pdpc
PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

DATA PROTECTION STARTER KIT

pdpc
PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Address: 460 Alexandra Road
#10-02 PSA Building
Singapore 119963
Main Line : +65 6377 3131
Fax : +65 6273 7370

Notations

Refer to PDPC's website for more information

Important information

Sample clauses

Sample forms

<xxxxx> Placeholder to insert your organisation's relevant information as indicated

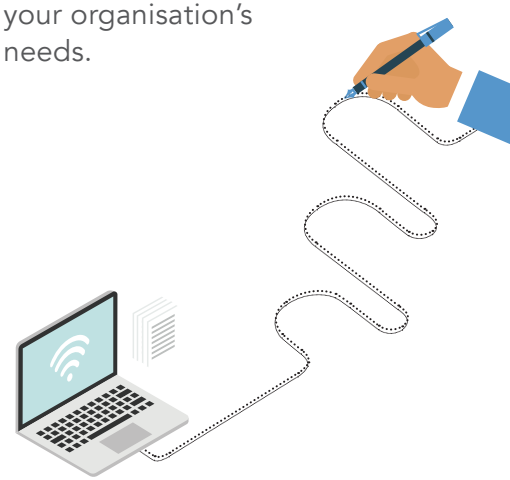
A Quick Start On How To Handle Personal Data

Do you collect, use or disclose personal data of employees, customers or other individuals? If the answer is yes, you should ensure that your organisation has put in place systems, policies and processes to comply with the Personal Data Protection Act.

Kick-start data protection practices within your organisation today!

The Personal Data Protection Commission (PDPC) has put together this Data Protection (DP) Starter Kit to help you kick-start data protection practices within your organisation. This kit contains useful information and resources such as sample forms, clauses and communication material that are easy to implement*. It will also guide you through common issues that you may face in complying with Data Protection (DP) and Do Not Call (DNC) provisions.

This may just be the start of your organisation's data protection journey, but it is an important first step to take. As this kit serves as a basic guide, you may need to consider whether or not to engage professional services to conduct a comprehensive assessment to evaluate your organisation's needs.



* Note that samples provided in this kit are for illustrative purposes. You should evaluate your own requirements in light of your obligations under the PDPA and customise the samples according to your business needs before inserting them into your organisation's forms or agreements (as appropriate).

About The PDPA

The Personal Data Protection Act (PDPA) governs the collection, use and disclosure of personal data by organisations, in a manner that recognises individuals' rights and the need of organisations to use such personal data for legitimate business purposes.

Full Name

Passport number

National Registration Identity Card (NRIC) number or Foreign Identification Number (FIN)

Thumbprint

Personal mobile telephone number

Iris image

DNA profile

Voice recording of an individual

Photograph or video image of an individual

The PDPA contains two main sets of provisions; namely Data Protection (DP) provisions and the Do Not Call (DNC) provisions.

9 Data Protection Obligations

Collection, use and disclosure of personal data

Consent

- Obtain consent to collect, use or disclose individuals' personal data.
- Allow individuals to withdraw consent.

Purpose

- Do not make customers consent to the collection, use or disclosure of their personal data beyond what is reasonable to provide the product or service.
- Collect, use or disclose personal data only for the purposes for which consent was obtained.

Notification

- Notify individuals of the purposes for the collection, use or disclosure of their personal data.

Accountability to individuals

Access and Correction

- Upon request, provide individuals with their personal data and the ways in which their personal data were collected, used or disclosed in the past year.
- Correct any error or omission in individuals' personal data upon their request.

Openness

- Appoint a Data Protection Officer and make his/her business contact information readily available to the public.
- Publish information on your data protection policies, practices and complaint-handling process.

Care of personal data

Protection

- Put in place reasonable security arrangements to protect personal data from unauthorised access, collection, use, disclosure and similar risks.

Accuracy

- Make reasonable effort to ensure that the personal data collected is accurate and complete.

Retention

- Cease retention or anonymise personal data when it is no longer necessary for any business or legal purposes.

Transfers

- Ensure that the standard of protection accorded to personal data is comparable to the PDPA when it is transferred overseas.

Data intermediaries that process personal data for other organisations under contract must meet the protection and retention requirements under the PDPA.

Do Not Call (DNC) Provisions

The DNC Provisions prohibit organisations from sending certain marketing messages to Singapore telephone numbers including mobile, fixed line, residential and business numbers registered with the DNC Registry.

Check the DNC Registry

Before sending a marketing message to a Singapore telephone number, you must check the DNC Registry established by the PDPC to confirm that the Singapore telephone numbers on your marketing list are not registered, unless you have obtained clear and unambiguous consent to send the marketing message to the user or subscriber of that number.*

For more information on the DNC Provisions, refer to the Advisory Guidelines on the Do Not Call Provisions (www.pdpc.gov.sg/ag).

*Note: Consent obtained has to be clear and unambiguous, and in written or other accessible form.

10 Steps To Get Started

Appoint A Data Protection Officer

All organisations, including sole proprietors and non-profit organisations, must appoint at least one person as the Data Protection Officer (DPO). The DPO function is management's responsibility and, ideally, the appointed DPO should be part of the management team, or at least have a direct line to management. The operational DPO functions, however, may be delegated to one or a few employees, or outsourced to a service provider.

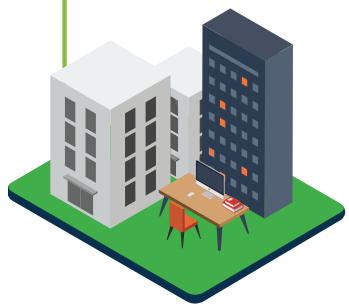
Once you have decided on the person(s) to appoint, it is important to brief him/her on his/her roles and responsibilities. Next, inform all your staff on who the DPO is so that they can forward all PDPA-related queries and complaints to him/her. Strong management support is necessary for the DPO to carry out his/her role effectively.

What does a DPO do?

- Ensures compliance of PDPA when developing and implementing policies and processes for handling personal data;
- Fosters a data protection culture among employees and communicate personal data protection policies to stakeholders;
- Manages personal data protection-related queries and complaints;
- Alerts management to any risks that might arise with regard to personal data; and
- Liaises with the PDPC on data protection matters, if necessary.

Make the business contact information of your DPO available

Organisations are required to ensure that the DPO can be easily contacted by the public.



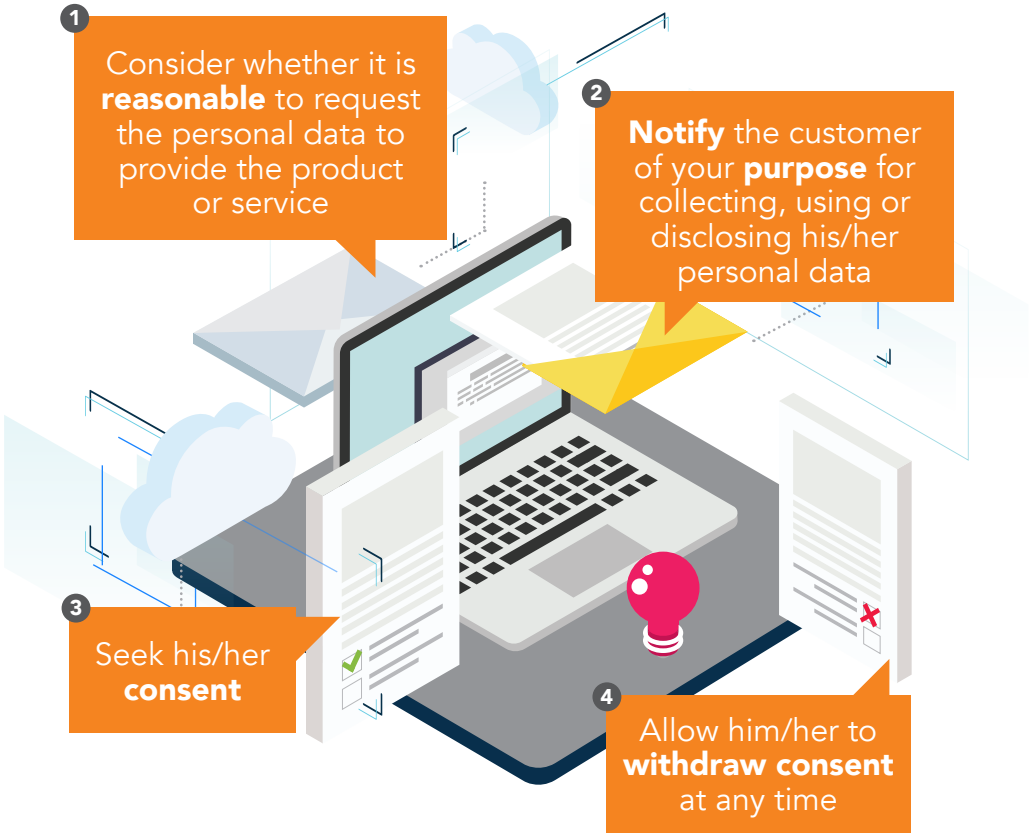
For more information about DPOs, refer to **www.pdpc.gov.sg/dpo.**

Note: The appointment of a DPO is a mandatory requirement under the PDPA. A DPO is an important driver to ensure the organisation's data protection measures are adequate.

Register your DPO with us at www.pdpc.gov.sg/dpo-contact!

Notify Purpose(s) And Seek Consent

Below are some steps to follow when collecting personal data:



Sample Clauses for Getting Consent from Customers and Employees

i) Consent Clause for Membership Application

This sample is applicable for organisations offering memberships.

Name: .....

Signature: .....

Date: .....

By signing this membership application form, you agree that <organisation name> may collect, use and disclose your personal data as provided in this application form, or (if applicable) as obtained by our organisation as a result of your membership, for the following purposes in accordance with the Personal Data Protection Act 2012 and our data protection policy (available at our website <webpage URL>):

(a) the processing of this membership application; and

(b) the administration of the membership with our organisation.

Please visit our website at (c) <webpage URL> for further details on our data protection policy, including how you may access and correct your personal data or withdraw consent to the collection, use or disclosure of your personal data.

ii) Consent Clause for Sending Marketing Materials

This sample is suitable for organisations that wish to send customers marketing materials.

You agree that <organisation name> may collect, use and disclose your personal data, which you have provided in this form, for providing marketing materials that you have agreed to receive, in accordance with the Personal Data Protection Act 2012 and our data protection policy (available at our website <webpage URL>).

Please tick the relevant boxes below if you agree to receive the following:

- ☐ Our organisation's monthly newsletter (sent by us via email)
- ☐ Information sent by our organisation about our organisation's products and services, including updates on our latest promotions and new products and services, via the following channels:
  - ☐ Email
  - ☐ Text Message
  - ☐ Phone Call
- ☐ Information sent by our organisation on selected third parties' products and services, such as updates on their latest promotions and their new products and services, via the following channels:
  - ☐ Email
  - ☐ Text Message
  - ☐ Phone Call
- ☐ Information sent by our business partners* on their products and services, via the following channels:
  - ☐ Email
  - ☐ Text Message
  - ☐ Phone Call

*Please note that information will be sent directly by our business partners, and we shall disclose the relevant contact information to them for that purpose.

Name: .....

Date: ..... **Signature:** .....

Please visit our website at <webpage URL> for further details on our data protection policy, including how you may access and correct your personal data or withdraw consent to the collection, use or disclosure of your personal data.

iii) Consent Clause for Lucky Draws

This sample is suitable for organisations conducting lucky draws.

By submitting this lucky draw entry form, you agree that <organisation name> may collect, use and disclose your personal data, as provided in this entry form, for the following purposes in accordance with the Personal Data Protection Act 2012 and our data protection policy (available at our website <webpage URL>):

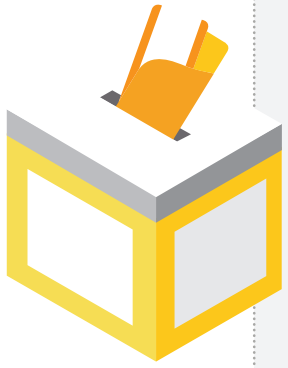
1) to administer this lucky draw, including to contact you for the administration of prizes in relation to this lucky draw.

Name: .....

Date: .....

Signature: .....

Please visit our website at <webpage URL> for further details on our data protection policy, including how you may access and correct your personal data or withdraw consent to the collection, use or disclosure of your personal data.



Do note the following:

- It is important to inform the individual that you are collecting, using or disclosing his personal data for a lucky draw and to obtain consent for that purpose.
- If you plan to use the personal data for some other purpose outside of the administration of the lucky draw, you must state so clearly.

iv) Consent Clause for Job Applicants

This sample can be adopted by an organisation for its recruitment activities.

By signing this form,

(a) you acknowledge that you have read, understood and agreed to the above Policy <refer to URL below>, and consent to the collection, use and/or disclosure of your personal data by us for the purposes set out in the Policy; and

(b) in the event that we have received your job application or personal data from any third party pursuant to the purposes set out in the Policy, you warrant that such third party has been duly authorised by you to disclose your personal data to us for the purposes set out in the Policy.

Name: _____

Signature & Date: _____

Please refer to the "Sample Clauses and Template for Employees and Job Applicants" at www.pdpc.gov.sg/org-resources.

v) Acknowledgement and Consent

This sample can be adopted by an organisation supplying and marketing business-to-consumer goods and/or services.

I acknowledge that I have read and understood the above Data Protection Notice <refer to URL below>, and consent to the collection, use and disclosure of my personal data by [name of organisation] for the purposes set out in the Notice.

Please tick the relevant boxes below if you agree to receive the following marketing materials:

- □ I do not wish to receive any marketing information.
- □ I would like to receive information about the goods and services which may be provided by [name of organisation], including (but not limited to) offers, promotions and information about new goods and services, via the following channels:
  - □ newsletter
  - □ email
  - □ text message
  - □ telephone call

Name: _____

Signature & Date : _____

Please refer to the "Sample Clauses and Template for Customers" at www.pdpc.gov.sg/org-resources.

Note:

- Organisations wishing to use this should ensure that the policies and processes described are aligned with their own internal policies and processes.
- Personal data should only be collected for reasonable purposes which have been notified to the individual in advance and for which the individual has consented, unless collection without consent is permitted or required under the PDPA or any other written law.

Withdrawal of Consent

An individual may at any time withdraw consent that he/she had given to an organisation for the collection, use or disclosure of his/her personal data.

When you receive a request to withdraw consent,

- You must inform the individual of the likely consequences of withdrawing his/her consent. You must stop using his/her personal data after the withdrawal. Do not keep the personal data if you have no business or legal purpose to do so.

- If it requires more than 10 business days to effect the withdrawal notice, it is good practice to inform the individual when he/she can expect the withdrawal of consent to take effect.

- Similarly, if an individual opts out of receiving your organisation's telemarketing messages, you must ensure that such messages will no longer be sent to his/her Singapore telephone number by the end of 30 days.

Sample Clause for Customers to Withdraw Consent

i) Sample Clause for Withdrawing Consent Given for Receiving Marketing Materials

This sample can be used for individuals to withdraw consent for receiving marketing materials.

I withdraw my consent to the use and disclosure of my personal data for receiving marketing material as follows*:

* Please tick the relevant boxes below to indicate the categories, and corresponding medium of communication, of the marketing materials for which consent is withdrawn.

- □ Your organisation's monthly newsletter (sent via email)
- □ Information about your organisation's products and services, including updates on the latest promotions and new products and services, via the following channels:
  - □ Email
  - □ Text Message
  - □ Phone Call

- □ Information sent by your organisation on third parties' products and services, such as updates on their latest promotions and their new products and services, via the following channels:
  - □ Email
  - □ Text Message
  - □ Phone Call

- □ The use of my contact details by third parties** to send me information on their products and services, via the following channels:
  - □ Email
  - □ Text Message
  - □ Phone Call

Name: ..... **Date:** .....

Signature: .....

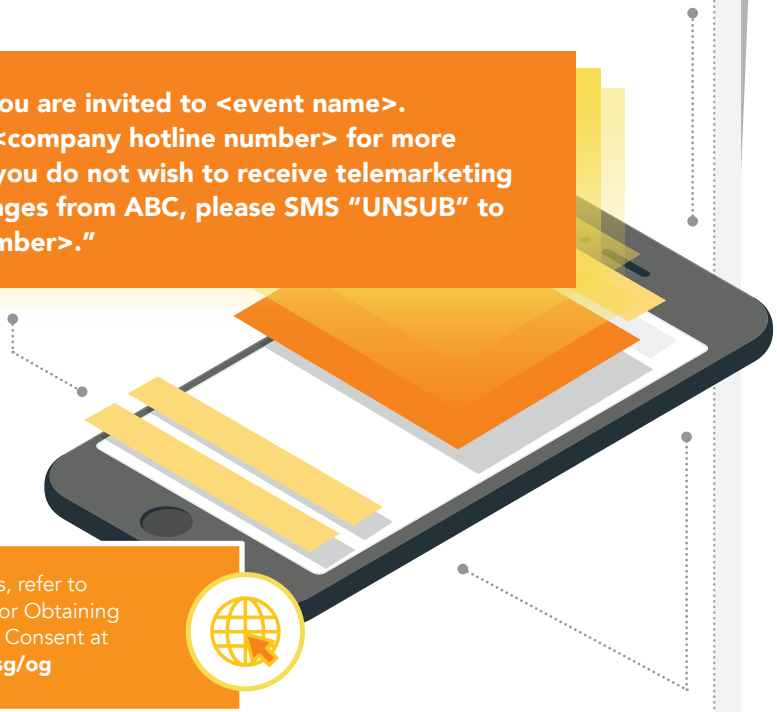
** Third parties that our organisation had disclosed your personal data to for this purpose will be informed of your withdrawal of consent and your personal data will no longer be disclosed to any third parties from the effective date of your withdrawal.

ii) Sample Clause for Opting Out of Receiving Telemarketing Text Messages

In your telemarketing messages, you may provide information on how individuals can opt out of such messages. If you choose to do so, indicate clearly what types of marketing message the withdrawal will affect. If the withdrawal notice is unclear, it may be considered an opt-out of all marketing materials sent via that medium.

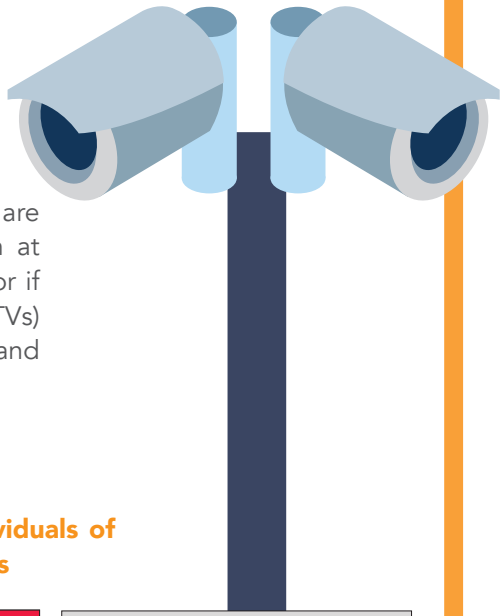
This sample can be used to let individuals opt out of receiving such messages.

"<ADV> You are invited to <event name>. Call us at <company hotline number> for more details. If you do not wish to receive telemarketing text messages from ABC, please SMS "UNSUB" to <unsubnumber>."



For more samples, refer to Sample Clauses for Obtaining and Withdrawing Consent at **www.pdpc.gov.sg/og**

Don't forget to notify when taking photographs or videos



You should inform individuals when you are taking photographs or videos of them at an event that your organisation hosts, or if you have closed-circuit televisions (CCTVs) monitoring the organisation's premises and recording images of visitors.

i) Samples of Notice to Inform Individuals of CCTV Recordings on Your Premises

Note:

- Your notice should state the purpose of the CCTVs (for example, for security purposes).
- Your notices must be clearly printed and placed in areas that are easily visible.
- You do not need to indicate the exact location of your CCTV cameras.

ii) Samples of Notice to Inform Individuals of Photography or Video Recording at Events

When taking photographs or recording videos at events, consider notifying attendees by using signages at the event and/or even before they sign up for it, such as via the registration form.

REGISTRATION FORM

EVENT NAME

Please complete information below

Date:
Venue:

1. Participant's Information

Family Name:
Title:____ ☐ Prof. ☐ DR. ☐ Other: ____ ☐ Mr. ☐ Ms. ☐ Mrs.
First Name:_____
Organisation:_____
Address:_____
Postal Code:_____ City:_____
Country:_____
Telephone:_____
Fax:_____ Email:_____

2. <This event may be recorded and photographed. Your presence at this event is deemed as your consent to being photographed.>

Signage

Photographs and videos may be taken during the event for news and publicity purposes.

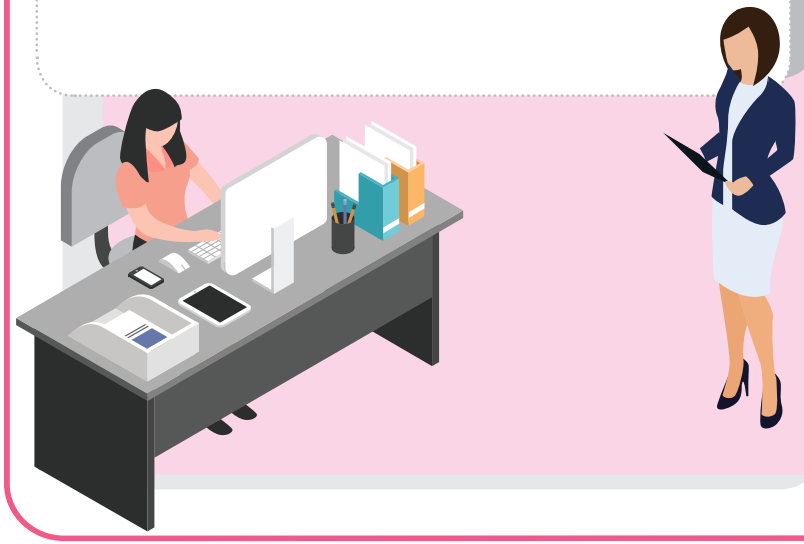
Note:

- You can also state the purposes on the invitation card or the registration form for the event.
- If you intend to rely on notices at the function venue, you should ensure that the notices are easily visible to all attendees e.g. by placing obvious notices at the reception and entrances to the venue.

Respond When Individuals Ask About Their Personal Data

When your customer wants to know what personal data you have collected about him/her and how it has been used and disclosed in the past year, you must provide that information as soon as reasonably possible. You may charge a reasonable fee to cover the processing cost for the request, provided that you give a written estimate of the fee beforehand.

If you are unable to provide it within 30 days, you must inform the individual within 30 days and let him/her know when you can respond.



i) Sample Forms for Access Request and Acknowledgement

Your organisation should state clearly the available channels for individuals to submit an access request. For example, an access request may be submitted in person, through email or by post.

I. APPLICATION TO ACCESS PERSONAL DATA

1. Under the Personal Data Protection Act 2012 ("PDPA"), you are entitled to request for your personal data that we have, and request to know how your personal data had been used or disclosed over the past year.

2. Please complete this form and submit it to:
   <Please specify any other modes to submit an access request below>

   In person or by post:
   Data Protection Officer, Organisation ABC,
   ABC Complex 123, ABC Road, Singapore 123456

   Alternatively, you can email the completed form to us:
   DPO@abc.com.sg

II. PARTICULARS OF REQUESTOR

<For this section, please determine the types of information your organisation requires in order to process the access request, including any documentation required to establish that the requestor is legally authorised to act on behalf of the other individual(s)>

Name of requestor: .....

Contact number: ..... Email address: .....

Please check the applicable box(es):

☐ I am making an access request for my own personal data

☐ I am making an access request on behalf of other individual(s)

Please complete this section if you are making an access request on behalf of other individual(s)

Name of other individual(s) whom you are making an access request on behalf of:

.....

Contact number: ..... Email address: .....

Please furnish a copy of <for organisation to insert proof of identity accepted> for vertification purposes.

III. DESCRIPTION OF THE PERSONAL DATA REQUESTED

Do state your purpose for accessing the personal data so that we can process your access request quickly and efficiently. In addition:

1. please provide the date, time and location of the event if you are requesting access to CCTV or audio records;
2. for all other personal data, please indicate the type of personal data you are requesting for and when you provided it to us.

ii) Sample Acknowledgement Form

It is best to keep a record of all access requests, and indicate whether the request was granted or rejected. This will help you in the event of a dispute. As part of your organisation's documentation process, you may also wish to consider using an acknowledgement form.

Acknowledgement Of Personal Data Received For An Access Request

Reference Number: .....

Name of Recipient: .....

Contact Details: .....

No.	Document/Material	Date Received

Signature of Recipient Date (DD/MM/YYYY)

For Internal Use Only

Staff of organisation handling access request:

.....

Date: ..... Time: .....

For more information, refer to Guide to Handling Access Request at www.pdpc.gov.sg/og

Allow Correction Of Personal Data

When an individual requests to correct an error or omission in his personal data, you must do so, unless an exception applies.

Sample Form for Correction Request

I) APPLICATION TO CORRECT PERSONAL DATA

1. Under the Personal Data Protection Act 2012 ("PDPA"), you are entitled to correct an error or omission in the personal data that we have.

2. Please complete this form and submit it to:
   <Please specify any other modes to submit a correction request below>
   In person or by post:
   Data Protection Officer, Organisation ABC,
   ABC Complex 123, ABC Road, Singapore 123456

   Alternatively, you can email the completed form to us: DPO@abc.com.sg

3. We will respond to your request for correction within 30 days. If we are unable to fulfil your correction request within 30 days after receiving the request, we will inform you in writing of the time in which we are able to fulfil the correction request.

4. Please note that the corrected personal data will be sent to the organisations to which the personal data was disclosed by us within one (1) year before the date the correction was made, unless they do not need it for any legal or business purpose. However, please let us know if you prefer or agree to send the corrected personal data only to specific organisations (not being a credit bureau), and we will send the corrected personal data only to those specific organisations.

5. Under Section 22(4) PDPA, we may not correct the personal data if we are satisfied on reasonable grounds that the correction should not be made.

II) PARTICULARS OF REQUESTOR

<For this section, please determine the types of information your organisation requires from the requestor in order to process the correction request such as proof of identity. If the requestor is initiating a correction request on behalf of another individual, please make clear the documentation required by your organisation to establish that the requestor is legally authorised to act on behalf of the other individual.>

Please check the applicable box(es):
☐ I am making a correction request for my own personal data

Name of requestor:
Contact number:
Email address:

Please furnish a copy of <for organisation to insert proof of identity accepted> for verification purposes.

☐ I am making a correction request on behalf of another individual

Name of the other individual whom you are making a correction request on behalf of:

Name of requestor:
Contact number:
Email address:

Please furnish a copy of <for organisation to insert proof of identity accepted> for verification purposes.

III) DESCRIPTION OF THE PERSONAL DATA TO CORRECT

To enable us to process your correction request quickly and efficiently, please
1) specify the personal data you wish to correct; and
2) provide us with any information that may enable us to locate the personal data to be corrected, including information obtained from your previous access request identifying the specific personal data, time and date of collection, and its location.

Secure The Personal Data Held By Your Organisation

Establish security arrangements to protect the personal data under your organisation. This is to prevent unauthorised access, collection, use or disclosure of the data and other similar risks.

HOW TO PROTECT YOUR ELECTRONIC DATA?

AT EMPLOYEE LEVEL

- Encrypt or password-protect any personal data held electronically that would cause harm if lost or stolen, such as in portable computing devices* and documents. This includes email attachments containing personal data. If sending to another party, communicate the password separately.
- Regularly back up information on computer systems and keep the backups in a separate location.
- Dispose properly documents containing personal data that are no longer needed. Use specialised software tools to erase personal data stored on hard disks or degauss hard disks.

*Portable computing devices include smartphones, tablets, laptops and portable hard disks.

AT ORGANISATION LEVEL

- Install firewalls and virus-checking software on employees' computers.
- Secure portable computing devices when not in use by locking them up or attaching them to a fixture by a security cable.
- Set computer screens to lock automatically when left unattended for a specified period.
- Restrict use of external devices on all company-issued computers to authorised persons only.
- Limit employee access to sensitive and confidential documents on a need-to-know basis.
- Use privacy filters, careful positioning of your computers and other means to prevent unauthorised persons from viewing your computer screens.
- Secure websites and applications (apps). Files containing personal data should not be made available online.
- Check that your appointed software developers keep pace with ICT security threats, and are able to design and maintain ICT systems with the capacity to protect stored personal data.

For more information on how to protect electronic personal data refer to Guide to Securing Personal Data in Electronic Medium at www.pdpc.gov.sg/og.

Sample Personal Data Breach Report Form

Data breaches can happen despite all the precautions that you may take, for various reasons. If it does, start by capturing full information about the data breach before proceeding with an investigation.

The sample form below shows what information you could capture about the data breach.

PERSONAL DATA BREACH REPORT FORM

Organisation *(including name of subsidiary, if applicable)*:

Data intermediary *(if applicable)*:

Date of Breach: **Time of breach discovery:**

Location of breach:

Types of personal data involved:

Key description of incident:

Number of affected individuals:

Remedial actions taken:

Staff in charge of post-breach remedial actions:

Time of record:

Regulatory authority notified:

Other supporting documents:

Dispose Of Personal Data That Is No Longer Needed

Stop holding on to personal data when you no longer have any business or legal use for it.

This means that you should:

1. Set a retention period for various types of personal data

Categorise the personal data and decide how long it should be retained. Keep personal data only as long as there is a business or legal purpose.

2. Safely dispose of personal data when you no longer need them

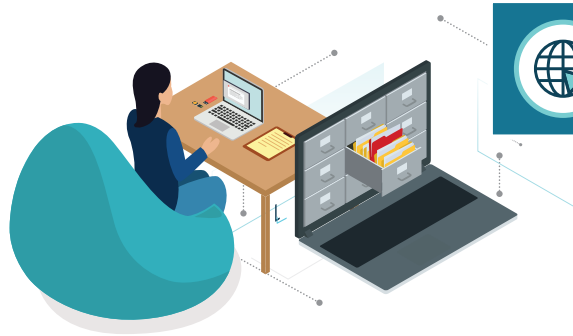
1 For paper such as documents and photos

Shred, pulp or incinerate them.

2 For electronic media

USB sticks and hard disks/SSDs:
Use specialised software to overwrite selected files or entire medium.

Write-once or read-only CDs, DVDs and other media that do not support overwriting:
Crush, drill, shred or otherwise physically destroy the medium.



For more information, refer to Guide to Disposal of Personal Data on Physical Medium at www.pdpc.gov.sg/og

Ensure Protection Of Personal Data When Transferring Overseas

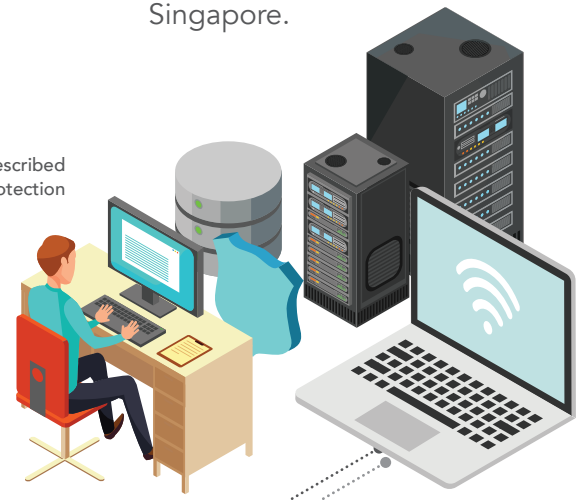
If your organisation intends to transfer personal data overseas, do take steps to ensure that the data protected in compliance with the PDPA while the personal data is still in your possession or control.

Should the transfer be to another organisation overseas, you must also ensure that the receiving organisation is bound by legally enforceable obligations to provide protection comparable to the standard under the PDPA. Such legally enforceable obligations may be imposed by law or by entering into a contract* with the recipient.

Alternatively, personal data may be transferred overseas to another organisation if it falls within other prescribed circumstances, such as if:

- the individual has been informed of the level of protection that will be accorded to his/her personal data as compared to the PDPA and consents to the transfer of the personal data to that recipient in that country or territory;
- the transfer is necessary for the performance of a contract between the organisation and the individual; or
- the personal data is publicly available in Singapore.

* The contract has to satisfy the prescribed conditions found in the Personal Data Protection Regulations 2014.



Closely Manage Service Providers That Handle Personal Data

If you engage a service provider to process personal data (this includes hosting, storing or processing the data), you may be held responsible if your service provider contravenes the PDPA while providing the service to you.

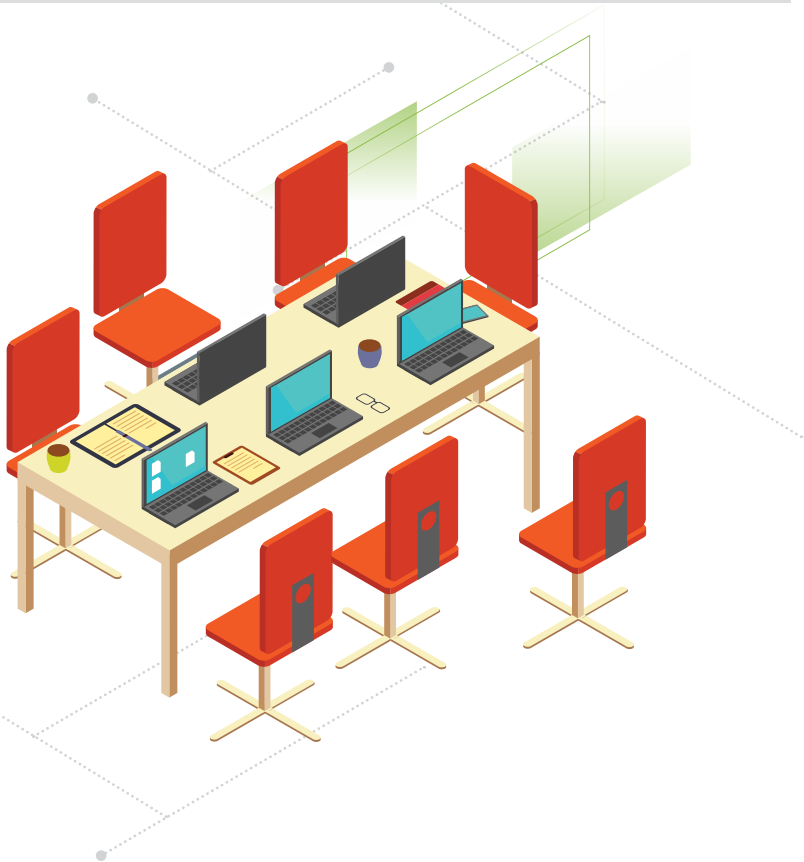
When entering into a service agreement with your service provider, ensure there are clauses that require them to take sufficient measures to ensure compliance with PDPA requirements.

Contracts alone are not the end of your organisation's accountability. You should also establish relevant standard operating procedures (SOPs) for your service provider on the processing of personal data, and include measures to monitor its compliance with these SOPs.

For more information on the sample data protection clauses that you may wish to include in your service agreements, refer to the Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data at www.pdpc.gov.sg/og.

Check The Do Not Call Registry

If you conduct telemarketing to subscribers or users of Singapore telephone numbers, you will need to submit the telephone numbers on your telemarketing list for checks against the Do Not Call (DNC) Registry, unless the subscriber or user has given his/her clear and unambiguous consent to receive such messages.



To check the DNC Registry:

Create an Account

Apply for a main account on the DNC Registry website using your CorpPass account. Each organisation or individual is allowed one main account. Each main account gets 1,000 free credits every year, valid for one year from date of issue.

Check the Registry

Telephone numbers submitted will be checked against all 3 DNC registers for voice calls, texts and faxes. There will be a charge for each number submitted for checking, regardless of whether the number has been submitted before.

Receive the results

You receive results for Small Number Lookup of telephone numbers (10 or less numbers at one time) immediately. For a bigger list, use Bulk Filtering. You will receive the results in less than 24 hours. All results are valid up to 30 days. Thereafter, you will need to re-check the DNC Registry.

For more information on the DNC Registry, please refer to www.dnc.gov.sg.

Communicate Your Data Protection Policies, Practices And Processes

For your Customers:

- Provide the business contact information of your DPO so that your customers can contact him/her for PDPA-related queries or complaints.

- Readily provide information about your data protection policies, practices and complaint process upon request.

For your Employees:

Communication

- Inform all employees of your data protection policies and practices. Make sure they know and adhere to your processes for protecting personal data. Emphasise their roles in safeguarding personal data and ensuring that the organisation complies with the PDPA.

- Use posters, email and other communication tools to raise awareness of the importance of personal data protection among your staff.

Training

Send your employees for training

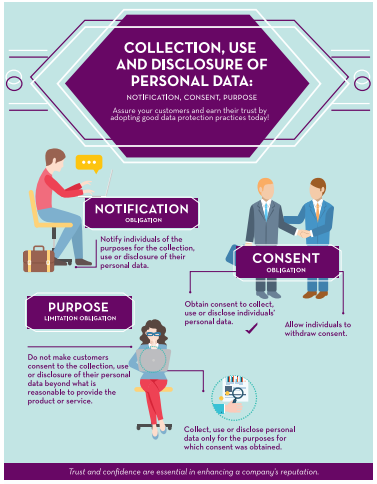
- Sign them up for the free PDPA e-Learning Programme offered on the PDPC website at www.pdpc.gov.sg/e-learning.

- Send key employees who handle personal data to attend a subsidised two-day course, "Fundamentals of the PDPA". SMEs can enjoy up to 90% course subsidy while non-SMEs and self-sponsored individuals enjoy up to 50% course subsidy.

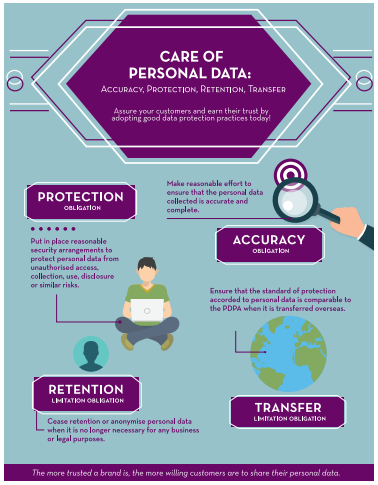
For more information, please refer to www.pdpc.gov.sg/org-resources.

Samples of posters to raise awareness of the importance of data protection among employees

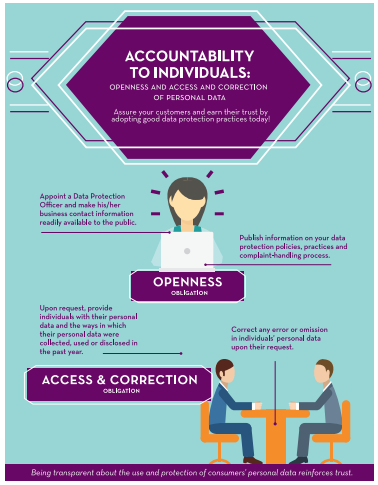
PDPA Obligations Poster 1 - Collection, Use and Disclosure



PDPA Obligations Poster 2 - Care of Personal Data



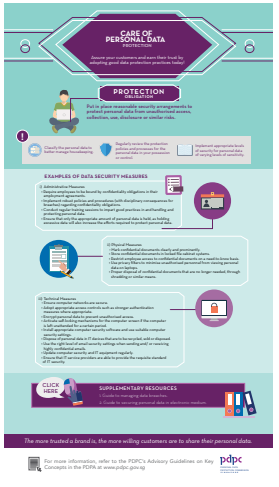
PDPA Obligations Poster 3 - Accountability to Individuals



To download the sample posters, refer to www.pdpc.gov.sg/org-resources

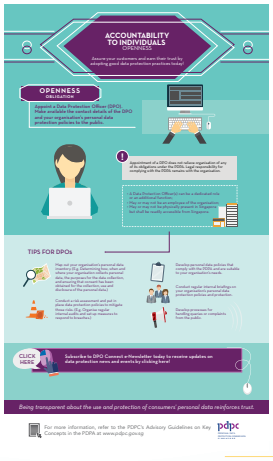
eDM 1 - Notification, Consent and Purpose

eDM 2 - Protection

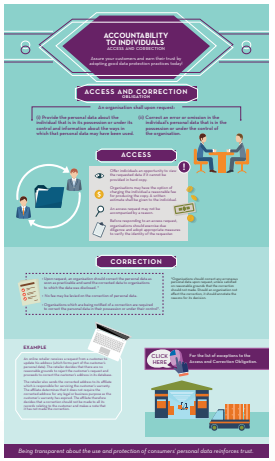


eDM 3 - Accuracy, Retention and Transfer

eDM 4 - Openness



eDM 5 - Access and Correction



Help For Organisations

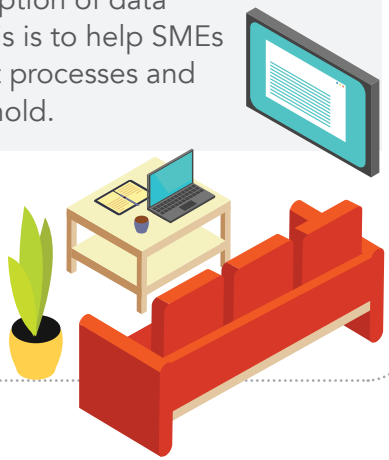
1 Guidance

PDPC provides guidance to organisations to help them reduce any uncertainty they may face in complying with specific obligations under the PDPA and its regulations in the context of its particular situation. It does not advise, recommend or confirm that an organisation should or should not adopt any particular course of action.

You may refer to the Conditions of Guidance and submit your request at www.pdpc.gov.sg/guidance.

2 Capability Development Grant

Organisations can tap on SPRING Singapore's Capability Development Grant (CDG) to defray up to 70 per cent of qualifying project costs such as consultancy and training, assessments and audits, and adoption of data protection software solutions. This is to help SMEs develop good data management processes and systems to secure the data they hold.



You may find out more at www.pdpc.gov.sg/help.

3 DP Advisory

Innovative and responsible use of data can provide competitive advantage by enabling new service offerings, as well as increase consumer confidence in an organisation. To help SMEs in Singapore use data responsibly, the PDPC has appointed a panel of DP Advisors to provide tailored support and assistance.

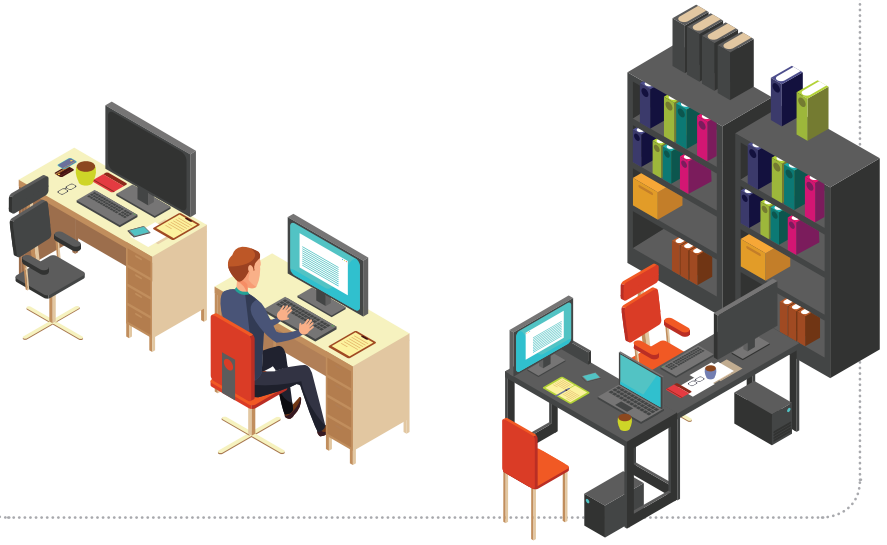
Basic Advisory Session (1 hour)

- Learn about your data protection obligations
- Uncover potential data protection gaps in your business processes
- Locate useful data protection resources
- Find out more about financial assistance schemes available

Step-up Advisory Session (2 hour)

- Receive in-depth, targeted advice tailored to your organisation's key business processes

You may register your interest at www.pdpc.gov.sg/dp-advisory.



4 List Of Professional Data Protection Service Providers

Visit www.pdpc.gov.sg/dp-services for a directory of data protection service providers.

The website lists the following professional service providers that may be helpful to you:

- Data protection solutions
- Data protection consulting service providers
- Legal advisors
- Outsourced DPO functions service providers
- Data protection training providers

This directory is meant to be a basic reference to the data protection services that are available in Singapore. This is to promote greater access to organisations or individuals seeking to obtain such services in Singapore.

Useful Resources For Organisations

PDPC Website

Download free educational videos, FAQs, factsheets, advisory guidelines, guides and templates from the PDPC website at www.pdpc.gov.sg/org-resources. These self-help resources are updated from time to time. The website contains:

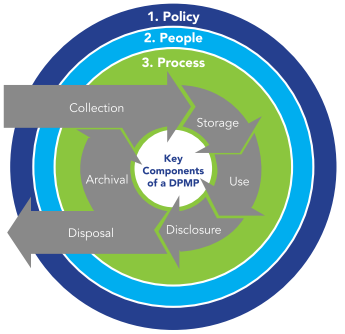
- Advisory guidelines
- Assessment Tool
- Brochures and leaflets
- Factsheets
- Education and training materials
- e-Newsletters
- Posters and e-direct mailers
- Publications
- Sample clauses
- Videos

TOWARDS ACCOUNTABILITY

A Data Protection Management Programme (DPMP) lays the foundation and provides a systematic approach for an organisation's data protection initiatives. It covers **management policies** and **processes** for the handling of personal data as well as defines governance and the roles and responsibilities of the **people** in the organisation in relation to personal data protection.

How to develop a DPMP?

There is no 'one size fits all' DPMP, and organisations should consider developing a DPMP that is reasonable and appropriate for their business need. Nevertheless, organisations may wish to follow the suggested steps below.



ESTABLISH A DATA PROTECTION POLICY

A personal data protection policy sets the direction and course of action by the organisation to meet its obligations under the PDPA.

DEFINE DATA PROTECTION ROLES, RESPONSIBILITIES OF PEOPLE

People are the backbone behind all measures and their roles and responsibilities in personal data protection should be defined and understood throughout the organisation.

IMPLEMENT PROCESSES ESTABLISHED IN POLICIES

Organisations may need to create, update or revise their processes to address the handling of personal data throughout the data lifecycle (from collection to disposal/archival).

For more information about DPMP, please visit www.pdpc.gov.sg/og.

Note

Note

This publication provides a general guide to basic data protection steps or considerations to get an organisation started on its data protection journey. The contents herein are not an authoritative statement of the law or a substitute for legal or other professional advice. The PDPC and its members, officers, employees and delegates shall not be responsible for any inaccuracy, error or omission in this publication or liable for any damage or loss of any kind as a result of any use of or reliance on this publication.