GUIDE TO

DEVELOPING A DATA PROTECTION MANAGEMENT PROGRAMME

SG:DIGITAL

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CONTENTS

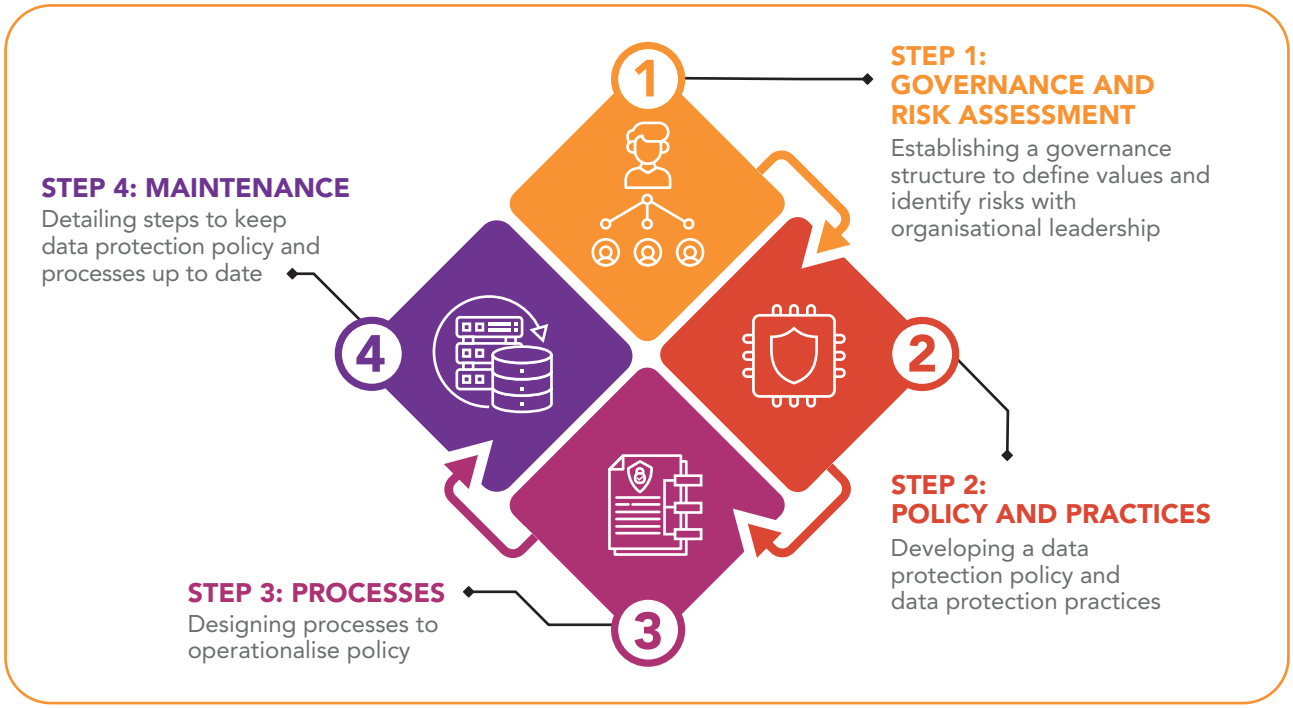
INTRODUCTION

Accountability requires organisations to undertake measures to manage and protect personal data in order to meet their obligations under the Personal Data Protection Act ("**PDPA**"). This includes adapting legal requirements into policies and practices, and utilising monitoring mechanisms and controls to ensure that those policies and processes are effectively implemented. It also includes building an organisational culture of responsibility through training and awareness programmes.

This guide provides information on how organisations may demonstrate accountability by implementing a Data Protection Management Programme ("**DPMP**"). Organisations may review and benchmark their existing personal data protection policies and practices against the framework and considerations provided in this guide[1]. Ultimately, organisations should tailor their personal data protection policies and processes to their organisational needs.

WHAT IS A DPMP?

The DPMP is a four-step programme to establish a robust data protection infrastructure:

