waystone | Compliance Solutions

Personal data protection in Singapore

September 2, 2024

Overview of the Singapore Personal Data Protection Act (PDPA)

The PDPA comprises various requirements governing the collection, use and disclosure of personal data in Singapore. It recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose the data for legitimate and reasonable purposes.

All organisations carrying out activities involving personal data in Singapore are required to comply with the PDPA. This comprises two main sets of requirements; personal data protection and the Do Not Call (DNC) registry.

What is personal data?

Personal data refers to data concerning 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. It does not apply to:

- an individual acting in a personal or domestic capacity
- an individual acting in his/her capacity as an employee within an organisation
- any public agency in relation to the collection, use or disclosure of personal data
- business contact information - this refers to an individual's name, position or title, business telephone number, business address, business email, business fax number and similar information.

Main obligations of the PDPA

The personal data protection requirement covers personal data stored in both electronic and non-electronic forms.

In summary, organisations are required to adhere to the personal data protection requirements as follows:

a) having reasonable purposes, notifying purposes and obtaining consent for the collection, use or disclosure of personal data

b) allowing individuals to access and correct their personal data

c) taking care of personal data (which relates to ensuring accuracy), protecting personal data in its possession or under its control (including protection in the case of international transfers) and not retaining personal data if no longer needed

d) notifying the Commission and affected individuals of data breaches

e) implementing policies and procedures to comply with the PDPA and make information about its policies and procedures publicly available.

Organisations can consider the following steps when managing personal data:

Step 1: Appoint a Data Protection Officer

Organisations are legally required to appoint a Data Protection Officer (DPO) and the DPO's contact information must be made available to the public, in compliance with PDPA. The DPO is responsible for ensuring that the business stays compliant with PDPA and other relevant data protection laws. The DPO would be the primary point of contact for matters relating to data protection/queries/breaches within the organisation as well as with the Personal Data Protection Commission (PDPC). This role may be assumed by an employee of the organisation or outsourced to a third-party service provider.

Step 2: Map out your personal data inventory

Develop an inventory of all the personal data that the organisation holds. Be responsible for the personal data in possession, be clear about how, when and where the data is collected. Know the purpose of data collection and obtain consent for the use and disclosure of the personal data collected.

Auditing and indexing the inventory will enable the organisation to manage its personal data records more effectively.

Step 3: Implement data protection processes

With the personal data inventory in place, the DPO should review the organisation's personal data protection practices and align them with the PDPA. This can come in the form of setting up policies and processes to inform an individual of the purpose of collection, use or disclosure of the personal data, obtaining consent, allowing the individual to withdraw consent at any time upon giving reasonable notice. It must establish clear practices for assessing and processing access, correction requests and complaints. In addition, it must also set clear timelines for the retention of personal data and cease retention of documents containing personal data when no longer required for any business or legal purposes.

Step 4: Communicate to employees

Inform all employees of the organisation's data protection policies and their role in safeguarding personal data. The DPO must ensure employees are aware of the internal processes regarding protecting personal data.

Step 5: Establish an internal audit policy

Conduct regular internal audits to ensure the organisation's processes adhere to the PDPA.

Do Not Call (DNC) registry

The DNC registry covers telephone calls, text messages and fax messages. Individuals may register their Singapore telephone number(s) with any or all of the DNC registers to opt out of unsolicited telemarketing messages, depending on their preferences. This registration does not expire, unless the individual withdraws their registrations or terminates their numbers.

Organisations have the following obligations, before sending any telemarketing messages via any means to Singapore telephone numbers:

a) checking the relevant DNC Register(s) to confirm if the Singapore telephone number is listed

b) providing information on the individual or organisation who sent or authorised the sending of the marketing message

c) not concealing or withholding the identity of the sender of the marketing message.

Exceptions

Organisations do not need to check the DNC Registry if:

- the individual has given clear and unambiguous consent in writing or in other accessible form to the sender of the marketing message to that Singapore telephone number
- organisations are sending certain messages related to the subject of the ongoing relationship with the individuals.

How Waystone can help

Waystone offers the following services to help organisations remain compliant with their data protection obligations:

- Assisting the organisation with designating an individual as a DPO and supporting the registration with the Accounting and Regulatory Authority of Singapore (ACRA).
- Addressing complex queries and complaints from data subjects or supervisory authorities such as PDPC and reviewing the approach of the organisation, where required.
- Conducting health checks and providing recommendations to address any compliance gaps related to Singapore's personal data protection requirements. This includes reviewing personal data frameworks and implementation measures that have been adopted.
- Assisting with the drafting of a PDP policy in line with the requirements of Singapore's PDPA and the industry best practices.
- Providing the relevant training and awareness session to the organisation, considering their level of exposure to the data protection risk.

Waystone Compliance Solutions' APAC team specialises in navigating the complex landscape of regulatory compliance in Singapore. If you would like to find out more information on this topic and how it may affect your organisation, please reach out to our APAC Compliance Solution team or your usual Waystone representative.

Contact Us →