SINGAPORE

LAW

Singapore enacted the Personal Data Protection Act of 2012 (No. 26 of 2012) (the Act) on October 15, 2012. The Act took effect in three phases:

1. Provisions relating to the formation of the Personal Data Protection Commission (the Commission) took effect on January 2, 2013.
3. The main data protection provisions took effect on July 2, 2014.

The Act has extraterritorial effect, meaning it applies to organizations collecting personal data from individuals in Singapore whether or not the organization itself has a physical presence in Singapore.

The data protection obligations under the Act do not apply to the public sector, to whom separate rules apply.

The Commission’s first public consultation reviewing the Act (PDPA Consultation) closed in October 2017, and focused on “approaches to managing personal data in the digital economy,” with topics including “challenges for alternatives to consent” and mandatory breach notification. It is anticipated that the Act will be amended sometime in 2019 to incorporate the changes proposed in the PDPA Consultation.

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
- From 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
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 (eg, 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.

The Commission has also stated in its enforcement decisions that the fact that personal data is of a sensitive financial nature is a relevant factor in its decisions, and a public condition in 2017 proposed draft additional safeguards for collection, use and disclosure of National Identification Registration Card (NRIC) numbers.

**NATIONAL DATA PROTECTION AUTHORITY**

Personal Data Protection Commission

460 Alexandra Road
#10-02 PSA Building
Singapore 119963

T +65 6377 3131
F +65 6273 7370

info@pdpc.gov.sg
http://www.pdpc.gov.sg/

**REGISTRATION**

There are no registration requirements under the Act.

While not a requirement, in April 2017 the Commission publicly encouraged 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**

Each organization must appoint one or more data protection officers 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.

While there is no requirement for the data protection officer to be a citizen or resident in Singapore, the Commission suggests that the data protection officer 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 data protection officer 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 offense. As a result, an individual may be subject to a fine of up to S$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 S$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).

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.

New data protection management program (DPMP) and data protection impact assessment (DPIA) guides were published by the Commission in November 2017.

In addition, due to the sensitive nature of the information contained in the National Identification Registration Card (NRIC) (and other similar forms of identification) and the physical card, new guidelines were published in August 2018 to provide organizations with guidance on the collection of the information contained in the NRIC as well as the collection of the physical card. From September 1, 2019, organizations will not be permitted to collect the NRIC or other national identification numbers or the physical cards, unless required by law, or if the collection is necessary for the verification of an individual’s identity to high fidelity.

**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).

The Act also contains offshore transfer restrictions, which require an organization to ensure “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 recently released guidance, 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 Commission has published a new guide to data sharing (covering intragroup and third party sharing) with practical nonbinding guidance 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 or similar risks. 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

Currently, there are no mandatory requirements under the Act for data users to notify the Commission or individuals regarding data protection breaches in Singapore. The Commission issued a best practice guide in May 2015 to help organizations manage personal data breaches effectively, and more recent guidelines provide practical tips on avoiding and managing risks such as accidental data disclosure. It is recommended that affected individuals be notified immediately if a data breach involves sensitive personal data. The Commission should be notified as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals. Aggrieved parties may either make a complaint to the Commission, or may take out a private action in civil proceedings. The Commission may also conduct investigations on its own motion.

However, there are now proposals to introduce mandatory data breach notifications in Singapore. It is anticipated that the Act will be amended sometime in 2019 to incorporate the amendments proposed in the PDPA Consultation. Organizations are advised to monitor developments.

In addition, the Cybersecurity Act 2018 (CSA) was recently passed in Parliament, and sections of the CSA have now come into force. As at the date of this update, the obligations under the CSA primarily fall on organizations which have been designated as owners of critical information infrastructure. 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. The powers of the Commission 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 not exceeding S$1 million

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 published the Advisory Guidelines on Enforcement of Data Protection Provisions in April 2016. These guidelines 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 lie 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; must not be a condition for supplying goods, services, land, interest or opportunity; and must 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 message. An individual may at any time apply to the Commission to add or remove his Singapore telephone number on the DNC Register.

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 Commission had a public consultation in April 2018 seeking views on the streamlining of the requirements under the "Do Not Call" provisions of the Act with the provisions under the SCA. The public consultation closed in June 2018, and organizations are advised to monitor developments in this area.

**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 the Collection & Processing chapter. The Commission has published nonbinding guidelines providing practical tips on pertinent topics such as securing electronic personal data and building websites, and a public consultation as “approaches to managing personal data in the digital economy” was undertaken by the Commission in Summer 2017.
KEY CONTACTS

Scott Thiel  
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group  
T +852 2103 0519  
scott.thiel@dlapiper.com

Carolyn Bigg  
Of Counsel  
T +852 2103 0576  
carolyn.bigg@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.
Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.