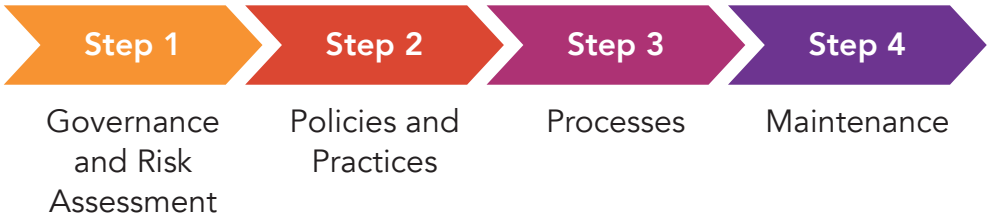


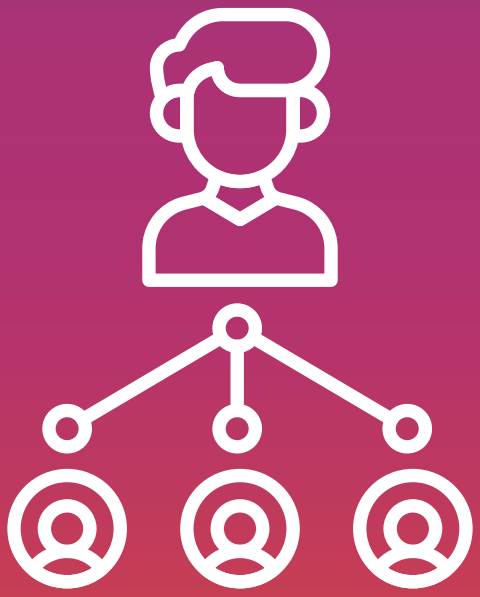
[1] *Organisations should note that adopting the suggestions in this guide does not mean that it would be in compliance with the PDPA. An organisation should consider whether the suggestions in this guide could be adapted for its specific circumstances.*

WHY DO YOU NEED A DPMP?

Having an established DPMP helps an organisation to demonstrate accountability in data protection. This provides confidence to stakeholders and fosters higher-trust relationships with customers and business partners for business competitiveness.

This guide will address the four-step process as follows:





PART I: GOVERNANCE AND RISK ASSESSMENT

GOVERNANCE STRUCTURE AND VALUES

Role of Senior Management

To demonstrate commitment to personal data protection, the senior management of an organisation should be responsible for the organisation's approach to handling personal data. The senior management provides leadership through:

- Defining the strategic corporate values and principles to align data protection obligations and responsibilities within the organisation;
- Allocating resources (e.g. budget, manpower) to data protection;
- Appointing and empowering the Data Protection Officer ("**DPO**");
- 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;
- Providing strategic guidance on the implementation of data protection initiatives;
- Approving the organisation's data protection policies and DPMP;
- Commissioning Data Protection Impact Assessments ("**DPIA**");
- Advocating data protection training;
- Providing direction to the DPO for handling of major complaints and managing data breaches, including implementation of remediation plans; and
- Providing direction to the DPO for communication and liaison with the Personal Data Protection Commission ("**PDPC**").

Role of the DPO

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

- Driving the development and review of data protecton policies and processes;
- Ensuring compliance with the PDPA through data protection policies and processes;
- Fostering a personal data protection culture within the organisation and communicating the organisation's personal data protection policies to stakeholders;
- Identifying and alerting management to any risk that might arise with regard to the personal data handled by the organisation;
- Handling access and correction requests to personal data;
- Managing personal data protection-related queries and complaints; and
- Engaging with the PDPC on personal data protection matters, if necessary.

DPOs are also strongly encouraged to use the **DPO Competency Framework and Training Roadmap**[2] to build core competencies and achieve the proficiency levels set out for a DPO.

Oversight and Governance

Data protection is a topic that should have board and senior management level oversight. An appropriate governance structure should be established at both board and senior management levels. It is perfectly fine to integrate data protection into existing governance structures within

[2] *Refer to the DPO Competency Framework and Training Roadmap.*

the organisation, whenever this is possible. As a start, organisations can refer to the **Board Risk Committee Guide** developed by the Singapore Institute of Directors (SID) for more information on the board's role of overseeing and 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.

The DPO is a key management function within this oversight and governance structure. Given the requirement for the DPO to effectively lead data protection initiatives across the organisation, a DPO should ideally be an appointment within the organisation's senior management. If the DPO is not appointed from the ranks of senior management, he/she should have a direct line of reporting to senior management. The responsibilities of the DPO can be taken on by one personnel or a group of personnel. Some organisations may decide to outsource DPO functions to, for example, a service provider or centralised corporate functions with a group of companies. When outsourcing the DPO function, the organisation should still ensure that a member of the senior management remains responsible to oversee and work with the outsourced DPO. Please refer to **Annex A** for an illustration on how a DPO may sit within the structure of an organisation.

Culture of Accountability and Staff Training

A culture of accountability towards data protection in an organisation is crucial. This includes awareness and alertness to data protection issues among all staff, which is dependent on education and buy-in from senior management.

It should be noted that personal data protection cuts across roles, functions and hierarchy in the organisation; and should be recognised and practised by all levels in the organisation (including volunteers, agents and contract staff), rather than being 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. It would thus be important for them to receive and undergo more thorough data protection training.

