AITI
Authority for Info-communications Technology Industry of Brunei Darussalam

GUIDE

Developing a Data Protection Management Programme

Version 1.0 | 4 June 2025

Contents

1. Introduction

1.1 Organisations are required to put in place measures to manage and protect personal data in their possession or under their control in order to meet their obligations under the PDPO. Such measures include developing and implementing the necessary data protection policies and practices, and having processes and controls to ensure that those policies and practices are implemented in an effective manner.

1.2 One key way of ensuring that an organisation demonstrates accountability-driven practices is by establishing a **Data Protection Management Programme** ("**DPMP**") within the organisation.

1.3 This Guide has been developed by the Authority for Info-communications Technology Industry of Brunei Darussalam ("**AITI**") to provide a baseline set of considerations on the implementation of a DPMP for their organisation. Where organisations have existing data protection policies and practices, they may consider aligning them with the general framework and practices in this Guide or adopt other measures as appropriate to meet their obligations under the PDPO.

1.4 Note: The implementation of the considerations within this Guide does not indicate an organisation's compliance with its obligations under the PDPO. Accordingly, organisations should adapt their DPMP to meet their business needs and customised to their own circumstances.

2. Data Protection Management Programme

2.1 A Data Protection Management Programme is a structured programme for the management of an organisation's data protection processes and practices.

2.2 It takes into account the organisation's responsibilities under any applicable data protection laws and is aimed at ensuring that there is appropriate oversight and management of the various measures that must be implemented for compliance. Organisations may implement the measures and controls it requires taking into account its governance, operational and business considerations.

2.3 Implementing a DPMP demonstrates an organisation's accountability with respect to their personal data handling practices. This cultivates an environment of trust with stakeholders such as customers and external third-party organisations and thus improves business competitiveness.

2.4 A DPMP typically address six (6) areas as follows:

(a) **Area 1: Governance and management structure**
Developing a governance structure for the organisation, setting out the management's roles and responsibilities and designation of key individuals including the Data Protection Officer ("**DPO**").

(b) **Area 2: Needs analysis and risk identification**
Understanding the organisation's needs, practices and risks relating to personal data.

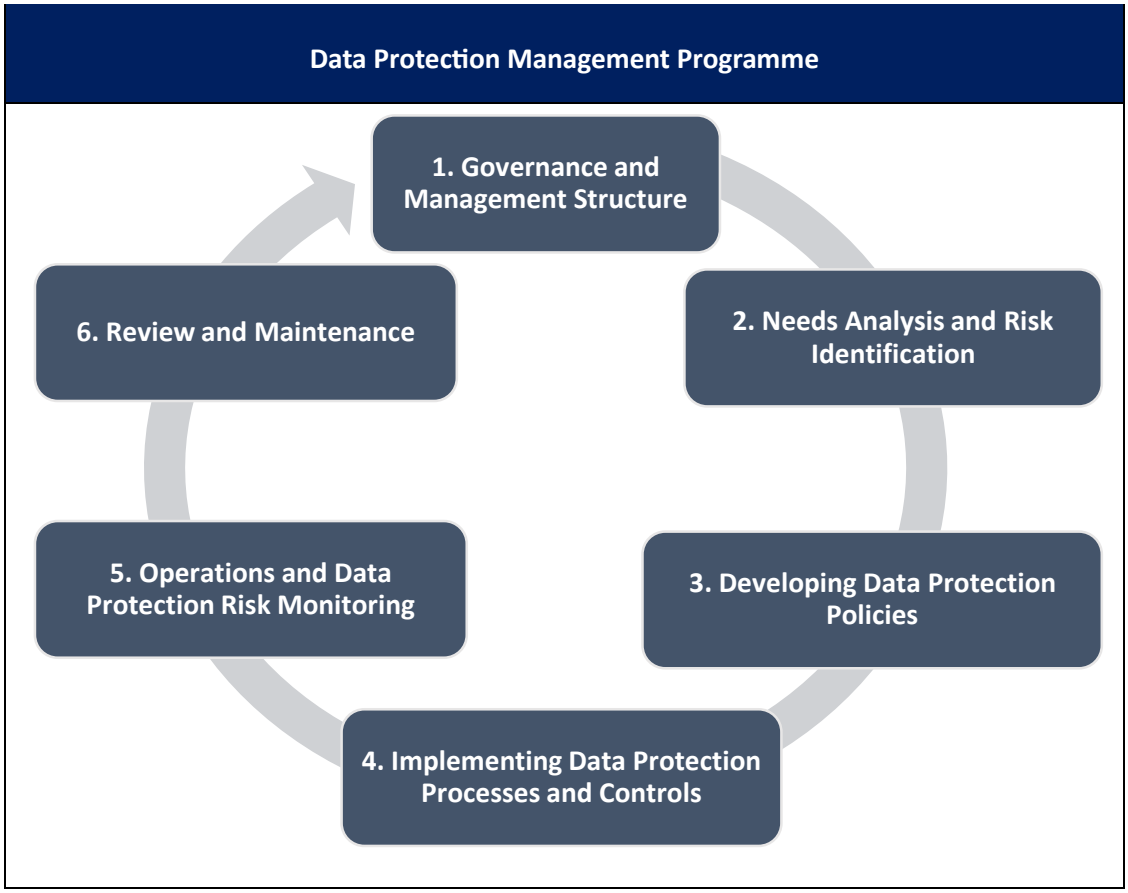
(c) **Area 3: Development of data protection policies**
Developing policies necessary for the organisation to comply with the requirements of the PDPO.

