MARGARETLAW®
CORPORATION

The Personal Data Protection Act

An Overview

Until recently, the use of personal data has been regulated by a combination of sector-specific legislation and the common law. The Personal Data Protection Act ("PDPA"), which was passed by the Singapore Parliament on 15 October 2012, now complements these existing laws and regulations by establishing a basic standard for the protection of personal data within the private sector.

In seeking to balance the legitimate need of organisations to collect and use personal data against the rights of individuals to protect their personal data, the PDPA institutes a framework of rights, rules and practices designed to safeguard personal data.

In brief, the PDPA:

(a) sets out the rules and practices that must be followed by private sector organisations with respect to the collection, use and disclosure of individuals' personal data;

(b) grants rights to individuals in respect of their personal data, including rights to access and correct that data;

(c) establishes the Personal Data Protection Commission (the "Commission") to administer and enforce these rights rules and practices; and

(d) creates a Do-Not-Call ("DNC") Registry to address unsolicited telemarketing calls and messages.

Implementation of PDPA

The PDPA is being implemented in three phases, as follows:

(a) Provisions relating to the formation of the Personal Data Protection Commission (PDPC) came into effect on 2 January 2013;

(b) Provisions relating to the DNC Registry came into effect on 2 January 2014; and

(c) The main data protection rules will come into force on 2 July 2014.

The phased implementation is intended to allow organisations to assess internal personal data protection policies and practices and adopt new measures to achieve and maintain compliance with the PDPA.

Scope and Application of PDPA

(i) What is "Personal Data"?

The PDPA covers personal data stored in electronic and non-electronic forms.

Personal data broadly refers to data, regardless of its veracity, about an individual who is:

(a) identifiable from that data; or

(b) identifiable from that data and other information to which the organisation has in its possession or is likely to be able to access.

Examples of personal data include an individual's full name, NRIC number, passport number, photograph, video image, personal telephone numbers, personal e-mail addresses, fingerprints and DNA profile.

In general, the specific context will be important in determining whether or not certain types of information may be considered personal data. For example, the Commission is of the view that IP addresses in isolation would not constitute personal data as they serve to identify particular networked devices. However, in certain circumstances where IP addresses are combined with other information, such as information that is collected by an organisation's use of cookies, it may become possible to identify individuals from their networked devices thereby bringing those IP addresses within the scope of the definition of personal data.

The PDPA also excludes specific categories of personal data, as follows:

(a) business contact information, which refers to an individual's name, position or title, and business contact details (e.g. telephone numbers, fax numbers, e-mail address and postal addresses used by the business);

(b) personal data contained in records that have been in existence for at least 100 years; and

(c) personal data pertaining to individuals who have been deceased for over 10 years.

(ii) Who are "Individuals"

The PDPA sets out the framework for protecting the personal data of individuals.

The PDPA defines an individual as a "natural person, whether living or deceased" although the extent to which the PDPA applies to deceased individuals has been limited.

The PDPA therefore does not regulate the personal data belonging to certain types of "legal persons" such as business entities or public organisations.

(iii) Who are "Organisations"

The PDPA sets out the framework for regulating how organisations collect, use and disclose personal data and applies to all organisations, with certain exceptions.

The PDPA defines an organisation as any individual, company, association or body of persons, incorporated or unincorporated, whether or not the organisation is formed under the laws of Singapore or is resident in Singapore.

The PDPA does not apply to:

(a) individuals acting in a personal or domestic capacity;

(b) employees acting in the course of their employment with an organization;

(c) public agencies or organisations acting on behalf of public agencies in relation to the collection, use or disclosure of the personal data. (The public sector will continue to be governed by sector-specific legislation).

Key Personal Data Protection Principles

The provisions of the PDPA for regulating the collection, use and disclosure of personal data are based on the following key principles:

(a) *Consent*: Organisations may collect, use or disclose personal data only with an individual's knowledge and consent;

(b) *Purpose*: Organisations can collect, use or disclose personal data in a manner appropriate for the circumstances, and only if they have informed the individual of its objectives or reasons for the collection, use or disclosure of the personal data; and

(c) *Reasonableness*: Organisations can collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.