In this regard, organisations should ensure that data protection awareness and education are implemented top-down, from the Board of Directors to management and staff. Organisations should also design their training and briefings according to the roles and responsibilities or job functions

in the organisation, share personal data protection measures and embed personal data protection-related topics into their staff training and communication plan. Regular circulars may be used to generate awareness and foster a culture of personal data protection. Staff should constantly stay alert to risks and take proactive steps in response. This could be backed by incentives and reward systems to encourage such behaviour and promote awareness of management support. An overview of possible training and communication initiatives, and the phases at which they may be conducted throughout a typical employment journey, is illustrated in **Annex B**.

RISK ASSESSMENT

Understanding Risks

The senior management of an organisation should have an understanding of risks and review the risks on a regular basis to take into consideration changes in business models, regulations, technology and other factors. An organisation should also consider other risks arising from data beyond personal data. An organisation may consider these four general categories of risk:

Strategic: Risks affecting achievement of the strategic objectives of the company (e.g. governance, strategic planning, major initiatives). This may affect a company's ability to comply with the PDPA.

Operational: Risks affecting the operations of the organisation (e.g. sales and marketing, supply chain). This may be a factor in whether the company can comply with the PDPA.

Compliance: Risks affecting the company's compliance with regulatory requirements (e.g. legal, code of conduct). This would include compliance with the PDPA.

Financial: Risks affecting the financial processes of the company (e.g. accounting and reporting, tax). This may arise as a result of fines incurred from failing to comply with the PDPA.

Enterprise Risk Management

The Enterprise Risk Management ("**ERM**")[3] is a process effected by the organisation's Board of Directors, management and staff. It is applied in strategy setting and across the organisation, to identify potential events that may affect the organisation, as well as manage risks. An ERM framework helps to codify and integrate a holistic, structured and disciplined approach to managing risks into the company's core business processes and decision-making. Organisations should ensure that data protection[4] is incorporated into their ERM framework to manage their risks.

Risk Identification and Assessment

An essential process for the identification and management of personal data is the DPIA at the system or operational level. The DPIA would enable organisations to:

- Identify the personal data handled by the system or operational process, as well as the reasons for collecting the personal data;
- Identify how the personal data flows through the system or operational process;
- Identify data protection risks by analysing the personal data handled and its data flows against PDPA requirements or data protection best practices;
- Address the identified risks by amending the system or operational process design, or introduce new organisation policies; and
- Check to ensure that identified risks are adequately addressed before the system or process is in effect or implemented.

[3] *Refer to Board Risk Committee Guide developed by the Singapore Institute of Directors for more information on the Enterprise Risk Management framework.*

[4] *Refer to Case Study 3B-5 in the Board Risk Committee Guide developed by the Singapore Institute of Directors on how organisations can mitigate data protection risks.*

By conducting a DPIA, an organisation would be in a better position to assess if the handling of personal data complies with the PDPA or data protection best practices, and to implement appropriate policy, technical or process measures. For more information on the DPIA, please refer to the **Guide to Data Protection Impact Assessments**.

As part of a DPIA, it is recommended to establish a data inventory (see **Data Inventory Maps, Data Flow Diagrams and Other Registers** on page 23) and classify the risk level of the data in the context that it is collected, used and disclosed throughout the data life cycle, from creation, distribution, storage, to disposal. This may be mapped onto a risk matrix for assessment and implementation of appropriate controls for the identified risk levels.

Risk levels may be determined by considering the following three industry-recognised parameters of impact in the event the data is compromised:

Confidentiality: Risk to organisation or individuals arising from unauthorised or inappropriate disclosure. For information to be confidential, the access to some information needs to be restricted as it could harm the interests of the stakeholders.

Integrity: Risk to information quality or corruption. For information to be useful and serve the purpose, it must be as accurate and complete as possible.

Availability: Risk of information not being available to intended users. For information to be useful and serve its purpose, it must be available when it is needed and in a form that is accessible by the intended users.

PART II: POLICY AND PRACTICES

DATA PROTECTION POLICIES AND PRACTICES

An organisation's governance and risk management structure will shape its data protection policies and practices. As part of its corporate governance structure, the organisation should develop appropriate data protection policy and practices, and communicate them to both its internal stakeholders (e.g. staff) and external parties (e.g. vendors, customers). This will provide clarity to internal stakeholders on the responsibilities and processes related to handling personal data in their day-to-day work. Policies also demonstrate accountability to external parties by informing them of the value the organisation places on data protection and how it will protect personal data in its care.

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 Stakeholders	External Parties
General		
a. What personal dataset does this policy apply to?	•	•
b. What is the purpose of the policy?		
c. How often is this policy reviewed?	•	
d. How is the policy aligned with my organisation's values and business code of conduct?	•	•
e. Is this policy transparent?		
People		
f. Who is the intended audience of the policy?	•	•
g. Who does the policy apply to? Are their roles and responsibilities clear and comprehensive?		
h. Who is the policy owner?		
i. Who approves the policy?		

