THE PERSONAL DATA PROTECTION ACT: AN OVERVIEW

After a year-long series of public and industry consultations, the Personal Data Protection Act 2012 ("PDPA") came into force on 2 January 2013. This long-awaited piece of legislation follows in the footsteps of equivalent data protection legislation already enacted in some parts of Asia in recent years. The PDPA establishes a regime in Singapore for the protection of personal data, and sets out what the Ministry of Communications and Information calls a “baseline” law that applies to all organisations, save for organisations in the public sector. Essentially, the law aims to safeguard consumers' personal data against misuse.

The PDPA will be enforced in phases. Currently, certain provisions relating to the establishment and powers of the Commission are already in force. The provisions relating to the new Do Not Call Registry (the “DNC Registry”) will come into effect from 2 January 2014, and the PDPA will come into full force on 2 July 2014. When the provisions of the PDPA are fully in force, complaints may be filed with the Personal Data Protection Commission (the “Commission”), in the event that there have been violations of the PDPA.

Definition of “Personal Data” under the PDPA

The “personal data” that will be protected under the PDPA is presently broadly defined in Section 2 of the act as data concerning an individual “who can be defined from that data, or from that data and other information to which the organisation is likely to have access. The PDPA will apply equally to data which is true or false.

Organisations Subject to the PDPA

The PDPA applies to all private sector organisations that are engaged in data collection, processing or disclosure within Singapore, even if the organization is physically located overseas. Therefore, the PDPA would likely apply to a company that was not incorporated in Singapore, but which collects data online from a person in Singapore.

The PDPA, however, excludes “data intermediaries” that process data on behalf of other organizations from having to comply with the provisions pertaining to:

- the general rules with respect to the protection of personal data;
- the collection, use and disclosure of personal data;
- the access to and correction of personal data; and
- the accuracy and retention of personal data.

Key Obligations under the PDPA

The cornerstone of the PDPA is the prohibition of the collection, use or disclosure by organisations of personal data without the consent of the relevant individuals, and generally requiring organisations to obtain the explicit consent of individuals. However, an individual would be deemed to have given his consent for the collection, use or disclosure of his personal data if that individual voluntarily provides his personal data to an organisation, and if it is reasonable that the individual would volunteer the data under the circumstances.
In any event, the PDPA will require organisations to inform individuals of the purpose behind the collection, use or disclosure of the personal data. This consent may be withdrawn at any time upon an individual giving “reasonable notice” to the relevant organisation.

It should be noted, however, that organisations will be excluded from the requirement to obtain consent under specific conditions set out in the PDPA. For example, the PDPA will not require employers to obtain the consent of prospective employees before collecting their personal data, nor is consent required for business contact information. In addition, individual consent need not be obtained where the data is collected, used or disclosed in certain situations such as where the use of data is for artistic or literary purposes or where it is used in investigations and proceedings.

In summary, the main obligations of relevant organisations under the PDPA when it comes into force in January 2014 will be to:

1. Appoint an officer to be responsible for ensuring that the organisation complies with the requirements of the PDPA;
2. Obtain consent for the collection, use or disclosure of personal data;
3. Make reasonable efforts to ensure that the personal data collected by or on behalf of the organisation is accurate and complete;
4. Protect the personal data in its possession or under its control by making reasonable security arrangements to prevent authorised access, collection, use, disclosure, copying, modification, disposal or similar risks;
5. Provide individuals with access to the personal data stored by the organisation upon request;
6. Correct the personal data of individuals upon request; and
7. Protect all personal data in its custody.

**Right of Private Action**

Individuals who have suffered loss or damage as a result of an organisation’s failure to comply with the abovementioned requirements of the PDPA will be able to seek redress through civil proceedings. In particular, the PDPA provides that in the event that the Commission established under the PDPA has already made a decision regarding the contravention in question, the civil proceedings will only be able to commence after the decision has been finalised, as a result of there being no further right of appeal.

**Do Not Call (“DNC”) Registry**

The PDPA also paves the way for the establishment of the DNC Registry, the provisions of which cover telephone calls, faxes and text messages. Under this scheme, individuals may register their Singapore numbers with the DNC signalling that they do not want to be contacted by companies for marketing purposes.

Affected organisations should note that no specified marketing messages may be sent out unless they have confirmed within 30 days of the actual delivery of such messages that the proposed recipients are not registered in the DNC Registry.

Further, the PDPA will require all specified marketing messages to clearly identify the sender of the messages, and to contain the contact details of the sender.

To enable companies to fulfil their obligations under the DNC provisions, the PDPC intends to roll out training and guidance for companies to assist them in understanding and complying with the PDPA.

**Transitional Arrangements**

The Ministry of Communications and Information has confirmed that provisions relating to the data protection rules are expected to come into force after a transition period of at least 18 months on 2 July
2014. This is to allow organisations to put into place the necessary measures to comply with their obligations under the PDPA. However, organisations ought to take note that there will be a shorter sunrise period of 12 months in respect of the DNC registry. Accordingly, the DNC registry provisions are expected to come into force on 2 January 2014.

In light of the significant impact that the PDPA has on the operations of all private sector organisations, such organisations would be well-advised to thoroughly familiarise themselves with the PDPA so that early preparations for the establishment of the necessary compliance measures can be put into place.

This article is intended to highlight the salient issues relating to the PDPA introduced recently in Singapore, and is not intended to be comprehensive nor should it be construed as legal advice. Please note that should you need to discuss how the PDPA will affect your organisation or require more information concerning the PDPA, our following Directors at Gateway Law Corporation would be glad to assist you:

Written by: Max Ng (Managing Director) | Teo Yi-Ling (Director) | Teo Yi Hui (Legal Trainee)