JONES DAY

OCTOBER 2014

COMMENTARY

Singapore's Data Protection Law

Vast amounts of personal data are collected from or about individuals every day, and then used and transferred by organizations. In response to this growing trend and concerns regarding how such personal data is used, Singapore recently introduced the Personal Data Protection Act (Act 26 of 2012) (the "PDPA") to regulate how personal data is handled. The PDPA establishes an overarching data protection framework, setting out baseline rules on the collection, use, disclosure, and protection of personal data by private sector organizations. The PDPA also establishes the Personal Data Privacy Commission (the "PDPC"), which is responsible for the administration and enforcement of the PDPA.

The PDPA establishes two distinct regimes in Singapore for the protection of personal data:

- The "Do Not Call" Regime, which came into force on January 2, 2014; and
- The Data Privacy Provisions, which came into force on July 2, 2014.

Personal Data Covered Under the PDPA

The PDPA applies to "personal data," which means all types of personal data (whether true or not), from which an individual (whether living or deceased) can be identified (except for personal data that has been expressly excluded—see below). The PDPA covers personal data stored in electronic and nonelectronic forms. Examples of personal data include passport number, date of birth, photographs, and DNA profiles.

If an organization collects certain information that does not by itself directly identify an individual, that information may still be protected under the PDPA if the organization has, or is likely to have, access to other data that, together with the information collected, can be used to identify an individual. Similarly, a single set of data that can be used to identify more than one individual will be deemed to be the personal data of all identified or identifiable individuals.

Personal Data Excluded Under the PDPA

The following forms of personal data are excluded:

- Business contact information (e.g., name, job title, business telephone, and business email address) as long as such details have been provided for a business purpose and not solely for personal purposes;
- Personal data contained in a record that has been in existence for at least 100 years; and
- Personal data of a person who has been deceased for more than 10 years.

Key Principles of Singapore's Personal Data Protection Law

Consent

An organization must obtain the consent of the individual before collecting, using, or disclosing his or her personal data for a particular purpose (unless an exception applies). The individual must know the purpose for which the personal data is collected in order for the consent to be valid.

Deemed Consent

An individual is deemed to consent to the collection, use, and disclosure of his or her personal data for a particular purpose if the individual voluntarily provides the personal data to the organization for such purpose and it is reasonable that the individual would voluntarily provide such data.

Withdrawal of Consent

Individuals may at any time withdraw consent given or deemed given in relation to the collection, use, or disclosure of their personal data. Organizations must not prohibit individuals from withdrawing consent, but this does not affect any legal consequences arising from withdrawal of consent (e.g., if the withdrawal makes it impossible for a contract to be fulfilled).

Reasonableness

Organizations may collect, use, or disclose personal data provided the purposes for which the data was collected would be considered appropriate to a reasonable person.

Accuracy

An organization must use reasonable efforts to ensure that personal data is accurate and complete if the data is likely to be used to make a decision affecting the individual concerned or to be disclosed to another organization.

Transfer

Personal data must not be transferred outside Singapore if such personal data cannot be protected in a manner comparable to the protection afforded under the PDPA.

Who is Covered Under the PDPA?

The PDPA applies to all private sector organizations that collect, use, or disclose personal data, unless they fall within one of the categories of organizations expressly excluded from the application of the PDPA.

The following are generally excluded from the application of the PDPA:

- Any individual acting in a personal or domestic capacity;
- Any employee acting in the course of his employment (in such cases, it is the employer who is liable to comply with the PDPA);
- Any public agency or any organization acting as agent of a public agency in relation to the collection, use, or disclosure of personal data; and
- Any other classes of organizations or personal data prescribed from time to time.

Enforcement

To ensure compliance with the foregoing, the PDPC may give an organization such directives as the PDPC thinks fit, including, among others:

- To stop collecting, using, or disclosing personal data in contravention of the PDPA;
- To destroy personal data collected in contravention of the PDPA;
- To pay a financial penalty not exceeding S$1 million.

The "Do Not Call" Regime

The PDPA establishes a "Do Not Call Regime" ("DNC Regime") consisting of three separate registers covering telephone calls, text messages, and faxes. Individuals are able to register their Singapore numbers on one or more of the registers depending on his or her preference. Subject to certain exceptions, registration of a number on a DNC register means that an organization is prohibited from sending certain marketing messages to that number, unless the organization has obtained clear and unambiguous consent from the intended recipient to be able to send marketing messages to the

relevant number. The organization must be able to give evidence of such consent in writing or some similar form (e.g., recording of verbal consent).

If consent has not been obtained, organizations wanting to send certain marketing messages to Singapore telephone numbers have two duties:

- A duty to check the relevant DNC register to confirm that the Singapore number to which the message is to be sent has not been listed in the register; and
- A duty to ensure that the message identifies the sender and includes information as to how the recipient can contact the sender to unsubscribe.

After conducting a search of the relevant register, an organization has 30 days to send its message to the intended recipient(s).

Breaching the provisions of the DNC Regime can result in fines of up to S$10,000 per offense. As of May 2014, the PDPC announced that it has made investigations in response to 3,700 valid complaints against 630 organizations for breaches of the DNC Regime. In connection with such investigations, it has charged a tuition agency and its sole director for offenses relating to the DNC Regime, and the agency and director were fined S$39,000 each. The PDPC has also censured multiple organizations for breaching the DNC Regime requirements.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Sushma Jobanputra
Singapore
+65.6233.5989
sjobanputra@jonesday.com

Elaine Ho
Singapore
+65.6233.5982
elaineho@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Anita Leung
Hong Kong
+852.3189.7313
aleung@jonesday.com