DATA PROTECTION LAWS OF THE WORLD

Singapore

SINGAPORE

Last modified 21 December 2021

LAW

Singapore enacted the Personal Data Protection Act of 2012 (No. 26 of 2012) (**"Act"**) on October 15, 2012. A draft Personal Data Protection (Amendment) Bill (**"Amendment Bill"**) was passed in the Singapore Parliament in November 2020.

Certain sections of the Amendment Bill are now in force under the Personal Data Protection (Amendment) Act 2020 (as of February 1, 2021). These include mandatory data breach notification, an expanded deemed consent framework, new exceptions to the express consent requirement and new offences for the egregious mishandling of personal data or the unauthorized re-identification of anonymized information. The sections on increased financial penalty and the right of data portability are expected to come into force no earlier than February 1, 2022.

In addition, the Personal Data Protection (Notification of Data Breaches) Regulations 2021 and the Personal Data Protection Regulations 2021 came in effect from October 1, 2021. The updates to these include, among other things, clarifications to the scope of significant harm for mandatory data breach reporting and additional defences to the offence of egregious mishandling of personal data.

The Act has extraterritorial effect, meaning it applies to organizations collecting, using or disclosing personal data in Singapore whether or not the organization itself has a physical presence or is registered as a company in Singapore.

In addition to the Act, the Singapore data protection regime consists of various general or sector / industry-specific guidelines issued by the Personal Data Protection Commission (**"Commission"**). While these guidelines are advisory in nature and not legally binding, they indicate the manner in which the Commission will interpret the Act. Therefore, it is best practice to carefully observe and follow these guidelines.

The data protection obligations under the Act do not apply to the public sector, to whom separate rules under the Government Instruction Manual 8 (**"IM8"**) and the Public Sector (Governance) Act apply. Collectively, these rules provide comparable standards of data protection compared to the Act, including similar investigations and enforcement actions taken against data security breaches. The Public Sector Data Security Review Committee was convened on March 31, 2019 to conduct a comprehensive review of data security policies and practices across the public sector. The Government implemented its recommendations and adopted changes to its data security measures. Examples include:

- Requiring officers to password-protect files containing sensitive data when sending out; and
- Enhancing the data incident management framework with standardized process to notify affected individuals in data incidents and conduct post-incident inquiry.

DEFINITIONS

Definition of personal data

Personal data is defined in the Act to mean data, whether true or not, about an individual (whether living or recently deceased*)

who can be identified from:

- that data; or
- that data and other information to which the organization has, or is likely to have access.

*The Act's application to recently deceased individuals is limited to disclosure and protection of personal data where such data is about an individual who has been deceased for ten years or fewer.

The data protection obligations under the Act do not apply to business contact information. This excludes from the Act the following if provided solely for business purposes:

- Name
- Position name or title
- Business telephone number
- Business address
- Business electronic mail address
- Business fax number

It is important to note that the Act still governs business contact information provided by individuals solely in their personal capacity. Where the purposes of provision of business contact information are mixed (that is, for both business and personal purposes), the Act does not apply.

Definition of sensitive personal data

There is no definition of sensitive personal data in the Act.

However, non-binding guidance from the Commission indicates that sensitivity of data is a factor for consideration in implementing policies and procedures to ensure appropriate levels of security for personal data. For example, encryption is recommended for sensitive data stored in an electronic medium that has a higher risk of adversely affecting the individual should it be compromised. Where any personal data collected is particularly sensitive (*e.g.* regarding physical or mental health), as a matter of best practice, such data should only be used for limited purposes and the security measures afforded to such data should take into account the sensitivity of the data.

In addition, the non-binding guidelines issued by the Commission also provide that, in its calculation of financial penalties for breaches of the Act, the Commission would consider whether the organization in question is in the business of handling large volumes of sensitive personal data, the disclosure of which may cause exceptional damage, injury or hardship to an individual (such as medical or financial data), but it has failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of such personal data.

The Commission has also issued a set of advisory guidelines to impose restrictions on the collection, use and disclosure of National Identification Registration Card ("**NRIC**") numbers, due to the sensitive nature of the information contained in NRICs (and other similar forms of identification). From September 1, 2019, organizations will not be permitted to collect either the NRIC number or the physical cards or other similar forms of identification unless the organization is permitted to do so under the law or if the collection is necessary for the verification of an individual's identity to "high degree of fidelity" (where it is extremely important the individual's identity is verified, and failure to do so may, for example, pose a significant safety or security risk).