Question	Applicable To	
	Internal Stakeholders	External Parties
Process		
j. Whose personal data is handled?	•	•
k. What is the purpose of collecting the personal data?		
l. What types of personal data are handled (e.g. name, NRIC, birth date, health details)?		
m. How are queries, feedback, disputes and requests handled?		
n. Which third party organisations is the personal data shared with, if any?		
o. How does the organisation ensure that third party organisations protect data in accordance with the PDPA requirements?		
p. How are the data protection and Do Not Call ("**DNC**") provisions of the PDPA complied with throughout the data life cycle?[5]		
q. How is the personal data protected?	•	
r. How long should the personal data be kept and how should it be disposed at the end of its life cycle?	•	•
s. How should data incidents[6] and data breaches be handled, including mandatory data breach notifications to the PDPC and affected individuals?		
t. When are DPIAs conducted, and on which systems or for which processes?	•	
u. How should policy exceptions be handled?		

Organisations should also consider having dedicated internal policies on specific areas that require elaboration. The following example lists some of the considerations when handling access requests:

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

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

Example: 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 does ABC intend to receive all access requests[7]? (e.g. Is there a standard access request form that the applicant may use? 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 available 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, date and time the personal data was collected)
Charging access fees	• Would ABC be charging a fee[8] to process the access request? If so, are the fees provided in writing to the applicant[9]? • If ABC intends to charge a fee for the access request that is higher than originally estimated, how would ABC communicate the higher fees in writing to the applicant? • How would ABC compute the access fee[10] in a way that accurately reflects the time and effort required to respond to the access request?

[7] *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 DPO 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.*

[8] *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.*

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

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

Determining response timeframe	• How long would ABC take to provide access to the requested personal data[11]? 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? What forms of proof of identity are required?
Assessing exceptions and prohibitions	• When processing an access request, ABC should also assess whether any prohibitions or exceptions may apply such that access to personal data may not be provided[12]. • When the access request contains personal data of other individuals, ABC should consider whether any prohibitions or exceptions may apply to the access request and whether ABC needs to redact the personal data of other individuals[13].
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[14]. • 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**.

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

[12] *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.*

[13] *Organisations need not redact personal data of other individuals if the data is considered part of any user activity data about, or any user-provided data from, the individual who made the request.*

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

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.

INCORPORATE GOOD DATA PROTECTION PRACTICES

A Data Protection by Design Approach

An effective data protection policy is one that can be operationalised into business processes. One way to translate data protection policies into business processes is by adopting a Data Protection by Design ("**DPbD**") approach, where organisations consider the protection of personal data from the earliest possible design stage of any project, and throughout the project's operational life cycle. 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 can 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. Organisations may wish to adapt the DPbD principles in the PDPC's **Guide to Data Protection by Design for ICT Systems** throughout their project design, development and operational life cycle.

Ensure Compliance with the PDPA

It is important for an organisation's staff, as well as third party organisations engaged to process personal data on its behalf, to know how the organisation expects the personal data to be handled and 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 Employee Handbook	• Update employment contract with clauses on responsibility to protect personal data • Details may be contained in the employee handbook, and updated periodically
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 to Managing Data Intermediaries** under the PDPA, **Guide on Data Protection Clauses Relating to the Processing of Personal Data**, and the **Guide to Data Protection by Design for ICT Systems**.	• Use standard contractual clauses in contracts and processing agreements with third party organisations to ensure protection for personal data • Use contractual clauses and retention schedules in contracts and processing agreements with third party organisations to ensure proper disposal of personal data • Establish measures to verify the identity of third party organisations that have access to the organisation's collected data
	Data protection clauses for cross-border personal data transfer contracts For more information, refer to the **Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data** and the **Guidance for Use of ASEAN Model Contractual Clauses for Cross-Border Data Flows**.	• Establish cross-border personal data transfer contracts (e.g. transfer of personal data within organisations outside of Singapore or the parent company) to ensure protection for personal data
Conduct regular review of contracts	Due diligence on third party organisations	• Conduct due diligence of the personal data protection and security policies, practices and processes of service vendors/third party organisations (e.g. conduct random spot checks, request for an independent audit report)

COMMUNICATE POLICIES TO CUSTOMERS (E.G. CLIENTS, DONORS, OTHER ORGANISATIONS)

Customers' trust is crucial and organisations should implement personal data protection initiatives to demonstrate accountability. Organisations should thus ensure that their data protection policies are communicated clearly and upfront. Useful initiatives include:

Notification: Publish policies and other information in simple language and place them in prominent locations and/or other relevant channels (e.g. websites) that are easily accessible by customers.

Consent: Ensure that customers understand what they are consenting to along their user journey by providing simple and clear consent clauses at appropriate touchpoints through dynamic consent.

Policy updates: Manage ongoing customer relationships with clear communication on any policy or service updates, and keep such communications clearly separated from marketing messages.

Staff's interactions with customers: Ensure that the staff assigned to interact with customers are trained in the content knowledge and sensitivity required in handling data protection feedback and queries.

Access and correction request handling: Provide easily accessible channels and proper processes for handling customers' access and correction requests, which are monitored to ensure prompt response.

Complaints handling: Ensure that there are proper channels and processes for handling customer complaints concerning personal data.

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

PART III: PROCESSES

The organisation's controls and processes should be designed to cater to risks earlier identified in **Risk Identification and Assessment** on page 12. Having identified risks, the organisation should ensure that such risks are minimised through the implementation of controls, and residual or ad-hoc risks monitored.

Risk identification and mapping: Tools such as data flow and consent registers can help to identify and map risks relating to personal data and to design controls.

Risk remediation and controls: Risks that have been identified should be remediated through the implementation of systems-based or process controls.

Risk monitoring and reporting: Operational monitoring systems should be designed to monitor occurrence of residual risks or ad-hoc risks, and internal reporting processes designed for escalation to management. Breach management plans can help with breach monitoring and management.

Finally, periodic internal and external audits should be conducted to ensure that all data protection risks are addressed amidst changing circumstances.

RISK IDENTIFICATION AND MAPPING

Data Inventory Maps, Data Flow Diagrams and Other Registers

Known risks should be managed through a good understanding of the life cycle and flow of personal data in your organisation. This can be done through documenting the personal data handled using diagrams and charts such as data inventory maps or data flow diagrams, as illustrated in **Annex C**.

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 the classification of the data to manage user access. They should also deal with when and how the organisation should dispose of or anonymise the personal data 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.

Organisations may also wish to adopt a risk register following their inventory mapping. The risk register should identify the risks associated with the nature of the personal data and the context in which it is used. This should be shaped by risks identified in **Risk Identification and Assessment** on page 12. In addition, organisations should consider existing whitelists of data, as determined internally and/or by relevant regulations, which may be subject to more stringent regulation, as highlighted in the **Guide on Managing and Notifying Data Breaches Under the PDPA**, for instance.

As good practice, organisations should create a consent register 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.

The tools described in this section will help with identification and management of risks, and can be translated into controls. These tools may need to be updated and reviewed periodically, and when conducting a DPIA.

Resources to Identify Risks and Gaps

PDPC provides many resources to support organisations in developing their data protection practices. Organisations may refer to the following tools as a start to identify and map their risks and gaps in data protection.

Tool	Description
Data Protection Starter Kit Checklist	The Data Protection Starter Kit Checklist allows organisations to conduct self-assessment and identify data protection gaps in the organisation.
Data Protection-as-a-Service for SMEs (DPaaS@SMEs)	The DPaaS@SMEs Programme (DPaaS@SMEs) makes it easier for SMEs to outsource data protection functions and supports SMEs in strengthening their data protection capabilities.
Sample Personal Data Inventory Map Template	The Personal Data Inventory Map helps organisations manage the personal data under their control. It is easy to develop, maintain and update, and does not require high-level software and skills.

Tool	Description
Sample Consent Registry Template	The consent registry helps organisations to record consent provided by individuals to the organisation for the collection, use and disclosure of their personal data for a particular purpose.
Data Flow Illustration	The Data Flow Illustration diagram helps organisations visualise the flow of data within their organisation.
DPOinBox	The DPOinBox supports organisations in the development and implementation of their DPMP for areas such as identifying risks, managing the programme, sustaining initiatives and responding to incidents and requests.
Personal Data Asset Inventory Tool (Docukit Data Protection App)	The Docukit Data Protection App helps DPOs track how personal data is being managed within their organisations, and therefore manage the data protection risks in a more effective and productive manner.
OneTrust Software for PDPA Compliance	The OneTrust Software for PDPA Compliance provides organisations with tools to build their Data Inventory Map ("**DIM**") and conduct DPIA to better manage their compliance with the PDPA.

RISK REMEDIATION AND CONTROLS

Put in Place System-based and Process Controls and Measures

Based on the risks and gaps identified above, organisations can then put in place relevant system-based and process controls and measures to address the risks and gaps. For example, the data inventory map, data flow diagram and risk register help organisations to identify where sensitive data is stored in the systems. This helps organisations to determine the level of IT security protection to put in place and the types of users/applications (internal and external) which can access such systems and data. Appropriate process controls can also be implemented to approve, review and manage the access rights of these users and applications. From the consent register, organisations will be able to identify the types of personal data that can be used for different purposes and put in place relevant approval processes for the use of these data.

When developing systems, organisations should consider and build data protection measures into ICT systems that involve the processing of personal data during the software development life cycle. By adopting DPbD, appropriate controls to protect personal data would have been embedded within the system which helps to reduce unnecessary delays and contain costs, compared to having to retrofit data protection features afterwards.