(d) **Area 4: Implementation of data protection processes and controls**
Implementing the organisation's data protection policies through appropriate processes and controls, including communication of policies (internally and externally), staff training.

(e) **Area 5: Operations and data protection risk monitoring**
Addressing data protection issues and risks that arise in the course of the organisation's business and day-to-day activities.

(f) **Area 6: Review and maintenance**

Periodically reviewing the organisation's data protection policies and practices taking into account changes in the organisation's needs and changes in the external environment (e.g. amendments to data protection laws).



3. Key Areas

The following section covers these six (6) areas in detail and provides steps organisations can consider to take when developing its Data Protection Management Programme.

3.1 Area 1: Governance and Management Structure

Senior Management

3.1.1 As the first step to developing a DPMP, senior management of an organisation should first develop the organisation's approach to handling personal data.

3.1.2 The role of senior management includes:

(a) Demonstrating the organisation's commitment towards personal data protection by defining the high-level, strategic corporate values and approach with respect to the organisation's data protection obligations and responsibilities;

(b) Appointing and empowering the DPO with an appropriate level of authority so that he/she would be sufficiently empowered to discharge their duties;

(c) Overseeing the DPO when communicating and interacting with AITI;

(d) Allocating resources (such as the organisation's financial budget, manpower and time) towards data protection;

(e) Overseeing and managing the organisation's data protection risks as part of corporate governance, such as the organisation's risk management framework;

(f) Approving the organisation's data protection policies, processes and DPMP;

(g) Conducting Data Protection Impact Assessments ("**DPIAs**");

(h) Directing the organisation's DPO when the organisation experiences data breaches or receives serious complaints;

(i) Laying out strategic guidance on the implementation of the organisation's data protection programmes and initiatives; and

(j) Championing internal data protection training and awareness.

Data Protection Officer

3.1.3 The role of a DPO is to facilitate the organisation's compliance with its responsibilities under the PDPO. The role of a DPO includes:

(a) Ensuring the organisation's compliance with the PDPO through the development and continual review of the organisation's data protection policies and processes;

(b) Cultivating a culture of accountability within the organisation and communicating the organisation's personal data protection policies and processes to internal and external stakeholders;

(c) Handling access and correction requests from individuals together with the relevant business units;

(d) Being in charge of responding to personal data protection-related queries and complaints directed to the organisation;

(e) Identifying any personal data protection-related risks the organisation is facing / may face and alerting members of the management team; and

(f) Where necessary, leading communications with AITI on personal data protection matters.

Management Oversight and Governance

3.1.4 Generally, the board and senior management of an organisation should maintain oversight and supervise the organisation's data protection practices.

3.1.5 This involves establishing a governance structure at both board and senior management levels, which may be built into the organisation's existing governance structures insofar as it is possible to do so.

3.1.6 Within such a data protection governance structure, the DPO performs an important management function. Therefore, it is generally good practice for a member of an organisation's senior management to be appointed as its DPO. Alternatively, organisations can form a DPO team comprising of the senior management representative as the main DPO with supporting roles from other relevant functions.