NATIONAL DATA PROTECTION AUTHORITY

Personal Data Protection Commission

Address

10 Pasir Panjang Road #03-01

Mapletree Business City
Singapore 117438

Telephone

+65 6377 3131

Fax

+65 6577 3888

Email

info@pdpc.gov.sg

Website

www.pdpc.gov.sg

REGISTRATION

There are no registration requirements under the Act.

While not a requirement, the Commission strongly encourages organizations to register their Data Protection Officers ("**DPOs**") with the Commission via the Commission's website, to assist DPOs in keeping up to date with developments in the law.

DATA PROTECTION OFFICERS

It is mandatory for each organization to appoint one or more DPOs to be responsible for ensuring the organization's compliance with the Act. An organization may appoint one person or a team of persons to be its DPO. Once appointed, the DPO may in turn delegate certain responsibilities, including to non-employees of the organization. The business contact information of the DPO must be made available to the public. The DPO's contact information may be made available to the public either through BizFile+ website (where the organisation is registered with the Accounting and Corporate Regulatory Authority) or provided in a readily accessible part of the organization's official website.

While there is no requirement for the DPO to be a citizen or resident in Singapore, the Commission suggests that the DPO should be readily contactable from Singapore, available during Singapore business hours and, where telephone numbers are provided, these should be Singapore telephone numbers.

Failure to appoint a DPO may lead to a preliminary investigation by the Commission. If an organization or an individual fails to cooperate with the investigation, this will constitute an offence. As a result, an individual may be subject to a fine of up to SGD 10,000 or imprisonment for a term not exceeding 12 months, or to both. An organization may be subject to a fine of up to SGD 100,000.

COLLECTION & PROCESSING

Organizations may only collect, use or disclose personal data in the following scenarios:

- They obtain express consent from the individual prior to the collection, use, or disclosure of the personal data (and such consent must not be a condition of providing a product or service, beyond what is reasonable to provide such product or service; and must not be obtained through the provision of false or misleading information or through deceptive or misleading practices), and have also provided the relevant data protection notice (notifying purposes of collection, use and disclosure) to the individual before, or at the time when they are collecting, using or disclosing the personal data
- There is deemed consent by the individual to the collection, use, or disclosure of the personal data in accordance with the relevant conditions of the Act.
- Where the limited specific exclusions prescribed in the Act apply (if no consent or deemed consent is given). Such

exclusions include vital interests of individuals, matters affecting public, legitimate interests, business asset transactions, business improvement purposes and other additional bases.

Such exclusions include vital interests of individuals, matters affecting public, legitimate interests, business asset transactions, business improvement purposes and other additional bases.

The Act currently in force expanded the concept of "deemed consent" to cover circumstances where: (i) the collection, use or disclosure of personal data is reasonably necessary to conclude or perform a contract or transaction; or (ii) (a) where individuals have been notified of the purpose of the intended collection, use or disclosure of personal data, given a reasonable opportunity to opt-out, and have not opted out, and (b) the organization has conducted an assessment on the likely adverse effect on such individuals, and identified and put in place reasonable measures to eliminate, reduce the likelihood of or mitigate any such adverse effect.

An individual may at any time withdraw any consent given, or deemed given under the Act, upon giving reasonable notice to the organization.

Further, any collection, use or disclosure of the personal data must only be for the purposes that a reasonable person would

consider appropriate in the circumstances, and for purposes to which the individual has been notified of. Such notification must be made in accordance with the requirements of the Act.

An organization must also do all of the following:

- Make information about its data protection policies, practices and complaints process publicly available.
- Cease to retain personal data or anonymize it where it is no longer necessary for any business or legal purpose.
- Ensure personal data collected is accurate and complete if likely to be used to make a decision about the individual or disclosed.
- Respond to requests by data subjects under their statutory rights, including a new right of data portability (this right is expected to come into force no earlier than February 1, 2022).

Data intermediaries that process personal data on behalf of another organization (i.e. data controller) pursuant to a written contract are exempt from most of the data protection obligations under the PDPA. However, data intermediaries are directly liable under two specific obligations relating to the retention (see above) and protection (see Security) of personal data.

Data protection management program ("**DPMP**") and data protection impact assessment ("**DPIA**") guides were published by the Commission in November 2017 and updated in September 2021.

TRANSFER

In disclosing or transferring personal data to onshore third parties (including affiliates), an organization should ensure that it has obtained the individual's deemed or express consent to such transfer (unless exemptions apply) and, if this was not done at the time the data was collected, additional consent will be required (unless exemptions apply).

