates possible telephone numbers by combining numbers into numerous permutations; and
- **Address Harvesting Software**: software specifically designed or marketed for: (a) searching the Internet for telephone numbers; and (b) collecting, compiling, capturing or otherwise harvesting the telephone numbers.

The Spam Control Act will also be amended to cover commercial text messages sent to instant messaging accounts and in bulk.

(d) Strengthening Effectiveness of Enforcement

Enhanced enforcement powers

The maximum financial penalty that the PDPC may impose on an organisation for contravention of the applicable provisions under the PDPA will be increased to up to **10% of an organisation's annual turnover in Singapore**, unless the organisation's annual turnover in Singapore does not exceed SGD $10 million (in which case the maximum penalty remains at SGD $1 million).

Minister for Communications and Information S. Iswaran stated during parliamentary debates that the revised financial penalty cap will come into effect no earlier than one year after the amendments come into force, and further gave the assurance that, notwithstanding the increased financial penalty cap, financial penalties imposed will continue to be proportionate to the severity of the data breach.

Concluding Remarks

The amendments to the PDPA and the enhancements to the enforcement regime signal the expectation that businesses should devote resources and pay close attention to how personal data is being processed and handled.

At the same time, in widening the ambit of deemed consent and introducing the concept of legitimate interests, businesses should now have greater flexibility to tap on their personal data repositories and data analytics tools to improve their business offerings.

Individuals with their new data portability rights may also have greater choice when switching service providers, since their personal data records held by their incumbent providers can be migrated.

Organisations should thus:

- proactively review their existing policies and practices for handling personal data to ensure that they are updated to reflect the new requirements of the PDPA;

- consider updating their data protection policies if they wish to avail of the new bases for processing personal data; and

- review their agreements with third party service providers to ensure that they are ready to meet the new requirements of the PDPA.

If you would like information or assistance on the above or any other area of law, you may wish to contact the partner at WongPartnership whom you normally work with or any of the following partners:

LAM Chung Nian
Head – Intellectual Property,
Technology & Data Group
d +65 6416 8271
e chungnian.lam
@wongpartnership.com
Click here to view Chung Nian's CV.

Kylie PEH
Partner – Intellectual Property,
Technology & Data Group
d +65 6416 8259
e kylie.peh
@wongpartnership.com
Click here to view Kylie's CV.

Connect with WongPartnership.

WPG MEMBERS AND OFFICES

- contactus@wongpartnership.com

SINGAPORE

-
WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
t +65 6416 8000
f +65 6532 5711/5722

CHINA

-
WongPartnership LLP
Beijing Representative Office
Unit 3111 China World Office 2
1 Jianguomenwai Avenue, Chaoyang District
Beijing 100004, PRC
t +86 10 6505 6900
f +86 10 6505 2562

-
WongPartnership LLP
Shanghai Representative Office
Unit 1015 Corporate Avenue 1
222 Hubin Road
Shanghai 200021, PRC
t +86 21 6340 3131
f +86 21 6340 3315

MYANMAR

-
WongPartnership Myanmar Ltd.
Junction City Tower, #09-03
Bogyoke Aung San Road
Pabedan Township, Yangon
Myanmar
t +95 1 925 3737
f +95 1 925 3742

INDONESIA

-
Makes & Partners Law Firm
Menara Batavia, 7th Floor
Jl. KH. Mas Mansyur Kav. 126
Jakarta 10220, Indonesia
t +62 21 574 7181
f +62 21 574 7180
w makeslaw.com

MALAYSIA

-
Foong & Partners
Advocates & Solicitors
13-1, Menara 1MK, Kompleks 1 Mont' Kiara
No 1 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia
t +60 3 6419 0822
f +60 3 6419 0823
w foongpartners.com

MIDDLE EAST

-
Al Aidarous International Legal Practice
Abdullah Al Mulla Building, Mezzanine Suite 02
39 Hameem Street (side street of Al Murroor Street)
Al Nahyan Camp Area
P.O. Box No. 71284
Abu Dhabi, UAE
t +971 2 6439 222
f +971 2 6349 229
w aidarous.com

-
Al Aidarous International Legal Practice
Zalfa Building, Suite 101 - 102
Sh. Rashid Road
Garhoud
P.O. Box No. 33299
Dubai, UAE
t +971 4 2828 000
f +971 4 2828 011

PHILIPPINES

-
ZGLaw
27/F 88 Corporate Center
141 Sedeño Street, Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w zglaw.com/~zglaw

wongpartnership.com