3.1.7 For avoidance of doubt, the role of a DPO can be performed by an individual or group of employees. Organisations can also choose to outsource the

function of the DPO function to external service providers. When the DPO function is outsourced, the organisation should still exercise adequate supervision and oversight over the outsourced DPO through a member of the organisation's senior management.

Culture of Accountability

3.1.8 Apart from establishing the appropriate governance structure, fostering a culture of accountability towards data protection is also important.

3.1.9 A culture of accountability includes data protection-related training and education for all employees and buy-in from senior management so as to create an environment of greater alertness and sensitivity to data protection issues. This is particularly important because aspects of personal data protection may be present across various functions, roles and positions in an organisation.

3.1.10 Therefore, data protection awareness should be demonstrated across all levels within the organisation (including any relevant stakeholders such as external vendors, volunteers and temporary staff).

3.1.11 Data protection education and awareness should be fostered in a top-down approach, from the management level to the employees and other relevant stakeholders. For instance, employees handling personal data (such as HR or marketing) or rolling out personal data protection measures (such as IT) should ensure that they comply with the organisation's data protection policies and processes.

3.1.12 Adequate data protection training for all employees is thus required. In this regard, data protection training should be tailored according to the job functions in the organisation. Data protection measures and topics should be integrated into staff training and communication plans.

3.1.13 Additionally, regular notices may be used to generate greater awareness. Incentives could also be provided by the organisation to encourage employees to demonstrate greater alertness to data protection issues and promote awareness of the management's support.

3.1.14 **Annex A** provides examples of training and communication initiatives that may be used by an organisation throughout the course of a typical employment journey.

3.2 Area 2: Needs Analysis and Risk Identification

Before an organisation designs its data protection policies and processes, it should identify and assess the risks through the following:

Risk Identification (Inventory Mapping and Data Protection Impact Assessments)

3.2.1 In order to identify and manage personal data at the system or operational level, and comprehensively assess the attendant risks, an organisation must first accurately identify its data assets and the data lifecycle. This can be documented in data inventory maps (as illustrated in **Annex B**) and data flow maps.

3.2.2 The type of Information that data inventory map and data flow maps should contain include:

(a) The purposes for collection, use and disclosure of personal data;
(b) The parties (e.g. internal departments or external vendors) handling the personal data;
(c) Classification of the data (to manage user access);
(d) Data retention period and how the personal data should be disposed of or anonymised.

3.2.3 Organisations should update and review their risk identification and mapping periodically and when conducting a Data Protection Impact Assessment ("DPIA").

3.2.4 When an organisation completes its data inventory map or data flow map, it may also consider establishing a risk register, which is illustrated in para 3.5. of this Guide.

Risk Identification and Assessment

3.2.5 After inventory mapping, the senior management of an organisation should understand various risks (arising from personal data and other types of data) and review them regularly basis to take into account changes in factors such as laws and regulations, technology and business models employed.

3.2.6 These risks may be broadly classified into the following four categories:

(a) **Strategic:** Risks that affect whether the organisation may meet its strategic objectives (such as its strategic plans and important targets or initiatives). Strategic risks may also affect the organisation's ability to comply with the PDPO.

(b) **Operational:** Risks that affect the organisation's operations (such as its supply chain, procurement and sales). Operational risks may also affect the organisation's ability to comply with the PDPO.

(c) **Compliance:** Risks that affect the organisation's compliance with regulatory requirements, including those under the PDPO.

(d) **Financial:** Risks that affect the organisation's financial processes (such as its accounting and reporting procedures). This may be affected by financial penalties imposed by AITI in the event of breaches of the PDPO.

3.2.7 In particular, a DPIA should be carried out at this juncture in respect of the relevant personal data flow. For example, within its data inventory, the organisation may designate the appropriate risk levels to the data identified based on the context in which it was collected, used or disclosed throughout its life cycle. In this regard, a risk matrix for assessment and implementation of suitable controls may be used.

3.2.8 This would help organisations with:

(a) Identifying the personal data handled by the particular department, system or operational process, and the purposes of collecting such data;

(b) The types of data being collected, and the classification. For example, would the data be deemed to result in significant harm under the data breach regulations or would the data otherwise be considered sensitive, and whether the data is regulated by other legislation;

(c) Identifying how the personal data moves along or is shared through the system or operational process;

(d) Identifying data protection risks by checking the handling of personal data and the data flows against PDPO requirements or best practices;

(e) Addressing the identified data protection risks by changing the system or operational process, or developing and enacting new policies; and

(f) Checking to ensure that identified risks are sufficiently mitigated before the system or process is enacted.

3.3 Area 3: Developing Data Protection Policies

Data Protection Policies and Practices

3.3.1 How an organisation designs its governance and risk management structure will influence and affect the development and implementation of its data protection policies and practices.

3.3.2 Organisations should ensure that they develop appropriate data protection policies and practices including, where appropriate, amending related corporate policies and practices which may affect compliance with its obligations under the PDPO. Examples of such policies and practices include the following:

(a) A publicly available or "external facing" data protection notice or policy ("**external data protection policy**");

(b) An internal data protection notice or policy relating to employees' personal data ("**employee data protection policy**");

(c) An internal data protection policy or handbook ("**internal data protection policy**");

(d) A security incident-response plan or data breach response plan ("**data breach plan**");

(e) Internal security policies (including related items such as data classification and confidentiality policies) ("**security policies**"); and

(f) A document retention policy ("**retention policy**").

External and Internal Data Protection Policies

3.3.3 An internal data protection policy provides internal stakeholders such as employees with clarity regarding the organisation's data protection obligations under the PDPO and the processes and practices required for its compliance. It also informs them of their roles and responsibilities in ensuring that the organisation meets its obligations under the PDPO.

3.3.4 On the other hand, an external data protection policy and an employee data protection policy informs external stakeholders (such as customers, business partners and, in the context of employee personal data, employees) of the organisation's purposes for collection, use and disclosure of personal data and its practices with respect to its obligations under the PDPO. They also help to

demonstrate how the organisation is accountable for personal data in its possession or under its control.

3.3.5 In general, the internal data protection policy must be aligned with the organisation's external data protection policy and employee data protection policy as the internal policy is, in effect, intended to aid internal stakeholders in performing their roles and responsibilities to ensure the organisation's compliance with the PDPO. For example, while an external data protection policy may set out the organisation's purposes for collection, use and disclosure of personal data, the internal data protection policy should indicate how the organisation obtains consent (if required) or fulfils the requirements of the PDPO in relation to such collection, use and disclosure of personal data.

3.3.6 The following table sets out a guide of the general points that organisations may consider when developing a data protection policy intended for its internal or external stakeholders.

Points that may be addressed in a Data Protection Policy (Internal or External)	
General	
a.	What personal data does the policy apply to?
b.	Purpose of the policy
c.	How often is the policy reviewed?
d.	How is the policy aligned with the organisation's values, business code of conduct and other corporate governance policies?
e.	Is there transparency regarding the organisation's data protection processes and practices
People	
f.	Intended audience of the policy
g.	Where the intended audience are internal stakeholders (e.g. employees), the roles and responsibilities of these stakeholders
h.	Policy owner
i.	Who is the policy approved by?
Process	
j.	Data subjects / Individuals from whom personal data is collected, used or disclosed
k.	Purposes of collecting the personal data
l.	Types of personal data that are handled
m.	Processes concerning the handling of queries, feedback, requests and disputes
n.	If applicable, the third-party organisations to whom personal data is shared with
o.	Measures to ensure that third-party organisations protect data in accordance with the PDPO requirements

p.	How the provisions of the PDPO are complied with by the organisation throughout the data life cycle
q.	Measures to protect personal data
r.	Duration of data retention and manner disposal
s.	How data incidents and breaches are handled and notified to AITI and affected individuals
t.	Situations where DPIAs are conducted
u.	How policy exceptions are to be handled

3.3.7 In addition to the types of data protection policies shown above, organisations are recommended to develop additional dedicated internal policies to address specific areas that require elaboration. For example, details on how access and correction requests from individuals ought to be handled across the organisation's departments may be set out in a separate dedicated policy.

3.3.8 The following example lists some considerations that an organisation may take into account to when developing an access and correction request handling policy.

Considerations on Handling of Access and Correction Request	
Channels to receive requests	How does the organisation intend to receive access and correction requests? In this regard, is there a standard form that individuals may use?
	How can an access or correction request be submitted to the organisation? For example, via email, post or online submission platform.
Obtaining specific information	What specific information is required so that the organisation can locate the requested personal data in a timely manner? For example, the type of personal data requested, and the date and time the personal data was provided to the organisation.
Charging access fees	With regards to access requests only, would the organisation be charging a fee to process such requests? If yes, what are the fees and are they provided in writing to the applicant?
	How would the organisation compute the access fee[1] in a way that accurately reflects the time and effort required to respond to the access request?
	Should the organisation intend to charge a fee for the access request that is higher than originally communicated to the applicant, how should the applicant be informed?