It is also a requirement under the Act for organizations to enter into written agreements with their data intermediaries to whom they transfer personal data and who process such data on behalf of the organizations.

The Act also contains offshore transfer restrictions, which require an organization to ensure that the receiving organization has in place "comparable protection" to the standards set out in the Act when transferring personal data outside of Singapore. Mechanisms to achieve this include (this is not a comprehensive list): data transfer agreements (for which the Commission has released including model clauses); the individual has given consent (and provided required notices have been provided); and where transfers are considered necessary in certain prescribed circumstances (which include in connection with performance of contracts between the transferring organization and the individual, subject to certain conditions being met). An organization may apply to be exempted from any requirement prescribed under the Act in respect of any transfer of personal data out of Singapore. An exemption may be granted on such conditions as the Commission may require.

The Amendment Act provides for a new right of data portability on electronic data (this right is expected to come into force no

earlier than February 1, 2022). Individuals may request an organization (**"Porting Organization"**) to transmit certain data about them to another organization. The Porting Organization must have an ongoing relationship with the individual, and have collected or created such data.

The Commission has published guides to data sharing (covering intragroup and third party sharing) with practical nonbinding guidance on data transfer / sharing for organizations, as well as DPMP and DPIA guides (see Collection & Processing).

SECURITY

Organizations must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, the loss of any storage medium or device on which personal data is stored, or similar risks. Data intermediaries are also directly liable and subject to the same security obligation. The Act does not specify security measures to adopt and implement, however the Commission has issued best practice guidance which provides specific examples, including with respect to cloud computing and IT outsourcing.

BREACH NOTIFICATION

Under the current Act, where an organization has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, it must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a "notifiable breach" (as defined in the current Act). A data breach constitutes a "notifiable breach" if:

- it results in, or is likely to result in, significant harm to the affected individuals (including one that compromises personal data prescribed under the Personal Data Protection (Notification of Data Breaches) Regulations 2021); or
- it is of a significant scale (i.e. one that affects 500 or more individuals).

An organization must notify the Commission as soon as practicable and in any case no later than three calendar days after the day the organization makes the above assessment of a notifiable breach. If the data breach results in, or is likely to result in, significant harm to the affected individual(s), an organization must also notify each affected individual in any manner that is reasonable in the circumstances.

The Personal Data Protection (Notification of Data Breaches) Regulations 2021 sets out the list of information to be included in notifications to the Commission and affected individuals.

Where a data breach is discovered by a data intermediary, the data intermediary must notify the organization (i.e. data controller) without undue delay from the time the data intermediary has credible grounds to believe that a data breach has occurred in relation to personal data that it is processing on behalf of and for the purposes of the organization. Upon notification by the data intermediary, the organization must conduct an assessment of whether the data breach is a notifiable data breach.

In addition, the Cybersecurity Act 2018 ("**CSA**") was passed in Singapore in early 2019. The CSA primarily contains obligations applicable to organizations which have been designated as owners of critical information infrastructure. In particular, if your organization has been designated by the Cybersecurity Commissioner as the owner of a critical information infrastructure, additional obligations will apply to your organization in relation to data breach incident handling and notification.

ENFORCEMENT

Enforcement of the Act is carried out by the Commission, which include giving directions to do any of the following:

- Stop collection, use or disclosure of personal data in contravention of the Act
- Destroy personal data collected in contravention of the Act
- Provide or refuse access to or correction of personal data
- Pay a financial penalty, currently the maximum financial penalty is not exceeding SGD 1 million. However, once the section on increased financial penalty of the Amendment Bill comes into force (no earlier than February 1, 2022), the penalty will be increased to either up to (i) 10% of an organization's annual turnover in Singapore for those with annual turnover that exceeds SGD 10 million, or (ii) SGD 1 million, whichever is higher.

These directions may be registered with the Singapore District Courts so that they may have the force and effect of an order of court.

The Commission issued revised Advisory Guidelines on Enforcement of Data Protection Provisions on February 1, 2021.

Further, new criminal offences are in force to hold individuals accountable for egregious mishandling of personal data, including knowing or reckless unauthorized disclosure, unauthorized re-identification of anonymized data, or use of personal data for a gain or to cause harm or loss to another person.

