HighQ

Global Data Privacy Guide

Singapore

Submitted by **Rajah & Tann Singapore LLP, the Lex Mundi member firm for Singapore**

This overview is provided by Rajah & Tann Singapore LLP, the Lex Mundi member firm for Singapore.

Contributor: Steve Tan

Contents

Key Legislation Overview

What is the key legislation?

Personal Data Protection Act 2012 (“PDPA”)

The PDPA regulates the collection, use, disclosure and processing of personal data in Singapore.

The PDPA also provides for the establishment of a Do-Not-Call (“DNC”) Registry, which allows individuals to opt out of marketing messages that are sent by way of voice calls, text messages or fax messages, by

registering their Singapore telephone numbers in the three (3) DNC registries (for voice calls, texts and faxes) (the “DNC Provisions”). The DNC Provisions would need to be strictly complied with as a breach is a criminal offence.

The Personal Data Protection Commission (“PDPC”) was established to administer and enforce the PDPA.

There are various subsidiary legislation such as the Personal Data Protection Regulations 2014.

The PDPC has also issued several guidelines to provide guidance on the PDPA, although these do not have the force of law and will not bind the PDPC in its administration and enforcement of the PDPA.

Details:	N/A N/A

Key Data Protection Provisions

What data is protected?	Any data that identifies or potentially identifies an individual (whether living or deceased) The PDPA regulates the processing of personal data. “personal data” is defined as data, whether true or not, about an individual who can be identified: (a) from that data; or (b) from that data and other information to which the organization has or is likely to have access.
Details:	N/A
Who is subject to privacy obligations?	All organizations (includes individuals, companies, associations or body of persons) regardless of size The data privacy obligations are imposed on any “organization”, which is broadly defined under the PDPA to include any individual, company, association or body of persons, corporate or unincorporated, whether or not: a. formed or recognized under the law of Singapore; or

	b. resident, or having an office or a place of business, in Singapore. This definition means that the PDPA has significant extraterritorial effect.
Details:	N/A N/A
How is the collection of personal data regulated?	Personal data of an individual cannot be collected and processed for any purpose unless at or prior to collection, the organisation notifies the individual of the purposes for which the personal data is collected, and obtains consent from the individual. Generally, an organization will be prohibited from collecting an individual's personal data, unless the individual gives, or is deemed to have given, his consent for the collection, use or disclosure of his personal data. Such consent must be 'valid' and the PDPA sets out additional obligations that organizations must comply with when obtaining consent, for example, prohibiting organisations from obtaining or attempting to obtain consent by providing false or misleading information or using deceptive or misleading practices. There is a limited list of exceptions for when an organisation may collect personal data about an individual without the consent of the individual. Further, the personal data must only be collected for purposes that a reasonable person would consider appropriate in the circumstances.
Details:	N/A
How are the use and disclosure of personal data regulated?	Personal data of an individual cannot be used or disclosed for any purpose unless the organisation had notified the individual of the purposes for which the personal data will be used or disclosed, and obtained consent from the individual. Generally, an organization will be prohibited from using or disclosing an individual's personal data, unless the individual gives, or is deemed to have given, his consent for the use or disclosure of his personal data. Such consent must be 'valid' and the PDPA sets out additional obligations that organisations must comply with when obtaining consent, for example,

	prohibiting organisations from obtaining or attempting to obtain consent by providing false or misleading information or using deceptive or misleading practices. There is a limited list of exceptions for when an organization may use or disclose personal data about an individual without the consent of the individual. Further, the personal data must only be used or disclosed for purposes that a reasonable person would consider appropriate in the circumstances.
Details:	N/A
How are storage, security and retention of personal data regulated?	Personal data must be protected from unauthorised access, collection, use, disclosure, etc. through security arrangements that are reasonable and appropriate in the circumstances. Organisations must not retain personal data where the purpose of collection is no longer relevant and there is no legal or business purpose to retain the same. In terms of storage and security, the PDPA requires an organization to put in place reasonable security arrangements to protect personal data in its possession or under its control in order to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks. In terms of retention of personal data, the PDPA requires an organization to destroy or anonymize personal data when the purpose for which that personal data was collected is no longer relevant and retention is no longer necessary for legal or business purpose.
Details:	N/A
Are there rights of access to and correction of personal data?	An individual has the right to request access and correction to his personal data.

	Upon request by an individual, an organization must provide the individual within a specified time, with: personal data about the individual that is in the possession or under the control of the organization; and information about the ways in which that personal data has been or may have been used or disclosed by the organization within a year before the date of the individual's request. There is a limited list of exceptions to the above mentioned access right. Upon a request for correction of personal data by an individual, an organization will be required to: a. correct the personal data within a specified time; and b. send the corrected personal data to every other organization to which the personal data was disclosed by the organization within a year before the date the correction was made unless that other organization does not need the corrected personal data for any legal or business purpose. There is a limited list of exceptions to the above mentioned access right.
Are there restrictions on cross border data transfers?	An organization is prohibited from transferring personal data of any individual out of Singapore unless certain conditions are met. An organization must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that organizations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA. The transferor must ensure that the recipient of the personal data in the country outside Singapore is bound by legally enforceable obligations to provide the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.
Details:	N/A
Are there any notification requirements for data breaches?	No There is no mandatory notification requirement for data breaches under the PDPA. However, the PDPC encourages notification. Further, it may be viewed as a point of mitigation.

Details:	N/A
Who is the privacy regulator?	The Personal Data Protection Commission The PDPA confers various powers on the Personal Data Protection Commission (PDPC), including powers of investigation, power to issue directions and penalties to non-compliant organisations, as well as the power to review an organisation's reply to a request made by an individual under the access and correction principles. It is important to note that the PDPC is empowered to issue fines of up to S$ 1 million per breach of the PDPA and that it may do so of its own accord.
Details:	N/A
What are the consequences of a privacy breach?	The PDPC may issue the breaching organisation a fine of up to S$ 1 million per breach and/or issue relevant directions. Some breaches may amount to a criminal offence. Affected individuals have statutory rights under the PDPA to commence a lawsuit against the breaching organisation. An individual may lodge a complaint to the organisation directly, or to the PDPC, if he or she is aware of non-compliance with the PDPA. The PDPC may conduct an investigation, either on its own accord or upon receiving a complaint from an individual or organisation, to determine if an organisation has complied with the PDPA. The PDPC is empowered to give directions to the organisation such as to : (a) stop collecting, using or disclosing personal data in contravention of the PDPA; destroy the personal data collected in contravention of the PDPA; and/or pay a financial penalty of an amount not exceeding $1 million. (b) Further, certain breaches of the PDPA may result in criminal liability. (c) Breaches of the DNC Provisions amount to criminal offences. In addition, the PDPA provides individuals who suffer loss or damage as a result of a breach of the PDPA the right to commence civil proceedings in the courts against the organisation.

Details:	N/A
How is electronic marketing regulated?	Organizations sending marketing messages will need to be aware of its obligations under the PDPA and Spam Control Act. Electronic marketing is regulated under 2 main pieces of legislation: a. PDPA; and b. Spam Control Act (Cap. 311A) (“SCA”). The DNC Provisions cover messages that contain marketing elements which can be received by recipients via: • voice calls; • smses / mmses (short message service / multimedia messaging service); and • facsimiles. One of the requirements of the DNC Provisions is that it requires a sender of such marketing messages to first check the respective DNC registry to ascertain whether the recipient’s number is on the registry. If the recipient’s number is on the registry, the sender must not send marketing messages to that number. This is unless the sender has received prior clear and unambiguous consent from the recipient. Other requirements are applicable as well. A breach of the DNC Provisions is criminal. The SCA was enacted to control email and mobile spam in Singapore. Under the SCA, marketers are under certain obligations when sending unsolicited communications through emails or text messages. Such obligations include providing a means to unsubscribe in the marketing message, and labeling the messages as advertisements with the letters.
Details:	N/A
Are there any recent developments or expected reforms?	There are no reform proposals currently in place. There are no reform proposals currently in place.
Details:	N/A
If you are based in the United States, what are state-driven	N/A

privacy laws that may be unique to your jurisdiction?	N/A
Details:	