The provisions of the PDPA granting rights to individuals with respect to their personal data are based on the following principles:

(a) *Access*: Individuals have the right to request that an organisation allows access to their personal data which is in that organisation's control and to be provided with information regarding the use and disclosure of that personal data over the one year period preceding the request; and

(b) *Correction*: Individuals have the right to request that an organisation corrects an error or omission with respect to their personal data which is in the control of that organisation.

The provisions of the PDPA with respect to the care of personal data in an organisation's possession are based on the following principles:

(a) *Accuracy*: Organisations must make reasonable efforts to ensure that personal data in its possession is accurate and complete if it is likely that the personal data will be disclosed to another organisation or if it is likely that the use of the personal data will affect the individual to whom it belongs;

(b) *Protection*: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful access, collection, use, disclosure, copying, modification or deletion of personal data and other similar risks;

(c) *Limited Retention*: Personal data shall not be kept by an organisation for longer than necessary to fulfil the purpose for which it was collected; and

(d) *Limited Transfer*: Personal data shall not be transferred to a country or territory outside Singapore

unless that jurisdiction ensures an adequate standard of protection of the personal data comparable to the protection offered under the PDPA.

The PDPA contains a number of exemptions from the above specified data protection principles. For example there are provisions which allow for personal data to be used in relation to investigations or for evaluative purposes. Exemptions also exist for publicly available personal data. More information can be obtained from the Second, Third and Fourth Schedules of the PDPA.

Enforcement of PDPA

The Commission is empowered to investigate non-compliance with the PDPA. Where the Commission is satisfied that an organisation is in non-compliance with the data protection framework under the PDPA, the Commission is empowered to issue remedial directions, including directions requiring an organisation to:

(a) stop collecting, using or disclosing personal data in violation of the PDPA;

(b) destroy personal data collected in violation of the PDPA;

(c) provide access to or correct personal data; and/or

(d) pay a financial penalty of up to SGD 1,000,000.

Ensuring Compliance with the PDPA

Under the PDPA, it is a requirement for organisations to designate one or more individuals to act as data protection officers who are responsible for ensuring that the organisation complies with the PDPA. Organisations are required to provide the contact details of at least one data protection officer to the public.

Organisations should also:

(a) develop and implement policies and practices necessary for the organisation to meet its obligations under the PDPA;

(b) ensure that staff is trained on the organisation's policies and practices with respect to the PDPA;

(c) develop procedures to receive and respond to complaints arising with respect to the application of the PDPA;

(d) develop procedures to respond to requests from individuals to access or correct their personal data;

(e) make reasonable efforts to ensure that personal data is accurate and complete and only retained as long as necessary;

(f) take measures must to keep personal data secure at all times;

(g) put in place suitable contracts with intermediaries who process personal data on behalf of the organisation; and

(h) review all transfers of personal data across borders.

Do-Not-Call Registry

The DNC Registry has been established under the PDPA and allows individuals to register to opt-out of receiving marketing messages in the form of voice calls, text messages or facsimiles. Marketing messages sent by e-mail or post will continue to be regulated by the Spam Control Act.

To be considered a marketing message, one of the purposes of the message must be to:

(a) offer to supply, advertise or promote goods or services, or to promote the suppliers or prospective suppliers of goods and services;

(b) offer to supply, advertise or promote land or an interest in land, or to promote a supplier or prospective supplier thereof; or

(c) offer to provide, advertise or promote a business or investment opportunity, or to promote a provider or prospective provider thereof.

Organisations sending a marketing message to a Singapore telephone number will be required to ensure that they have checked (within the prescribed duration) that the recipient's number is not registered in the DNC register. The organisation must also ensure that the message includes clear and accurate information identifying the sender along with the sender's contact details. For voice calls, the caller's line identity cannot be concealed.

In a recent development, the Commission granted an exemption to organisations from the obligation to check the DNC register before sending specified text or fax messages to individuals with whom they have an ongoing business relationship.

February 2014

Lawyer	E-mail Address	Direct Dial
Mr Syn Yi Ming Director	yiming@margaretlaw.com.sg	65-6636 7718
Ms Margaret Law Director	margaret@margaretlaw.com.sg	65-6835 7250