Guidelines published by the Commission indicate how in practice the Commission proposes to handle complaints, reviews and investigations of breaches of the data protection rules under the Act, and to approach enforcement and sanctions. Amongst other things, they set out the Commission's enforcement objectives, and guidance regarding the mitigating and aggravating factors that the Commission will take into account when issuing directions and sanctions (for example, prompt initial response and resolution of incidents; cooperation with investigations; and breach notification). The Commission has in the past couple of years stepped up its efforts to enforce the Act, highlighting the growing risks of non-compliance with the Act in Singapore.

Directions or decisions given are subject to reconsideration by the Commission, upon written application by any aggrieved party.

Directions, decisions or reconsiderations of the Commission may also be subject to appeal to a Data Protection Appeal Committee, unless the direction or decision to be appealed is the subject of an application for reconsideration, in which case such appeal would be deemed withdrawn.

Directions may only be appealed to the High Court and Court of Appeal with regard to the following:

- A point of law arising from a direction or decision of the Appeal Committee
- Any direction of the Appeal Committee as to the amount of a financial penalty

Any person who has suffered loss or damage directly as a result of a contravention of the Act is also entitled to pursue a private action in court. However, where the Commission has made a decision with regard to the said loss or damage, a right of private action will only be possible after the decision has become final as a result of there being no further right of appeal. The court may grant to the plaintiff all or any of the following:

- Relief by way of injunction or declaration
- Damages
- Such other relief as the court thinks fit

ELECTRONIC MARKETING

The data protection principles in the Act apply to any marketing activities (including electronic marketing) which involve the collection, use or disclosure of personal data.

In addition, any organization or person that wishes to engage in any telemarketing activities will need to comply with the "Do Not Call" provisions under the Act. Generally, a person or organization who wishes to send marketing messages to a Singapore telephone number should first obtain the clear and unambiguous consent of the individual to the sending of the messages to such Singapore telephone number. The consent must:

- be evidenced in written or other form so as to be accessible for subsequent reference;
- not be a condition for supplying goods, services, land, interest or opportunity; and
- not be obtained through the provision of false or misleading information or through deceptive or misleading practices.

In the absence of such consent, organizations must check and ensure that the telephone number is not on a Do-Not-Call register maintained by the Commission (**"DNC Register"**), unless such checks are exempted under the Act. There are also other requirements, including a duty to identify the sender of the marketing message and provide clear and accurate contact information, as well as a duty not to conceal the calling line identity of any voice calls containing such marketing messages. An individual may at any time apply to the Commission to add or remove his Singapore telephone number on the DNC Register.

Further, the current Act provides the role of "checkers" which are entities that provide information for gain on whether a Singapore telephone number is listed in the DNC Register for the purposes of another organization's obligations under the Act. It imposes obligations on third party checkers, and checkers will be liable for DNC infringements resulting from any erroneous information provided by them.

The Act will apply to marketing messages addressed to a Singapore telephone number in the following circumstances:

- The sender of the marketing message is present in Singapore when the message was sent.
- The recipient of the marketing message is present in Singapore when the message is accessed.

Electronic marketing activities are also regulated under the Spam Control Act (Cap 311A) (**"SCA"**), to the extent that such activities involve the sending of unsolicited commercial communications in bulk by electronic mail or by SMS or MMS to a mobile telephone number.

The DNC provisions under the current Act include a prohibition on sending messages to telephone numbers generated or obtained through dictionary attacks (generating telephone numbers by combining numbers into numerous permutations) or address-harvesting software. Related amendments to the SCA to prohibit sending unsolicited electronic messages to instant messaging accounts are also in force.

The Commission issued the revised Advisory Guidelines on the Do Not Call Provisions on February 1, 2021.

ONLINE PRIVACY

Currently, there are no specific requirements relating to online privacy (including cookies and location) under the Act. Nevertheless, an organization that wishes to engage in any online activity that involves the collection, use or disclosure of personal data will still need to comply with the general data protection obligations under the Act. For example, if an organization intends to use cookies to collect personal data, it must obtain consent before use of any such cookies. For details of the consent required, please see Collection & Processing. The Commission has published nonbinding guidelines providing practical tips on pertinent topics such as securing electronic personal data, building websites, the capture of IP addresses and the use of cookies.

KEY CONTACTS

Carolyn Bigg
Partner, Global Co-Chair of Data Protection, Privacy and Security Group
T +852 2103 0576
carolyn.bigg@dlapiper.com

Yue Lin Lee
Senior Associate
T +852 2103 0890
yuelin.lee@dlapiper.com

Jing Qin Cho
Registered Foreign Lawyer (Singapore)
T +852 2103 0410
jingqin.cho@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.