WHEN BUSINESS GETS PERSONAL

A QUICK GUIDE TO THE PERSONAL DATA PROTECTION ACT 2012 FOR ORGANISATIONS

pdpc

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

www.pdpc.gov.sg

Introduction

Organisations today collect and use personal data of individuals such as customers, employees or members of associations. They need such data for providing products and services to customers, understanding customers' profile and market trends to develop better products and services so as to retain their competitive edge, and managing employment and members' relationships. These individuals trust organisations to use and disclose their personal data appropriately and keep their information safe.

The Personal Data Protection Act 2012

The Personal Data Protection Act 2012 (PDPA) governs the collection, use and disclosure of personal data by private organisations, in a way that recognises both the needs of individuals and organisations.

BENEFITS

Individuals

- Gives individuals more control over how their personal data is collected, used and disclosed.
- Allows individuals to access and correct their personal data held by organisations.

Organisations

- Builds consumer confidence.
- Facilitates safe and protected cross-border transfer of information.
- Enhances efficiency and productivity, branding and competitiveness.

Singapore

- Serves to strengthen Singapore's position as a trusted hub for data hosting and management activities.

The PDPA contains two sets of requirements, covering personal data protection and the Do Not Call (DNC) Registry, which came into force on 2 July 2014 and 2 January 2014 respectively. There was an 18-month transition period to allow organisations time to review and adopt internal personal data protection policies and practices in accordance with the PDPA.

The personal data protection requirements cover personal data stored in electronic and non-electronic forms. The requirements, however, do not apply to:

- An individual acting in a personal or domestic capacity.
- An employee acting in the course of his/her employment with an organisation.
- A public agency or an organisation acting on behalf of a public agency in relation to the collection, use or disclosure of personal data.
- Business contact information. This refers to an individual's name, position name or title, business telephone number/address/email address/fax number and any other similar information about the individual, not provided by the individual solely for his/her personal purposes.
- Personal data about a deceased individual, except that the provisions relating to disclosure and protection of personal data will apply to personal data about an individual who has been dead for 10 years or fewer.
- Personal data contained in a record that has been in existence for at least 100 years.

9 Main Obligations of the PDPA

1 CONSENT OBLIGATION

Only collect, use or disclose personal data when an individual has given his/her consent.

Allow individuals to withdraw consent, with reasonable notice, and inform them of the likely consequences of withdrawal. Upon withdrawal, and depending on the withdrawal request, you must cease to collect, use or disclose their personal data.

2 PURPOSE LIMITATION OBLIGATION

You may collect, use or disclose personal data about an individual for the purpose for which he/she has given consent. You may not, as a condition of providing a product or service, require the individual to consent to the collection, use or disclosure of his/her personal data beyond what is reasonable to provide that product or service.

3 NOTIFICATION OBLIGATION

Notify individuals of the purposes for which you are intending to collect, use or disclose their personal data on or before such collection, use or disclosure of personal data.

9 OPENNESS OBLIGATION

Make information about your data protection policies, practices and complaints process available on request.

Designate one or more individuals to implement personal data protection policies within your organisation. The business contact information of your data protection officer(s) should also be made available to the public. However, compliance with the PDPA remains the responsibility of the organisation.

ORGANISATION

Subject to all the obligations under the PDPA, unless an exception applies.

Data Intermediary

Subject to the Protection and Retention Limitation Obligations only, where it processes personal data for another organisation under a written contract.

4 ACCESS & CORRECTION OBLIGATION

Upon request, the personal data of an individual and information about the ways in which his/her personal data may have been used or disclosed in the past year should be provided.

You are also required to correct any error or omission in an individual's personal data upon his/her request.

8 TRANSFER LIMITATION OBLIGATION

Transfer personal data to another country only according to the requirements prescribed under the regulations, to ensure that the standard of protection provided to the personal data so transferred will be comparable to the protection under the PDPA.

7 RETENTION LIMITATION OBLIGATION

Cease retention of personal data or remove the means by which the personal data can be associated with particular individuals when it is no longer necessary for any business or legal purposes.