Controls adopted should correspond to the risk level and nature of the data, and should include both digital and non-digital solutions (e.g. encryption and access controls).

For more information, please refer to the the PDPC's **Guide to Data Protection by Design for ICT Systems**.

Include Processes for Managing Service Vendors

Organisations are required to communicate their personal data protection requirements to their service vendors or data intermediaries clearly. When handling personal data of the organisation, these data intermediaries are responsible for adhering to the Protection, Retention Limitation and Data Breach Notification Obligations under the PDPA. In this regard, a binding contractual agreement that highlights the responsibilities with regard to the processing of the personal data should be in place. In addition, where data is transferred internationally, organisations should ensure that such transfers are done in compliance with the PDPA (e.g. by ensuring that the service vendor is certified under the APEC Cross Border Privacy Rules ("**CBPR**") or Privacy Recognition for Processors ("**PRP**") systems). For more information on managing data intermediaries in the context of personal data protection, refer to the PDPC's **Guide to Managing Data Intermediaries**.

PDPA Assessment Tool for Organisations ("**PATO**")

Organisations should also use the **PATO** as a self-assessment tool to assess any residual gaps from their systems-based and process controls, as well as monitor the implementation of these controls. Based on the assessment report, organisations would be able to ascertain how internal processes on handling personal data can be refined.

RISK MONITORING AND REPORTING

Organisations should ensure that all risks, especially residual risks that cannot be addressed by systems-based controls and processes, are monitored through regular reporting to the committees within the organisation's governance structure and through operational monitoring and reporting (e.g. management reports). The DPO should ensure that there is regular monitoring of identified personal data protection risks, reporting of data incidents and remediation to the relevant oversight body at the board and 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:

Frequency	Possible topics for discussion
Quarterly	1. Changes to personal data protection policies and practices made in the last quarter 2. Results and action plans/remedial measures after completing the PATO or DPIA 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

Organisations should be able to demonstrate that they have in place accountable practices, such as monitoring and remediation plans. Under the PDPC's **Active Enforcement Framework**, this may allow the organisation to qualify for an undertaking option in the case of a data breach, allowing for a better outcome as opposed to a full investigation.

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**ontaining the breach
- **A**ssessing the risk
- **R**eporting the incident
- **E**valuating 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 responsibilities of reporting, investigating and taking remedial actions.

Organisations must also notify the PDPC and affected individuals when they have credible grounds to believe that a data breach has occurred. They should conduct this assessment on whether it is a notifiable data breach within 30 calendar days. The steps taken in assessing the data breach should be documented to demonstrate that the organisation has been reasonable and expeditious in doing so.

For more information, please refer to the **Guide on Managing and Notifying Data Breaches Under the PDPA** and **Guide on Active Enforcement**.

PART IV: MAINTENANCE

REVIEWING DATA PROTECTION POLICIES AND PRACTICES

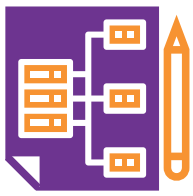
Organisations are encouraged to routinely review their data protection policies and practices to enable them to identify data protection gaps and the appropriate remedies through effective oversight by the board and senior management. In Singapore's evolving digital economy, this will provide the assurance that the organisation's data protection practices are kept updated with regulatory and technological developments and that data protection risks are being managed effectively.

FREQUENCY OF REVIEW

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 • Occurrence of organisational changes (e.g. re-structuring, mergers and acquisitions, process changes)	• Revision of data protection policies and processes at regular intervals, with a pre-specified time interval, to ensure that policies and processes remain relevant • Batch review of occurences of minor incidents (e.g. accidental access to personal data by unauthorised employee) • Revision of processes or systems that have minimal effect on data protection (e.g. change in DPO's business contact information)

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



ESTABLISH AN AUDIT STRUCTURE

As part of corporate governance, organisations are encouraged to establish an ERM 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.

Audit

Organisations can conduct an 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 **IMDA's website**.

KEEPING DATA PROTECTION POLICIES AND PRACTICES RELEVANT

Monitor External and Internal Environment

To ensure that data protection policies and practices remain 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 resources from the PDPC • Changes to sector-specific regulations • Data breaches in other organisations • Data protection best practices by other organisations • Technological changes or emerging technologies that might result in increased data protection risks	• Systems or processes (that process personal data) which are being newly designed or undergoing major changes • New business engagement or business model • Feedback from stakeholders (e.g. direction from senior management, complaints/ feedback from customers) • Data incidents
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 conferences and training • Research on developments in data protection	• Conduct DPIAs on systems and processes (that process personal data) that are being newly designed or undergoing major changes • Conduct staff surveys to understand data protection awareness or feedback on data protection practices in the organisation • Attend to feedback from customers

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 **Culture of Accountability and Staff Training** on page 10 of this guide.

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

- Store information on these policies and practices on the organisation's repository for all staff's reference (e.g. Intranet) and create awareness through regular staff update emails
- Work with outsourced vendors to disseminate the information to their staff who are handling the organisation's personal data
- Update the information onto the organisation's website and push updates to customers through emails, newsletters or other CRM channels

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 DPTM Certification. These are good practices to provide their stakeholders with the confidence and assurance that the organisation has put in place robust data protection measures in line with the PDPA and comparable to industry standards.

Review by external party	Getting the 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 helps 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, building trust and fostering 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 **IMDA's website**.

ANNEX A: ILLUSTRATION OF THE DPO IN AN ORGANISATION

(A) Personnel within senior management appointed as the DPO

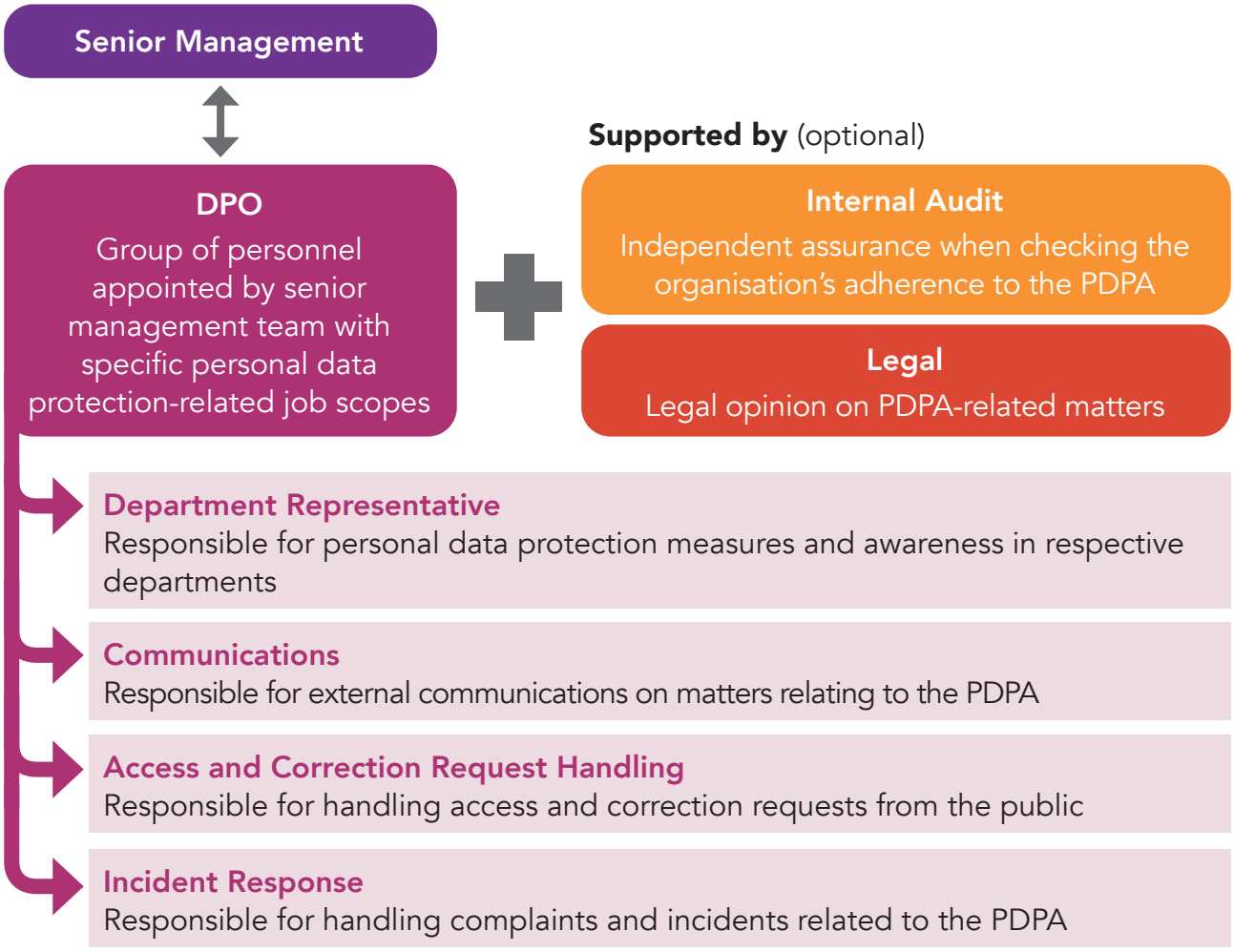
Senior Management

Regional OR Group DPO

Personnel appointed from senior management team that

- oversees all personal data protection-related matters;
- oversees data transfer activities; and
- provides leadership guidance on personal data protection law in local and/or other jurisdictions.

(B) A group of personnel appointed (with support from the Audit and Legal departments)



ANNEX B: TRAINING AND COMMUNICATION INITIATIVES IN A TYPICAL EMPLOYMENT JOURNEY

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

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

No	Type	Timing	Target	Details	How
1	Board of Directors' support	• At the start of the organisation's personal data protection journey • Periodically, when corporate risk register[14] 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. seminars, briefings) • Briefings to Board of Directors by external vendors

[14] *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
2	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. seminars, briefings) • PDPC's E-learning Programme • PDPC's sectoral briefings • Training by external vendors
3	PDPA training	• Onboarding of staff • Ad-hoc when there is a revision to the PDPA, PDPC guidelines or organisation's data protection policies and practices	• All staff	• Educate staff on the PDPA and the organisation's data protection policies and processes • Make available data protection training materials on an accessible platform (e.g. intranet) • Suggested topics include: a. Importance of personal data protection b. Main obligations under the PDPA c. The organisation's personal data protection policies and processes d. Business benefits of increased accountability to data protection	• PDPC's E-Learning Programme • In-house trainings or briefings by the DPO on data protection policies and practices • Training by external vendors • eDMs, posters, videos, organisation's intranet, circulars to inform and update staff on organisation's new or revised data protection policies and practices

No	Type	Timing	Target	Details	How
4	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) • Practitioner Certificate in Personal Data Protection (Singapore) Preparatory Course • Training by external vendors
5	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 the organisation's data protection practices and policies through newsletters, eDMs, posters, videos, organisation's Intranet, circulars, roadshows, town hall or brown bag discussions • PDPC events (e.g. seminars, briefings)
6	Obtain professional certification	• As part of career development	• The DPO and staff who are part of the DPO's 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

For more information on help for organisations, please refer to the **PDPC's website**.

ANNEX C: DATA INVENTORY MAP AND DATA FLOW DIAGRAM

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	Data 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 Draw 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 Starhub, M1, Singtel	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	NA	1 year	Physical - Shredding Electronic - Cleanup software

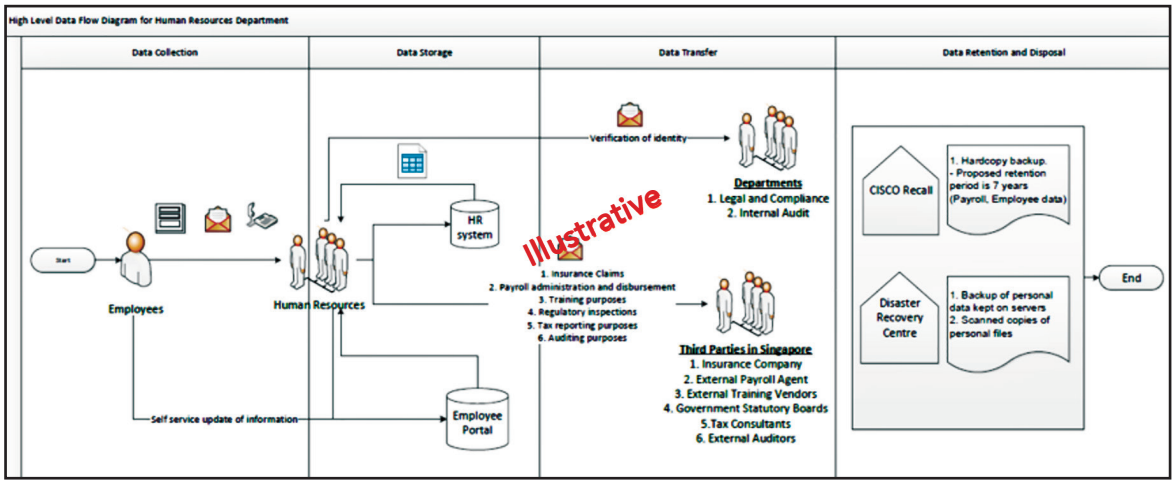
Pros

- Easy to develop, maintain and update
- Does not require high-level software and skills
- No limitations on recording of information
- Effective for extensive and complex data flows

Cons

- Lacks visual representation of data flow
- Limited representation on interconnectivity of personal data

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

#SGDIGITAL

Singapore Digital (SG:D) gives Singapore's digitalisation efforts a face, identifying our digital programmes and initiatives with one set of visuals, and speaking to our local and international audiences in the same language.

The SG:D logo is made up of rounded fonts that evolve from the expressive dot that is red. SG stands for Singapore and :D refers to our digital economy. The :D smiley face icon also signifies the optimism of Singaporeans moving into a digital economy. As we progress into the digital economy, it's all about the people — empathy and assurance will be at the heart of all that we do.

BROUGHT TO YOU BY

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE