pdpc
PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

GUIDE TO DEVELOPING A DATA PROTECTION MANAGEMENT PROGRAMME

Published 1 November 2017

Revised 15 July 2019

TABLE OF CONTENTS

PART 1: INTRODUCTION

Organisations that collect, use and disclose personal data are required to develop and implement policies and practices that are necessary for the organisation to comply with the Personal Data Protection Act 2012 (PDPA). This guide seeks to help organisations develop or improve their personal data protection policies and practices through the implementation of a Data Protection Management Programme (DPMP)[1]. Organisations may benchmark their existing personal data protection policies and practices against this guide. Ultimately, organisations should tailor their personal data protection policies and practices to their organisational needs.

1.1 What is a DPMP?

A DPMP is a systematic framework to help organisations establish a robust data protection infrastructure. It covers management **policies** and **processes** for the handling of personal data as well as defines roles and responsibilities of the **people** in the organisation in relation to personal data protection. Having an established DPMP helps an organisation to demonstrate accountability in data protection. This provides confidence to stakeholders and fosters high-trust relationships with customers and business partners.

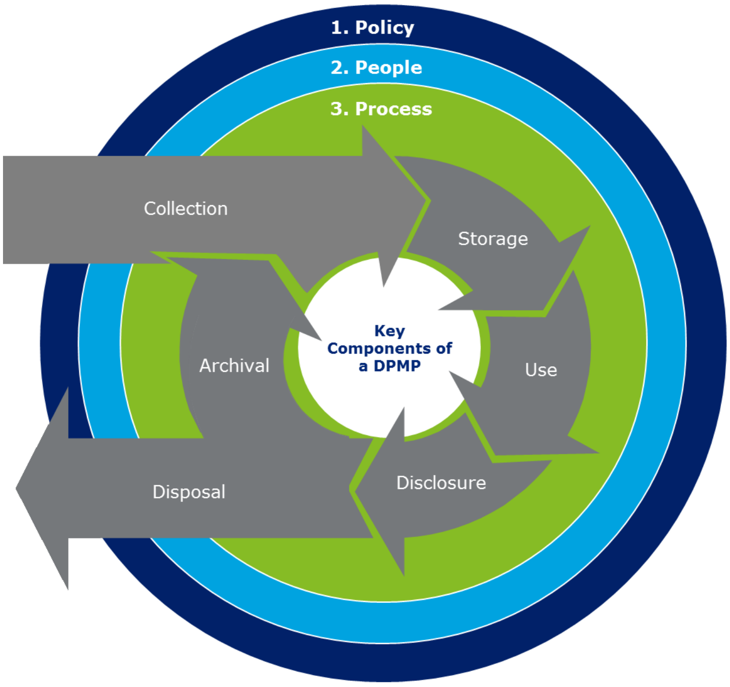


Illustration of a DPMP (Policy, People, Process),
with a Data Lifecycle (From Collection to Archival/Disposal)

[1] Organisations should note that adopting the suggestions in this guide does not mean that it would be in compliance with the PDPA. An organisation should consider whether the suggestions in this guide could be adapted for its specific circumstances.

1.2 How to develop a DPMP?

Organisations may follow the suggested steps below when developing their DPMP.

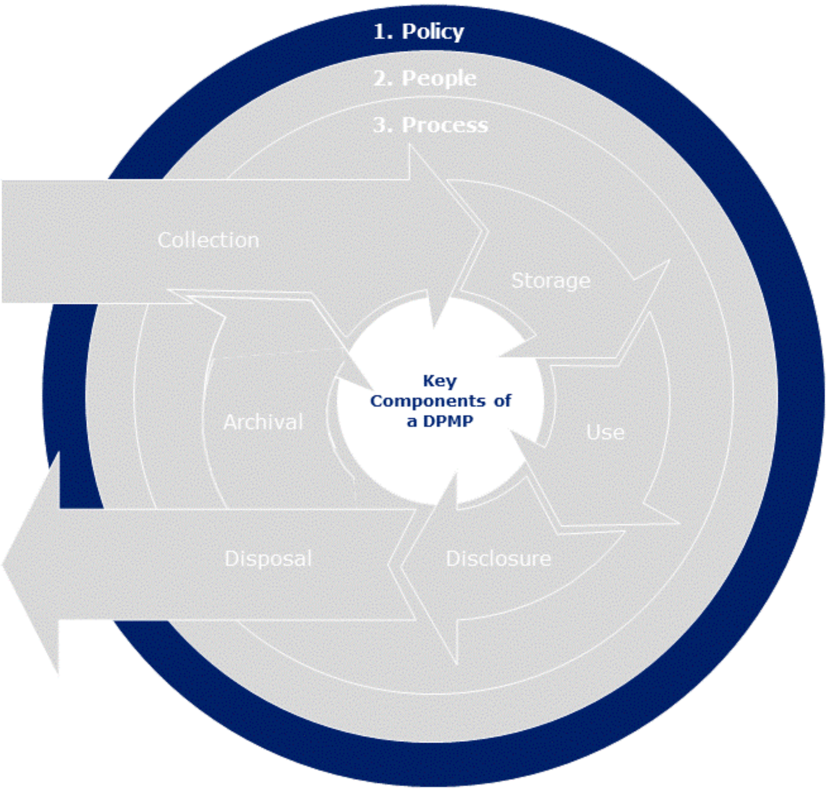
Steps	Description	Details
1. **Develop a data protection policy as part of coporate governance**	A **coporate governance and policies** set the direction and course of action by the organisation to meet its obligations under the PDPA.	Part 2 contains guidance on developing a Personal Data Protection policy as part of the organisation's coporate governance.
2. **Designate data protection roles and responsibilities of the 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.	Part 3 covers suggested roles, responsibilities, training and communication initiatives.
3. **Design processes to operationalise policies**	Organisations need to ***create or revise processes*** to operationalise their data protection policies	Part 4 presents processes and good practices to operationalise the Personal Data Protection policy.
4. **Detail ways to stay relevant**	Organisations need to develop ways to **monitor and maintain** the relevancy of their data protection related policies, processes and people.	Part 5 provides guidance on keeping data protection practices relevant.

1.3 Available resources

Organisations can refer to the resources at the end of each part to guide the development of their DPMP. As a start, please refer to the introductory resources provided to help organisations better understand the requirements and obligations or the PDPA.

No.	Resource
1	An Introduction to the Personal Data Protection Act in Singapore
2	Do Not Call Registry for Organisations
3	Your Personal Data, Our Responsibility
4	保护个人资料，人人有责 (Mandarin version)

PART 2: POLICY



2.1 Corporate governance and policies

Organisations should consider including personal data protection policies into its corporate governance policies. This will enable organisations to leverage on their corporate governance structures to monitor and manage personal data protection issues. For example, a corporate risk management framework that incorporates personal data protection matters would aid organisations in monitoring and managing data protection risks.

The involvement and support of an organisation's leadership is important in demonstrating commitment to personal data protection. The Senior Management of an organisation provides leadership via its various responsibilities, such as:

- Appointing and empowering the Data Protection Officer (DPO)
- Approving the organisation's Data Protection policies and Data Protection Management Programme (DPMP)
- Monitoring and managing personal data protection risks as part of corporate governance (e.g. corporate risk management framework), and where relevant, reporting to the Board which typically oversees risk governance
- Commissioning Data Protection Impact Assessments (DPIA)

- Advocating data protection training
- Allocating resources (e.g. budget, manpower) to data protection
- Providing strategic guidance on the implementation of data protection initiatives
- Providing direction to DPO for the handling of major complaints and managing data breaches, including implementation of remediation plans
- Providing direction to DPO for communication and liaison with the Personal Data Protection Commission (PDPC)

2.2 Why is it important to develop a personal data protection policy?

As part of its corporate governance structure, organisations should develop and communicate a personal data protection policy for both its **internal** stakeholders (e.g. staff) and **external** parties (e.g. customers). This will provide clarity to internal stakeholders on the responsibilities and processes on handling personal data in their day-to-day work. Policies also demonstrate accountability to external parties by informing them on the ways in which the organisation handles personal data.

2.3 What should be in a policy?

Organisations may consider some general questions in the following table to develop their policies to suit their business or organisational needs.

Questions	Applicable to	
	Internal	External
General		
1. What is the definition of personal data?	√	√
2. What is the purpose of the policy?	√	√
3. How often is this policy reviewed?	√	
People		
4. Who are the intended audience of the policy?	√	√
5. Who does the policy apply to? Are their roles and responsibilities clear and comprehensive?	√	√
6. Who is the policy owner?	√	
7. Who approves the policy?	√	

Questions	Applicable to	
	Internal	External
Process		
8. Whose personal data is handled?	√	√
9. What is the purpose for collecting the personal data?	√	√
10. What types of personal data is handled (e.g. name, NRIC, birth date, health details)?	√	√
11. How are queries, feedback, disputes and requests handled?	√	√
12. Which are the third party organisations personal data is shared with, if any?	√	√
13. How does the organisation ensure that third party service vendors protect data in accordance with the PDPA requirements?	√	√
14. How are the data protection and Do-Not-Call provisions of the PDPA complied with throughout the data lifecycle?[2]	√	√
15. How is the personal data protected?	√	
16. How should data incidents[3] and data breaches be handled?	√	
17. When are Data Protection Impact Assessments (DPIA) conducted, and on which systems or processes?	√	
18. How should policy exceptions be handled?	√	

Organisations should also consider having dedicated internal policies on specific areas that require elaboration. For example, the table below lists some of the considerations on handling access requests:

Example: Considerations on developing policy on handling Access Request

Organisation ABC wishes to establish an internal policy on handling access requests and considers the following points when developing the policy -

Establishing and making access request channels available

- How ABC intends to receive all access requests[4]

[2] This segment may be expanded to elaborate on how the organisation complies with the PDPA.

[3] Data incidents refer to a potential, but unconfirmed, breach of the Protection Obligation under the PDPA.

[4] Under PDP Regulation 3(1), A request to an organisation must be made in writing and shall include sufficient detail to enable the organisation, with a reasonable effort, to identify (a) the applicant making the request; (b) in relation to a request under section 21(1) of the Act, the personal data and use and disclosure information requested by the applicant; and (c) in relation to a request under section 22 of the Act, the correction requested by the applicant. (2) A request must be sent to the organisation – (a) in accordance with section 48A of the Interpretation Act (Cap.1); (b) by sending it to the organisation's data protection officer in accordance with the business contact information provided under section 11(5) of the Act; or (c) in such other manner as is acceptable to the organisation.

(e.g. is there a standard access request form that the applicant may use, or in the absence of any access request forms provided by the organisation, what information is required from the applicant for ABC to proceed with the access request?)

- What are the channels for the applicant to submit the access request?
  (e.g. via email, post or any other avenue specified by the organisation)

Obtaining specific information

- What specific information would ABC require to search for and locate the requested personal data in a timely manner (e.g. type of personal data requested, data and time the personal data was collected)?

Charging access fees

- Would ABC be charging a fee[5] to process the access request and are the fees provided in writing to the applicant[6]?
- If ABC intends to charge a fee for the access request that is higher than originally estimated, how would the ABC communicate the higher fees in writing to the applicant?
- How would ABC compute the access fee[7] in a way that accurately reflects the time and effort required to respond to the access request?

Determining response timeframe

- How long would ABC take to provide access to the requested personal data[8] and how would the individual be informed if ABC is unable to provide access within 30 days?

Ascertaining identity

- What procedures are established by ABC to verify the identity of the individual making the request (e.g. proof of identity required from the applicant, verification questions to be asked to establish the identity of the requestor)?
- What procedures are established by ABC to verify the identity of an individual making an access request on behalf of another individual, and what forms of proof of identity are required?

[5] Under PDP Regulation 7(1) Subject to section 28 of the Act, an organisation may charge an applicant who makes a request to it under section 21(1) of the Act a reasonable fee for services provided to the applicant to enable the organisation to respond to the applicant's request. (2) An organisation must not charge a fee to respond to the applicant's request under section 21(1) of the Act unless the organisation has – (a) provided the applicant with a written estimate of the fee; and (b) if the organisation wishes to charge a fee that is higher than the written estimate provided under sub-paragraph (a), notified the applicant in writing of the higher fee. Organisations may charge the individual a reasonable fee to recover any incremental costs of responding to his access request. However, under the PDPA, on application of a complainant, the Commission may review a fee required from the complainant by an organisation in relation to a request by the complainant under section 21 or 22. Upon completion of the review, the Commission may confirm, reduce or disallow a fee, or direct the organisation to make a refund to the complainant.

[6] Organisations may refuse to provide access to the personal data requested until the individual agrees to pay the relevant fee.

[7] The PDPA does not prescribe a standard fee or range of fees applicable to access request.

[8] Organisations must provide access to the requested personal data as soon as reasonably possible.

Assessing exceptions and prohibitions

- When processing an access request, ABC should also assess the prohibitions or exceptions that may apply such that access to personal data cannot be provided[9].

Keeping records of access requests

- What is ABC's documentation process for recording all access requests received and processed? Documentation may also include all access requests received but not processed due to an applicable exception[10].
- What is ABC's retention policy for keeping records of access requests received?

These are some details that an organisation developing a specific policy should consider and are not meant to be exhaustive. For more information on handling access requests, please refer to the PDPC's Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 15) and Guide to Handling Access Requests.

Policies should be approved by the management, communicated to all relevant parties and reviewed regularly to ensure they remain relevant. Organisations may also use the PDPC's Data Protection Notice Generator to generate basic data protection template notices to inform their stakeholders on how they manage personal data.

After developing the relevant policies, an organisation would need to implement them. Chapter 4 of this guide provides guidance for operationalising data protection policies.

2.4 Available resources

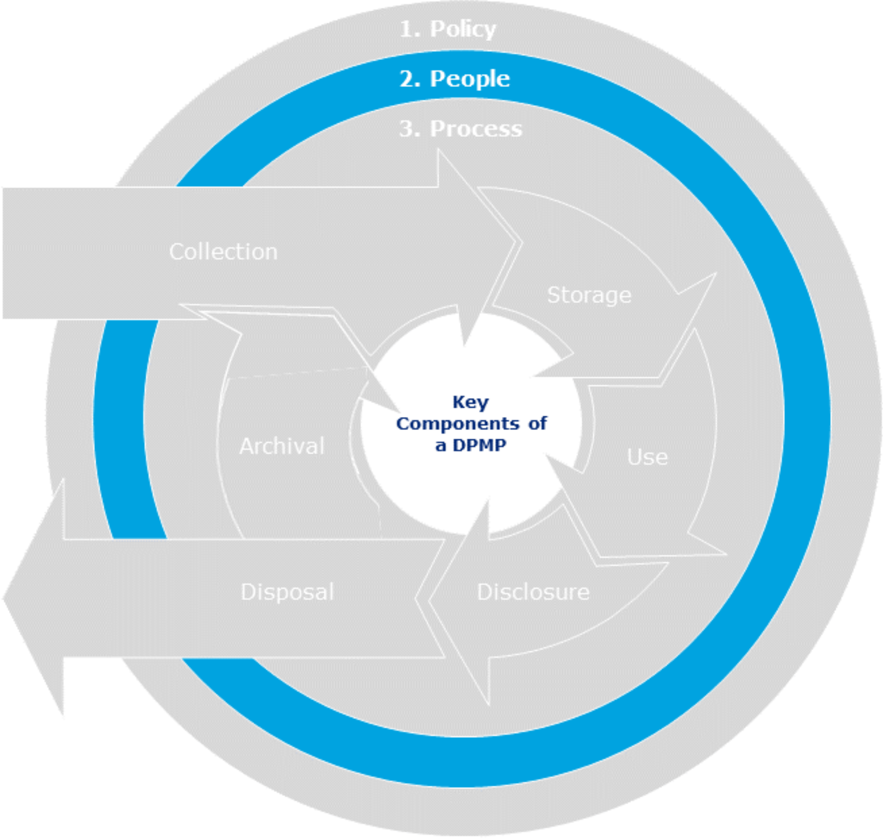
Please refer to the templates below for more information.

No.	Resource
1	Guide to Handling Access Requests
2	Data Protection Notice Generator

[9] Please refer to section 21 of the PDPA, Part II of the Personal Data Protection Regulations 2014 and Advisory Guidelines on Key Concepts in the PDPA for more information on exceptions and prohibitions under the Access Obligation.

[10] For more information, please refer to Chapter 15 of the Advisory Guidelines on Key Concepts in the PDPA.

PART 3: PEOPLE



3.1 What is the Senior Management's role in data protection?

As illustrated in the previous chapter, the Senior Management of an organisation is responsible for the organisation's approach to handling personal data through their corporate goverance, policies and communication throughout the organisation.

3.2 The Data Protection Officer (DPO)

It is mandatory for organisations to designate at least one individual to be the Data Protection Officer (DPO) responsible for ensuring that the organisation complies with the PDPA. Having an established DPMP would help the DPO meet the following key responsibilities:

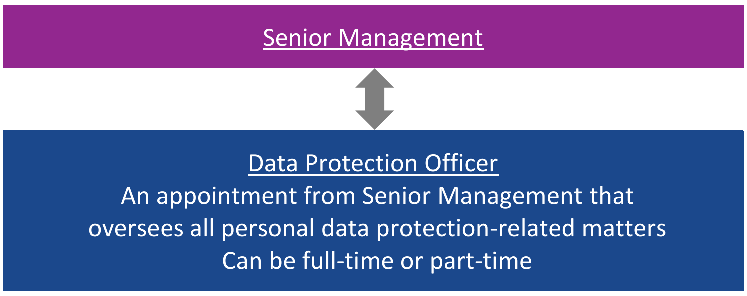
- Ensuring compliance with the PDPA through data protection policies and processes;
- Fostering a personal data protection culture and communicating personal data protection policies to stakeholders;
- Handling access and correction requests to personal data;
- Managing personal data protection-related queries and complaints;
- Alerting management to any risks that might arise with regard to the personal data handled by the organisation; and
- Liaising with the PDPC on personal data protection matters, if necessary.

DPOs are also strongly encouraged to attend the Fundamentals of the Personal Data Protection Act (PDPA).

3.2.1 How should the DPO be appointed?

Given the significant contribution of a DPO and the seniority required to lead data protection initiatives, a DPO should ideally be an appointment from senior management. Their responsibilities can be taken on by one employee, a group of employees, or outsourced. When outsourcing the DPO function, the organisation should still ensure that an individual appointed from senior management remains responsible to work with the outsourced DPO. The following diagrams are examples of how a DPO may be structured in an organisation.

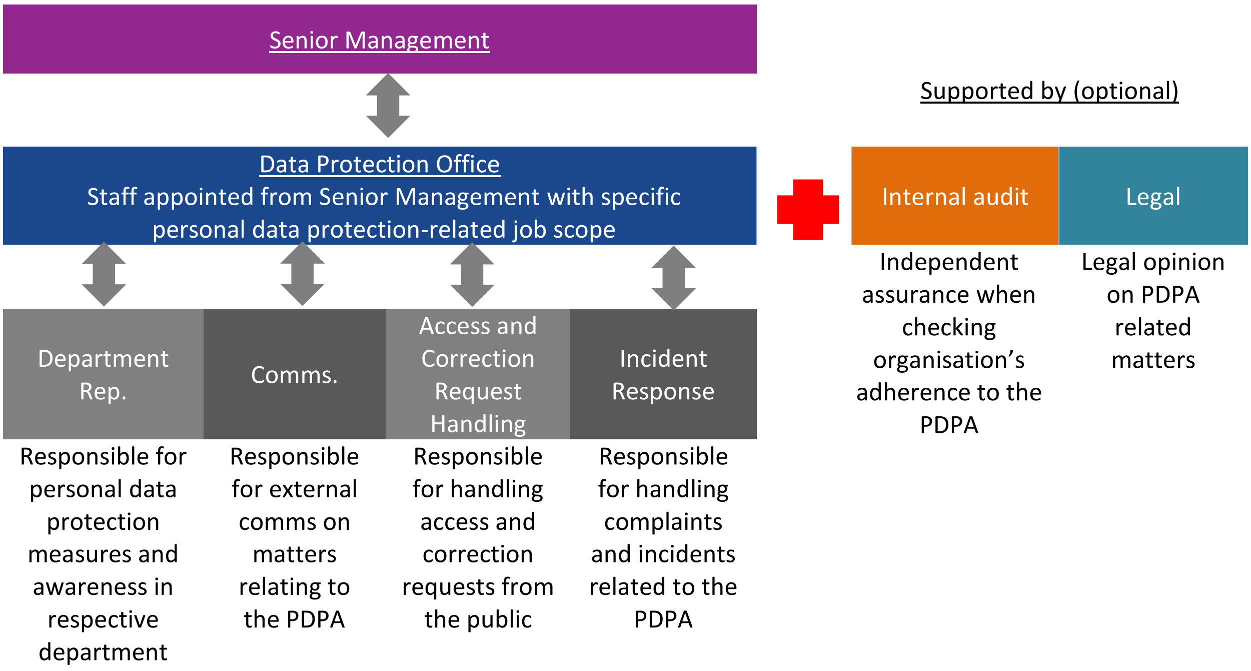
A. One staff appointed as the DPO



Senior Management

Data Protection Officer
An appointment from Senior Management that oversees all personal data protection-related matters
Can be full-time or part-time

B. Multiple staff appointed (with support from the audit and legal department)



Senior Management

Data Protection Office
Staff appointed from Senior Management with specific personal data protection-related job scope

Department Rep.
Responsible for personal data protection measures and awareness in respective department

Comms.
Responsible for external comms on matters relating to the PDPA

Access and Correction Request Handling
Responsible for handling access and correction requests from the public

Incident Response
Responsible for handling complaints and incidents related to the PDPA

Supported by (optional)

Internal audit
Independent assurance when checking organisation's adherence to the PDPA

Legal
Legal opinion on PDPA related matters

3.3 Does staff other than the DPO and Senior Management have any roles and responsibilities in protecting personal data?

Personal data protection cuts across roles, functions and hierarchy in the organisation; it should be recognised and practiced by all levels in the organisation (including volunteers, agents and contract staff) and not limited to the appointed data protection representatives.

In particular, staff that handle personal data (e.g. sales), or are responsible for implementing personal data protection measures (e.g. IT), would need to be diligent in adhering to the organisation's data protection policies and processes.

In this regard, organisations should educate their staff on their personal data protection responsibilities. Regular circulars may be used to generate awareness and foster a culture of personal data protection. Refer to the end of this chapter for resources to raise awareness on personal data protection.

3.4 How about external parties?

Organisations typically deal with third party service vendors (e.g. outsourced printers, telemarketing providers) and customers as part of their business operations. Here are some considerations in dealing with these parties.

3.4.1 Service Vendors

Organisations are encouraged to communicate their personal data protection requirements to their service vendors as clearly as possible. When handling personal data of the organisation, your service vendors are responsible for adhering to the Protection and Retention Obligations under the PDPA. In this regard, a binding contractual agreement between the organisation and their service vendors that highlight the responsibilities of service vendors with regard to the processing of the personal data should be in place.

3.4.2 Customers (e.g. clients, donors, other organisations)

Customers' trust is paramount and organisations should implement personal data protection initiatives to demonstrate accountability. Useful initiatives include:

- Increasing customers' awareness about the organisation's personal data protection initiatives (e.g. making personal data protection policy available on website, providing the data protection policy promptly when requested by customers)

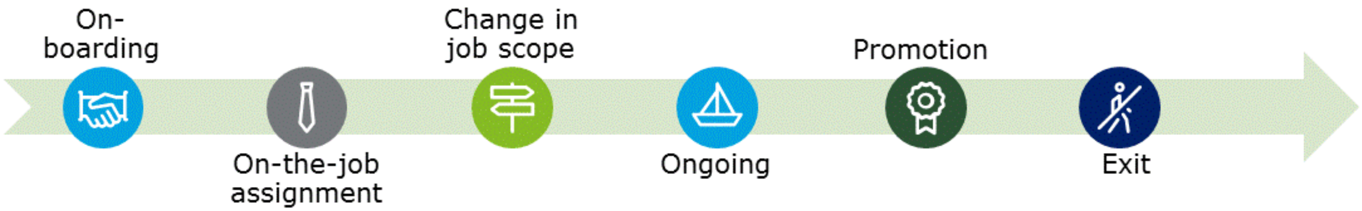
- Ensuring staff is able to handle customers' personal data protection related requests (e.g. consent withdrawal requests, access and correction requests)
- Providing regular updates on key developments in the organisation's personal data protection policies (e.g. through e-newsletters to customers)
- Be open to feedback from customers on the handling of personal data. If your customers are organisations and you process personal data on behalf of them, you may wish to actively engage these organisations and seek clarity on dealing with the type of personal data and its security requirements, especially those that are potentially sensitive in nature (e.g. health and financial information).

Such approaches may help to assure customers that your organisation takes responsibility over the personal data under your care.

3.5 What should organisations do to make stakeholders aware of their roles and responsibilities?

Organisations may wish to consider adopting practical ways to share personal data protection measures and embed personal data protection-related topics into their staff training and communication plan. A snapshot of the various initiatives, and the phases at which they may be conducted throughout a typical employment journey, is illustrated below. Organisations may also use the resources at the end of this chapter.

Employment Journey



Training (Illustrative)	• Briefing on the fundamentals of the PDPA	• In-depth training on organisation's data protection processes	• In-depth training on specific data protection process, if any	• Refresher on the fundamentals of the PDPA • Briefings on specific data protection policies and processes	• In-depth training on specific data protection process, if any	• Requirements on proper handling of personal data upon exit (e.g. not misusing personal data handled)
Communication (Illustrative)	• Access to an internal repository on data protection matters (e.g. policies)			• Reminders on data protection policies and processes • Update on any changes to data protection policy or processes		
Target Audience (Illustrative)	• All staff	• Staff handling personal data (e.g. HR, Sales and Marketing)		• All staff	• Staff with greater responsibility over personal data protection	• Staff who are leaving the organisation

3.5.1 What are the different types of trainings for different groups of stakeholders?

DPOs can refer to the suggested training types in the table below to develop their training and communication initiatives.

No	Type	Timing	Target	Details	How
	Board of directors support	• At the start of the organisation's personal data protection journey • Periodically, when corporate risk register[11] is reviewed	• Board of Directors	• Awareness and support of personal data protection risks • Inclusion of personal data protection risks into corporate risk management framework	• PDPC events (e.g. Seminar, Briefings) • Briefings to Board of Directors by external vendors
1	Senior management buy-in	• At the start of the organisation's personal data protection journey • Periodically (e.g. during formulation of annual internal audit plans)	• Senior Management	• Rationalise business benefits of personal data protection • Highlight importance of personal data protection and implication of data breaches • Highlight the key roles of senior management in personal data protection • Establish risk reporting structure to identify and manage risk • Implement internal audits to evaluate effectiveness	• PDPC events (e.g. Seminar, Briefings) • PDPC's E-learning module • PDPC's sectoral briefings • Training by external vendors • DP Advisory Sessions
2	PDPA Training	• On-boarding of staff • Ad-hoc when there is a revision to the PDPA, PDPC guidelines or organisation's data	• All staff	• Educate staff on the PDPA and the organisation's data protection policies and processes • Make available data protection training materials in an accessible platform (e.g. intranet) • Suggested topics include:	• PDPC's E-learning module • In-house trainings or briefings by DPO on data protection policies and practices • Training by external vendors • Electronic direct mailers (eDMs), posters, videos,

[11] A risk register is a tool for documenting risks, and actions to manage each risk. It provides an organisation with a list of identified risk to assist in risk management.

No	Type	Timing	Target	Details	How
		protection policies and practices		A. Importance of Personal Data Protection B. Main obligations under the PDPA C. The organisation's personal data protection policies and processes	organisation's intranet, circulars to inform and update staff on organisation's new or revised data protection policies and practices
3	In-depth PDPA training specific to internal policies and processes	• Upon assignment to a specific job role or change in role/job scope • When there are new data protection policies or processes	• Staff handling personal data	• Develop targeted data protection training aligned with organisation's internal policies and processes	• PDPC sectoral briefings • An Introduction to the Fundamentals of Personal Data Protection Act (under the Business Management WSQ) • Training by external vendors
4	Refresher courses	• On a periodic basis (e.g. annually) • Ad-hoc when there is a revision to the PDPA, PDPC guidelines or organisation's data protection policies and processes	• All Staff	• Provide a refresher course for all employees to refresh their knowledge and facilitate compliance to the PDPA • Circulate updated materials on personal data protection	• Remind or update stakeholders on organisation's data protection practices and policies through: newsletters, electronic direct mailers (eDMs), posters, videos, organisation's intranet, circulars, roadshows, town hall or brownbag discussions. • PDPC events (e.g. seminars, briefings)
5	Obtain professional certification	• As part of career development	• The DPO and staff who are part of the DPO team	• Attend personal data protection related trainings to be updated of the regulations and requirements • Obtain personal data protection certification	• Certified Information Privacy Manager Programme • Certified Information Privacy Technologist Programme • Certified Information Privacy Professional Asia Programme

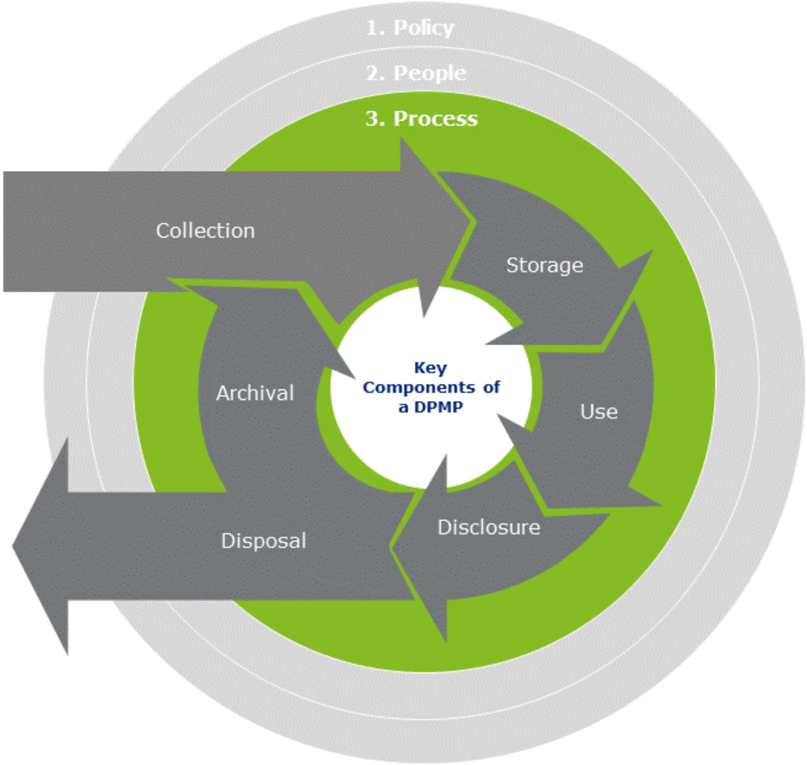
Please refer to the PDPC's website for more information on help for organisation.

3.6 Available resources

Please refer to the resources below for more information.

No.	Resource
1	An Introduction to the Fundamentals of the Personal Data Protection Act
2	Appoint a Data Protection Officer
3	eDM 1 - Notification, Consent and Purpose
4	eDM 2 - Protection
5	eDM 3 - Accuracy, Retention and Transfer
6	eDM 4 - Openness
7	eDM 5 - Access and Correction
8	PDPA Obligations Poster 1 - Collection, Use and Disclosure
9	PDPA Obligations Poster 2 - Care of Personal Data
10	PDPA Obligations Poster 3 - Accountability to Individuals
11	PDPA Obligations Poster 4 - General

PART 4: PROCESS



4.1 An overview

Organisations may consider these steps to apply data protection policies throughout the data lifecycle (from collecting personal data to archiving/disposing personal data) and across their business processes, systems, products or services -

What	How
1. Document personal data flows in your organisation to understand how personal data is being collected, stored, used, disclosed, archived/disposed	• Use a data inventory map or data flow diagram • Create a consent registry
2. Adopt accountability tools to identify key gaps and areas for improvement with respect to data protection	• Identify gaps using the PDPC's PDPA Assessment Tool for Organisations (PATO) • Use the relevant tools to address gaps after identifying them • Refer to relevant Advisory Guidelines and Guides published by the PDPC, as well as industry best practices
3. Incorporate data protection good practices into business processes, systems, products or services	• Adopt a Data Protection by Design approach, including conducting Data Protection Impact Assessments (DPIA) for

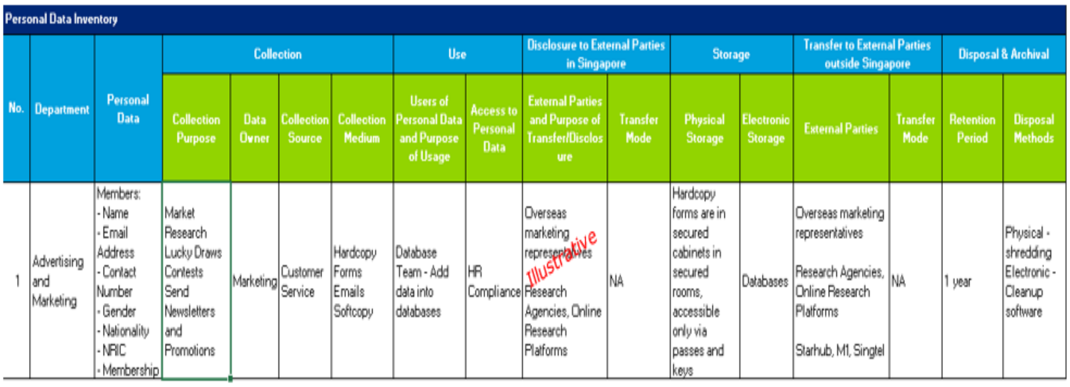
	systems or processes that are new or undergoing major changes • Ensure compliance to the PDPA and the organisation's data protection policies ○ Use contractual clauses ○ Conduct checks on compliance to clauses • Establish a process for data breaches by observing the PDPC's CARE framework and use an incident record log to document incidents and post-breach response
4. Establish risk monitoring and reporting structure	• Manage risk through an enterprise risk management framework with reporting mechanisms • Conduct internal audits to monitor and evaluate the implementation of data protection policies and processes

The following segments provide more details to guide organisations.

4.2 Document data flows in the organisation

To understand the lifecycle of personal data in your organisation and effectively identify the flows of personal data, organisations are encouraged to document the personal data handled using diagrams and charts such as **data inventory maps** or **data flow diagrams**, as illustrated below:

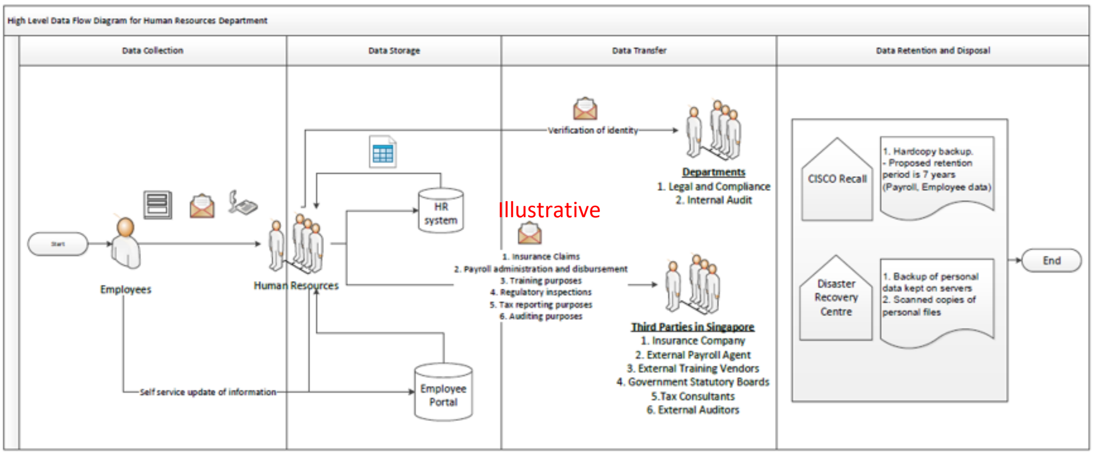
No.	Option
1	**Data Inventory Map**



Personal Data Inventory

No.	Department	Personal Data	Collection				Use		Disclosure to External Parties in Singapore		Storage		Transfer to External Parties outside Singapore		Disposal & Archival	
			Collection Purpose	Data Owner	Collection Source	Collection Medium	Users of Personal Data and Purpose of Usage	Access to Personal Data	External Parties and Purpose of Transfer/Disclosure	Transfer Mode	Physical Storage	Electronic Storage	External Parties	Transfer Mode	Retention Period	Disposal Methods
1	Advertising and Marketing	Members: - Name - Email Address - Contact Number - Gender - Nationality - NRIC - Membership	Market Research Lucky Draws Contests Send Newsletters and Promotions	Marketing	Customer Service	Hardcopy Forms Emails Softcopy	Database Team - Add data into databases	HR Compliance	Overseas marketing representatives Research Agencies, Online Research Platforms	NA	Hardcopy forms are in secured cabinets in secured rooms, accessible only via passes and keys	Databases	Overseas marketing representatives Research Agencies, Online Research Platforms Starhub, M1, Singtel	NA	1 year	Physical - shredding Electronic - Cleanup software

Pros	Cons
• Easy to develop, maintain and update • Does not require high level software and skills	• Lacks visual representation of data flow • Limited representation on interconnectivity of personal data

No.	Option	
	• No limitations on recording of information • Effective for extensive and complex data flows	
2	**Data Flow Diagram** 	
	Pros	**Cons**
	• Handy for quick reference • General flow of personal data can be easily understood • No technical knowledge is required to understand with simple notation • Effective for small, interconnected data	• Challenging to develop and maintain • Information to be presented is limited depending on size and/or type of personal data • Might not be effective for large, interconnected data

High Level Data Flow Diagram for Human Resources Department
Data Collection
Data Storage
Data Transfer
Data Retention and Disposal
Start
Employees
Human Resources
HR system
Employee Portal
Self service update of information
Verification of identity
Illustrative
Departments
1. Legal and Compliance
2. Internal Audit
1. Insurance Claims
2. Payroll administration and disbursement
3. Training purposes
4. Regulatory inspections
5. Tax reporting purposes
6. Auditing purposes
Third Parties in Singapore
1. Insurance Company
2. External Payroll Agent
3. External Training Vendors
4. Government Statutory Boards
5.Tax Consultants
6. External Auditors
CISCO Recall
1. Hardcopy backup.
- Proposed retention period is 7 years (Payroll, Employee data)
Disaster Recovery Centre
1. Backup of personal data kept on servers
2. Scanned copies of personal files
End

Please refer to the resources table at the end of this chapter for editable versions of the **data inventory map** and **data flow diagram.**

The **data inventory map** and **data flow diagram** should also include information on the business purposes for collection, use and disclosure of personal data, the individuals and third parties who handle personal data under the organisation's possession or control, as well as a classification of the data to manage user access. They should also deal with when and how the organisation should dispose of personal data or anonymised for long term archival. As good practice, it is important that employees and third parties access personal data on a need-to-know basis. Different sets of data may be accessed by different parties.

As good practice, organisations should also create a **consent registry** to record consent provided by individuals to the organisation for the collection, use and disclosure of their personal data for a particular purpose. This could be a document for the organisation to demonstrate and verify that an individual has provided consent, and for the organisation to have oversight of the consent provided, or withdrawn, by an individual. As an organisation updates its consent clauses, the consent registry can help to keep track of what is permitted for each version of the consent clause and the version of the consent clause that each customer has agreed to. Please refer to the resources table at the end of this chapter for an editable sample of a **consent registry**.

4.3 Adopt Accountability Tools

The PDPC has developed and actively promoted the adoption of accountability tools to assist organisations in demonstrating and practicing accountability. Some of the accountability tools are described below.

4.3.1 PDPA Assessment Tool for Organisations (PATO)

As a start, organisations may use the PATO to get a high level report on the implementation status of their data protection measures. This may be done prior to developing a DPMP as the results may guide the development of the DPMP, or any time when the organisation needs to have a sense of the possible areas for improvement. This would help to identify gaps and areas for improvement. Based on the assessment report, organisations would be able to ascertain how internal processes on handling personal data can be refined.

4.3.2 Use relevant resources to address gaps

While there are many resources available, organisations may refer to the following tools as a start.

Tool	Description
Developed by the PDPC	
Data Protection Starter Kit	The Data Protection Starter Kit contains useful information and resources such as sample forms, clauses and communication materials that organisations can adopt to kick-start the implementation of their data protection management programme.
Corporate e-Learning Programme	The Corporate e-Learning Programme helps organisations to equip their employees with the essentials of PDPA as well as evaluate their understanding through the assessment module.
Other resources	Other resources available for organisations on the PDPC’s website include advertisements, e-newsletters, videos, posters and electronic direct mailers to promote awareness of the PDPA, brochures, handbooks and leaflets to provide concise information in bite-size format, and sample clauses and templates to enable organisations to demonstrate accountability.
Developed by industry	

Personal Data Asset Inventory Tool (Docukit Data Protection App)	The Docukit Data Protection App helps Data Protection Officers track how personal data is being managed within their organisations, and therefore manage the data protection risks in a more effective and productive manner.
DPOinBox	The DPOinBox supports organisations in the development and implementation of their data protection management programme for areas such as identifying risks, managing programme, sustaining initiatives and responding to incidents and requests.

4.4 Incorporate good data protection practices

4.4.1 A Data Protection by Design approach

An effective data protection policy is one that is able to be operationalised into business processes. One way to translate data protection policies to business processes is by adopting a Data Protection by Design (DPbD) approach in which organisations consider the protection of personal data from the earliest possible design stage of any project, and throughout the project's operational lifecycle. This can be as simple as putting data protection considerations in the foreground of any project development instead of as an afterthought.

Designing data protection from the start may help organisations to (a) identify data protection issues early, (b) increase awareness of data protection across the organisation and (c) meet the data protection obligations under the PDPA. For more information on DPbD, please refer to the PDPC's Guide to Data Protection by Design for ICT Systems.

4.4.2 Identifying and addressing data protection risks

An essential tool for the identification and management of data protection risks is the Data Protection Impact Assessment (DPIA). This involves identifying, assessing and addressing personal data protection risks based on the organisation's functions, needs and processes.

By conducting a DPIA, an organisation would be better positioned to assess if the handling of personal data complies with the PDPA or data protection best practices, and implement appropriate technical or organisational measures to safeguard against data protection risks to individuals. For more information on DPIA, please refer to the Guide to DPIA.

4.4.3 Ensure compliance with the PDPA

When organisations hire staff (including volunteers and agents) or engage service vendors to manage the personal data, it is important to know how the personal data can be protected. In this regard, organisations may consider the following:

Key activity	Component	Examples
State the personal data protection clauses clearly in the staff contract	Employment Contract	• Update employment contract with clauses on personal data protection
Set clear requirements on how vendors should manage and dispose the data	Data protection clauses in third party agreements. For more information, refer to the Guide on Data Protection Clauses Relating to the Processing of Personal Data, and the Guide to Securing Personal Data in Electronic Medium and Guide to Disposal of Personal Data on Physical Medium	• Use standard contractual clauses in contracts and processing agreements with third party service vendors to ensure protection for personal data • Use contractual clauses and retention schedules in contracts and processing agreements with third party service vendors to ensure proper disposal of personal data • Establish measures to verify the identity of third party organisations that have access to your organisation's collected data
	Data protection clauses in cross-border transfer agreements	• Establish cross-border personal data transfer contracts (e.g. transfer of personal data within organisation outside of Singapore, or parent company) to ensure protection for personal data
Conduct regular review of contracts following every sign off and renewal	Due diligence on third party service vendors	• Conduct due diligence of the personal data protection and security policies, practices and processes of potential vendors/third party sources (e.g. conduct random spot-checks, request for an independent audit report)

4.4.4 Establish a process for managing data breaches

Personal data breaches can occur due to various reasons such as malicious activity, human error or computer system error. Organisations should develop and implement a personal data breach management process to address data breaches. The plan may include the following set of activities –

C – Containing the breach
A – Assessing the risk
R – Reporting the incident
E – Evaluating the response and recovery to prevent future breaches

The organisation's DPO may also document data incidents and data breaches in an incident record log. Refer to the end of this chapter for an example of an incident record log. As good practice, organisations should also actively engage their data intermediaries and delineate the responsibility of reporting, investigating and taking remedial actions. For more information, please refer to the PDPC's Guide to Managing Data Breaches 2.0 and Guide to Active Enforcement.

4.5 Establish risk monitoring and reporting structure

As part of corporate governance, organisations are encouraged to establish an enterprise risk management framework with monitoring and reporting mechanisms (i.e. regular risk reporting and internal audit) that addresses personal data protection issues. Such a structure provides clarity on the direction and manner in which an organisation manages personal data protection risks, among others.

<table>
<tr>
<td><b>Risk Reporting</b></td>
<td>The DPO should ensure there is regular monitoring of identified personal data protection risks, reporting of data incidents and remediation to Senior Management to get their support, direction and feedback. Organisations may wish to develop reporting processes and frequency (e.g. every quarter or annually) for various feedback mechanisms from the working level to Senior Management. For instance:
<table>
<tr><th>Frequency</th><th>Possible topics for discussion</th></tr>
<tr><td>Quarterly</td><td>1. Changes to personal data protection policies and practices made in the last quarter
2. Results and action plans/remedial measures after completing the PDPA Assessment Tool for Organisations or Data Protection Impact Assessment</td></tr>
</table>
</td>
</tr>
</table>

		3. Status of or updates to existing risks, risk ratings and action plans/remedial measures 4. New risks, risk ratings and action plans/remedial measures added in this reporting quarter 5. Personal Data Protection Audit Plans 6. Key personal data protection issues to note
	Annually	1. Refreshed personal data protection risk profile for the year 2. Summary of risk remediation plans
		As a start, organisations can refer to the Board Risk Committee (BRC) Guide developed by the Singapore Institute of Directors for more information on the board's oversight role of ensuring the adequacy and effectiveness of a company's risk management and internal controls within the context of the business and regulatory environment in Singapore.
Internal Audit		Organisations can conduct an internal audit to monitor and evaluate the overall implementation of their data protection policies and processes. This could be done by: • Conducting an internal audit on a periodic basis • Conducting an ad-hoc walk through and inspection • Engaging an external party (on a periodic basis or as required) to evaluate implementation • Obtaining and maintaining certifications for the organisation's data protection measures, such as the Data Protection Trustmark (DPTM) Certification. For more information on the DPTM, please visit www.imda.gov.sg/dptm

4.6 Available resources

Please refer to the resources below for more information.

No.	Resource
1	Advisory Guidelines on Key Concepts in the PDPA
2	Guide to Data Protection Impact Assessments (DPIA)
3	Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data
4	Guide to Notification
5	Guide to Handling Access Requests
6	Guide to Securing Personal Data in Electronic Medium

7	Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data
8	Guide to Disposal of Personal Data on Physical Medium
9	Guide to Building Websites for SMEs
10	Guide to Managing Data Breaches 2.0
11	Incident Record Log
12	Sample Personal Data Inventory Map Template
13	Sample Data Flow Diagram (HR) – pdf
14	Sample Data Flow Diagram (HR) – vsd
15	Sample Clauses on Obtaining and Withdrawing Consent
16	Sample Consent Registry
17	Develop a Process for Dispute Resolution
18	Sample Clauses and Templates for Employees and Job Applicants
19	Sample Clauses and Templates for Customers
20	Template Notice for Collection of NRIC Numbers
21	Board Risk Committee (BRC) Guide by the Singapore Institute of Directors (SID)
22	Guide to Data Protection by Design for ICT Systems
23	Guide to Active Enforcement

PART 5: MAINTENANCE

5.1 Why do organisations need to review their data protection policies and practices?

Organisations are encouraged to routinely review their data protection policies and practices to enable them to identify data protection gaps and the appropriate remedies. In Singapore's evolving digital economy, this will provide the assurance that the organisation's data protection practices are in line with regulatory and technological developments and that data protection risks are being managed effectively.

5.2 How do organisations keep their data protection policies and practices relevant?

Organisations may consider the following steps:

1. Monitoring external and internal environment to be apprised of any developments
2. Conducting regular reviews of data protection policies and practices
3. Keeping staff and external stakeholders apprised of changes to data protection policies and practices
4. Validating the DPMP

5.2.1 Monitor external and internal environment

To ensure that data protection policies and practices remains relevant and updated, organisations need to keep abreast of the changes and developments within and outside the organisation. Some suggestions on how to monitor the environment include:

	External Environment	Internal Environment
What to monitor?	• Amendments to the PDPA and PDP Regulations • Issuance of new resource from the PDPC • Data breaches in other organisations • Changes in sector-specific regulations • Data protection best practices by other organisations	• Systems or processes (that process personal data) that are being newly designed or undergoing major changes • New business engagement • Data incidents • Feedback from stakeholders (e.g. direction by senior management, complaints/feedback by customers)

How to monitor?	• Sign up with DPO Connect to get updates on data protection developments and related events • Subscribe to reporting services and circulars by law firms to get updates on legislative and regulatory developments • Attend data protection related conference and training • Research on developments in data protection	• Conduct staff survey to understand data protection awareness or feedback on data protection practices in organisation • Conduct Data Protection Impact Assessments (DPIAs) on systems and processes (that process personal data) that are being newly designed or undergoing major changes • Attend to feedback from customers

5.2.2 Review and revise the DPMP

Changes in environment may require revisions to data protection policies and processes. Organisations would have to decide whether the revisions should be applied immediately (ad-hoc) or during a periodic review of the DPMP. The table shows examples of circumstances that may prompt either immediate or periodic changes.

Immediate (ad-hoc)	Periodic
• Occurrence of major incidents (e.g. leakage of personal data to public due to new technology) • Legislative and regulatory amendments • Major changes within the organisation such as re-organisation, merger or acquisition.	• Occurrence of minor incidents (e.g. accidental unauthorised access by employee to personal data) • Revision of processes or systems that have minimal effect on data protection (e.g. change of DPO's business contact information)

Organisations may also conduct a Data Protection Impact Assessment (DPIA) to help identify, assess and address data protection risks associated with the new changes. Please refer to the PDPC's Guide to DPIAs for more information.

5.2.3 Notify stakeholders on changes to data protection policies and practices

Organisations should keep stakeholders apprised of the changes to their policies or practices as part of their training and communication plan as suggested in Chapter 3 of this guide.

An organisation's data protection policies and practices should be accessible. For example:

- Softcopy stored on organisation's repository for all staff's reference (e.g. intranet)
- Hardcopy version filed and kept with each department

5.2.4 Validate the DPMP

Organisations may choose to validate their DPMP through an external review. For example, they may seek to certify their data protection practices through the Data Protection Trustmark (DPTM) Certification. These are good practices to get the confidence and assurance that the organisation has in place robust data protection measures that are in line with the PDPA and comparable to industry standards.

Review by external party	Getting DPMP validated by an external party helps ensure that the organisation's data protection policies and practices are robust and comparable to industry standards.
Apply for DPTM certification	The DPTM is a voluntary enterprise-wide certification that help organisations demonstrate accountable and responsible data protection practices. Obtaining the DPTM certification demonstrates to customers that the organisation has robust data protection policies and practices in place to safeguard their personal data. DPTM-certified companies could look forward to: • Increased business competitiveness by strengthening the organisation's reputation, build trust and foster confidence in the organisation, raising its competitiveness both locally and overseas; and • Validation of the organisation's data protection governance and protection standards and practices, as well as identification of potential weaknesses which will allow the organisation to take steps or put in place remedial measures to mitigate the risks. For more information, please visit: www.imda.gov.sg/dptm

END OF DOCUMENT

BROUGHT TO YOU BY

pdpc
PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Copyright 2019 – Personal Data Protection Commission Singapore (PDPC)

This publication gives a general guide to establishing a Data Protection Management Programme (DPMP). The contents herein are not intended to be 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.

The contents of this publication are protected by copyright, trademark or other forms of proprietary rights and may not be reproduced, republished or transmitted in any form or by any means, in whole or in part, without written permission.