6 PROTECTION OBLIGATION

Make security arrangements to protect the personal data that you possess or control to prevent unauthorised access, collection, use, disclosure, or similar risks.

5 ACCURACY OBLIGATION

Ensure that personal data collected by or on behalf of your organisation is reasonably accurate and complete.

What is Personal Data?

Personal data refers to data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which an organisation has or is likely to have access. These can range from names, contact numbers and addresses to other types of data that do not directly identify an individual on its own but form part of an accessible record about an individual.

Existing Data

You may continue to use personal data that has been collected before the PDPA comes into effect for the purposes for which the personal data was collected, unless the individual has withdrawn consent. If there is a fresh purpose for the use of the personal data, consent has to be obtained anew. For personal data collected after the PDPA comes into effect, you will have to notify and obtain the individual's consent to the collection, use and disclosure of his/her personal data.

* Please refer to the PDPA for further details on the scope of the Data Protection provisions including the exceptions. Organisations should assess and be satisfied if any exception provided in the PDPA would apply.

Getting Started

Here are some possible steps you can take to get started:

STEP 1 Appoint a Data Protection Officer

Designate at least one person to oversee your organisation's compliance with the PDPA. This person may be an employee in your organisation, and his/her role may include developing policies for handling personal data in electronic or non-electronic forms, communicating internal personal data policies to customers, and handling any queries or complaints about personal data.

STEP 2 Map Out Your Personal Data Inventory

Be responsible for the personal data in your possession or under your control. Be clear about how, when and where you collected the data. Know the purpose of data collection and obtain consent for the use and disclosure of the personal data collected.

STEP 3 Implement Data Protection Processes

After understanding your organisation's personal data inventory, you should review its data management framework and processes to align them with the PDPA. Here are some things to consider:

- Set up policies and processes to inform an individual of the purpose of the collection, use or disclosure of his personal data and obtain his consent. Set up policies and processes to allow the individual to withdraw consent at anytime upon giving reasonable notice.
- Establish a clear practice for assessing and processing access and correction requests and complaints. Provide information to customers on how they may request to access and correct their personal data or file a complaint with your organisation.
- Regularly review the sufficiency of the protection policy and mechanisms for the personal data in your possession or control. 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.
- Review the terms of engagement with third parties such as agents, partners or data intermediaries to ensure adherence to the PDPA.

STEP 4 Communicate to Employees

Inform all employees of the organisation's data protection policies and their role in safeguarding personal data. Ensure your employees know what the internal processes are with regard to protecting personal data.

STEP 5 Establish an Internal Audit Policy

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

DNC Registry Provisions

There will be three Do Not Call (DNC) Registers created for **voice calls**, **text messages (e.g.SMS/MMS)** and **fax messages**. To opt out of unsolicited telemarketing messages, individuals may register their Singapore telephone numbers with any or all of the DNC Registers for free. Their registration does not expire, unless they withdraw their registrations or terminate their numbers.

If your organisation would like to send telemarketing messages via any or all three means, before doing so, you will need to:

- check the relevant register(s) before sending telemarketing messages;
- provide contact information about the organisation who sent or authorised the sending of the telemarketing messages within the message; and
- ensure the calling line identity is not concealed or withheld (for voice calls).

If you have obtained the individual's clear and unambiguous consent in written or other accessible form to receive telemarketing messages specifically through voice calls, text messages or fax messages from your organisation, you may do so regardless of whether he/she is registered with the DNC Registry.

The DNC Registry, however, does not cover messages sent for other purposes, such as service calls or reminder messages sent by organisations to render services bought by the individual. Telemarketing calls or messages of a commercial nature that target businesses are also excluded from the DNC Registry provisions.

For more information on the exclusion of marketing messages under the DNC provisions, please refer to the Eighth Schedule of the PDPA.

Useful Information

Call Us

General Enquiries: +65 6377 3131

Quality Service Manager: 1800 270 0222 / +65 6270 0222

Fax Us

Fax: +65 6273 7370

Email Us

General Enquiries: info@pdpc.gov.sg

Quality Service Manager: pdpc_qsm@pdpc.gov.sg

Or fill up our online feedback form at www.pdpc.gov.sg/feedback

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE