February 2013

AMICA LAW UPDATE

30 Raffles Place #18-03/04 Chevron House Singapore 048622
www.amicalaw.com

LEGISLATION UPDATE – NEW PERSONAL DATA PROTECTION ACT 2012

The new Personal Data Protection Act 2012 (No. 26 of 2012) ("**Act**") was passed by the Singapore Parliament on 15 October 2012. The Act will take effect in 3 phases:

1. provisions relating to the formation, administration and powers of the Personal Data Protection Commission (the "**Commission**") and Data Protection Advisory Committee (the "**Advisory Committee**") came into force on 2 January 2013;
2. provisions relating to the National Do-Not-Call Registry ("**DNC Registry**") will come into force in early 2014; and
3. the main data protection provisions will come into force in mid-2014.

The phased implementation of the Act serves as a transition period for organisations to review and adopt internal personal data protection policies and practices, so that they may comply with the Act. The exact dates on which the DNC Registry provisions and other data protection provisions will come into force will be announced at a later date.

Some of the key aspects of the Act are summarily set out below:

Definition of "Personal Data"

"*Personal data*" is defined broadly to mean "*data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access*". This definition covers both electronic and non-electronic forms of data.

Scope of Application

The Act will apply to the collection, use and disclosure of personal data by all organisations with certain exceptions. An "organisation" is defined broadly, and includes "*any individual, company, association or body of persons, corporate or unincorporated, whether or not: (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore*". Public agencies, individuals acting in a personal or domestic capacity or as an employee acting in the course of his employment with an organisation, and other prescribed organisations or prescribed personal data are exempted from the data protection requirements under the Act. Data intermediaries are also exempted from certain data protection obligations under the Act.

Certain types of information are also exempted from the data protection requirements of the Act. For example, unless otherwise stated in the Act, the data protection requirements of the Act do not apply to "business contact information", which is defined as "*an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes*".

The Act is intended to apply concurrently with the existing laws and regulations in Singapore which govern data protection. In the event of any conflict or inconsistency, the provisions of other written laws will prevail unless otherwise stated in the Act.

General compliance obligations |

- *Appointment of a Personal Data officer* – An organisation is required to appoint one or more individuals to be responsible for ensuring the organisation's compliance with the Act. The contact details of at least one of these individuals must be published.
- *Policies & Practices* – An organisation is also required to develop and implement adequate data protection policies, practices and processes that will enable the organisation to meet its obligations under the Act.

Consent

Before collection, use or disclosure of personal data of an individual, *c*onsent must be validly obtained from the individual, unless such consent is deemed given or is not required under the Act. In seeking consent, an organisation must comply with the notification requirements under the Act. The Act also specifies circumstances in which consent obtained may be regarded as invalid. For example, consent may be considered invalid if false or misleading practices or information was used to obtain the consent for collecting, using or disclosing personal data. There is also a reasonableness test for consent obtained as a condition for providing a product or service. The Act also provides that an individual may at any time withdraw his/her consent.

Purpose must be reasonable

The Act states that organisations may collect, use or disclose personal data only for purposes that a reasonable person would consider appropriate in the circumstances.

Access and correction requirements

There are also access and correction requirements under the Act. An organisation is required to provide an individual with access to their personal data and with information about how his/her personal data has been or may have used or disclosed by the organisation within a year before the date of request. An individual also has the right to request correction of errors or omissions in his/her personal data. An individual's right to access and correct his or her personal data is subject to certain exceptions.

Care & Security of Personal Data

In certain circumstances, organisations will have

to make reasonable efforts to ensure that the personal data it collects is accurate and complete. Organisations are also obliged to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The Act does not specify specific security measures to adopt and implement.

Retention of Personal Data

There is no mandatory retention period under the Act. An organisation is only obliged to cease retention (or remove the means by which the personal data can be associated with particular individuals) as soon as the purpose for which personal data was collected is no longer being served by such retention, or such retention is no longer necessary for legal or business purposes. Any mandatory data retention period prescribed in any other legislation will still apply.

Transfer of personal data outside Singapore

Transfer of personal data out of Singapore is allowed, provided that the organisation ensures that a comparable standard of protection as the standard set out in the Act is accorded to personal data that is to be transferred overseas.

An organisation may also 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 Minister for Communications and Information may require.

Enforcement

Enforcement of the Act is carried out by the Commission. The Commission is given broad powers to issue guidelines, give directions to remedy non-compliance, review complaints, initiate investigations and impose financial penalties of up to S$1 million.

There are also reconsideration and appeal processes and procedures in place which aggrieved parties may rely upon. Aggrieved parties may also take out a private action in civil proceedings.

DNC Registry

The Act also introduces the setting up of a DNC Registry. Organisations will be prohibited from sending unsolicited "specified messages" to Singapore telephone numbers registered on a Do-Not-Call (DNC) register to be maintained by the Commission. A "specified message" refers to a message for which one of the purposes relates to marketing.

"Message" means any message, whether in sound, text, visual or other form. This includes any voice calls, faxes, short messaging service (SMS) or multimedia messaging service (MMS) messages. The Act will apply to specified messages addressed to a Singapore telephone number where:

1. the sender of the specified message is present in Singapore when the specified message was sent; or
2. the recipient of the specified message is present in Singapore when the message is accessed.

Therefore, prior to conducting any electronic marketing activities by sending a specified message to a Singapore telephone number, organisations will have a duty to check the DNC register and must obtain confirmation from the Commission that its intended recipient is not listed on the DNC register. There are also other obligations imposed on an organisation that sends a specified message. Failure to comply with any of the above obligations constitutes an offence and may attract a fine of up to S$10,000.

Implications of Act

The new Act will affect all organisations which collect and process personal data. It is advisable that organisations, especially those which handle a large amount of personal data on a day to day basis, start planning and preparing themselves for compliance with the Act. Some steps that may need to be taken by an organisation include:

1. conducting an internal data compliance audit to ascertain and the types of personal data that are currently collected and processed by the organisation, and the manner in which such data is currently collected, used, handled, stored and retained by the organisation;
2. appointing one or more personal data manager(s);
3. formulating, publishing and implementing proper corporate policies and procedures to ensure compliance with the Act; and
4. communicating and educating staff of the new corporate policies and procedures implemented to ensure compliance with the Act.

The above represents a summary of some of the significant features of the Act, and is not a complete listing of its provisions, nor are the comments on each provision exhaustive.

For questions, please contact:

Wilson Wong
Director
Head of Technology & Licensing Practice
DID: +65 6303 6213
Email: wilson.wong@amicalaw.com

Geraldine Tan
Associate Director
DID: +65 6303 6221
Email: geraldine.tan@amicalaw.com