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

Response timeframe	How long would the organisation require to provide access to the requested personal data (i.e. what is the timeframe in light of the requirement for it to be as soon as reasonably possible for access requests, and the requirement for it to be as soon as practicable for correction requests)?
	How would the individual be informed if the organisation is unable to provide access / correction within 30 days?
Ascertaining identity	What procedures are established in order to verify the identity of the individual making the request? For example, proof of identity may be required from the applicant, and verification questions which may be used to establish the requestor's identity.
	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 the application of exceptions and prohibitions	When processing an access /correction request, how should they be assessed in order to determine whether any prohibitions or exceptions may apply such that access may not be provided / correction need not be carried out?
	If no correction is made despite it having been requested by an individual, how should the personal data be annotated?
Keeping records of access and correction requests	How does the organisation keep records of all access and correction requests it receives and processes? Such records may also include access requests received but not processed as they were subject to applicable exceptions.
	What is the organisation's retention policy for keeping records of access and correction requests received?

3.3.9 All of an organisation's data protection policies should be approved by its management, clearly communicated to all relevant stakeholders and reviewed regularly to ensure that they remain up-to-date.

Data Breach Management Plan

3.3.10 It is key for relevant stakeholders in an organisation to establish a sufficiently robust data breach management plan ("**DPMP**") in order to respond quickly and efficiently in the event of a personal data breach incident.

3.3.11 For avoidance of doubt, certain aspects of an organisation's data breach response may already be dealt with its existing organisational policies (e.g. IT and incident management policies and processes). Insofar as such policies do not cover processes specific to the organisation's obligations under the PDPO,

they may be supplemented by a data breach management plan, so as to enable the organisation to manage data breaches effectively and in compliance with the PDPO.

3.3.12 Organisations must notify AITI (and where applicable, affected individuals) when they have credible grounds to believe that a data breach has occurred. They must conduct an assessment to determine whether the data breach is a notifiable one within 30 days. The steps taken in relation to the organisation's data breach management plan (and other relevant organisational policies) should be documented to demonstrate that the organisation has been reasonable and expeditious in responding to a data breach.

3.3.13 As a general rule, the organisation's DPO should ensure that data incidents and breaches are recorded in an incident record log. Organisations are encouraged to actively engage their data processors and set out clearly their responsibilities with respect to reporting, investigating data breaches and rolling out remedial plans.

3.3.14 Organisations may consider having their DPMP reviewed by external parties or certified by external certification programmes. Though not necessary, doing so can help provide stakeholders greater assurance that the organisation had put in place effective data protection measures that are not only in line with the PDPO but are also comparable to industry standards.

Security, Retention and Other Relevant Corporate Policies

3.3.15 An organisation may have developed other corporate policies to ensure good corporate governance and appropriate management of its risks. For example, it may have security policies that describe and establish requirements for how the organisation protects its computer systems, networks and data. It may have retention policies that establishes minimum or maximum periods for the organisation to retain various types of documents in order to meet its legal requirements and to enable it to better manage its risks (including legal risks). Where these policies apply in relation to personal data, organisations may wish to amend their existing policies instead of establishing new policies solely for personal data. For example:

(a) An organisation may amend its security policies to explain how it has established reasonable security arrangements for the protection of personal data (as required under the PDPO); and

(b) An organisation may amend its retention policies to explain how long personal data should be retained for its various purposes.

Good Data Protection Practices

3.3.16 Organisations should ensure that internal and external parties which are engaged to process data on their behalf are continuously aware the requirement of comply with the PDPO. The table below sets out some measures that organisations may consider implementing:

Measure	What the measure applies to	Examples
State personal data protection clauses clearly in the employee agreement	Employee Agreement	• Update employment agreement with clauses setting out the employee's responsibility with respect to personal data protection
	Employee Data Protection Policy	• Such details may also be reflected in the Employee Data Protection Policy, which should be reviewed at appropriate intervals
Set clear obligations regarding how third-party organisations should manage and dispose data	Data protection clauses in third-party agreements	• Use standard contractual clauses in contracts and processing agreements with third-party organisations to ensure protection for personal data • Impose contractual obligations and provide retention schedules in contracts and data processing agreements to ensure proper disposal of personal data • Establish measures to verify the identity of third-party organisations that is granted access to the organisation's data
	Data protection clauses for cross-border personal data transfer contracts	• Use cross-border personal data transfer contracts to ensure protection for personal data
Conduct regular reviews of contracts with third-party service providers	Due diligence on third-party service providers	• Conduct due diligence of the personal data protection and processes of service vendors / third-party organisations (such as request for an independent audit report and random checks)

3.4 Area 4: Implementation of Data Protection Processes and Control

3.4.1 When an organisation designs its data protection policies, appropriate processes and controls (including internal and external communication of policies and staff training) will also need to be put in place to address identified risks, as mentioned in Para 3.2 of the Guide. The identified risks should be mitigated by employing the appropriate controls, including the monitoring of residual or ad-hoc risks.

Systems-based and Process Controls

3.4.2 Based on the risks identified, organisations can subsequently implement suitable system-based and process controls to address such risks. For instance, a data inventory map, data flow map and risk register may help to identify where sensitive data is located in an organisation's internal systems. Accordingly, the organisation is better able to ascertain the appropriate level of technical security measures to be put in place and the design an appropriate access management system for such data. The controls adopted by an organisation should be tailored to the risk level and nature of the personal data, and should include both digital and non-digital solutions.

3.4.3 The security risks may be identified by considering the CIA triad, a widely-used model to guide information security:

(a) **Confidentiality:** Risk arising from unauthorised or inappropriate disclosure of information. In order for information to be considered confidential, the organisation must have made efforts to restrict access to the information to prevent such unauthorised disclosure.

(b) **Integrity:** Risk to information quality and trustworthiness, or risk of corruption. Information needs to be as accurate, reliable and be free from tampering in order to be useful.

(c) **Availability:** Risk of information not being available to intended users. Information must be available when it is needed by the intended users and in an accessible form in order to be useful.

Data Protection by Design

3.4.4 In order to integrate data protection policies into business and operational processes, one method organisations may use is to adopt a Data Protection by Design ("**DPbD**") approach. This means that personal data protection is considered right from the earliest design stage of any project (e.g. when developing systems), and throughout the rest of the operational life cycle of

the project. This helps to identify data protection issues early on in project development and reduce unnecessary delays and costs of having to modify data protection features afterwards.

Service Vendor Management

3.4.5 Organisations should ensure that they communicate their data protection requirements to their external service vendors or data processors clearly. Under the PDPO, data processors are responsible for complying with the obligations in relation to protection, retention and cross-border transfers of personal data and aspects of data breach notification.

3.4.6 As such, organisations should ensure that it puts in place a binding contractual agreement that states the parties' respective responsibilities with regards to the processing of the personal data. Where data is transferred internationally, such transfers should also be carried in compliance with the PDPO.

Communicate Policies to Customers

3.4.7 Organisations should also ensure they communicate data protection policies and practices clearly and transparently to their customers. In this regard, organisations may consider the following:

(a) Publishing policies and other information in simple, plain language and place them in prominent locations that are easily accessible by customers.

(b) Ensuring that customers understand what they are consenting to throughout their user journey. This may be done by providing concise consent clauses at appropriate touchpoints.

(c) Managing customer relationships through clear communications so that customers may be kept abreast of any policy updates. Such communications should be separated from marketing messages (which require prior express, opt-in consent).

(d) Ensuring that customer-facing staff possess adequate knowledge and sensitivity to handle data protection feedback and queries and complaints. In this regard, there should also be appropriate channels and processes for handling customer complaint.

(e) Establishing accessible channels and efficient processes for handling customers' access and correction requests.

3.5 Area 5: Operations and Data Protection Risk Monitoring

Operations: Establishing Relevant Registers

3.5.1 At the outset, after an organisation identifies its risks, organisations may consider establishing a risk register. The register should identify the risks associated with the nature of the organisation's personal data and the context in which it is used. Organisations should also consider existing whitelists of data which may be subject to stricter regulation, which can be determined internally and applicable regulations.

3.5.2 Organisations are also encouraged to create a consent register to record consent given by individuals to the organisation for the collection, use and disclosure of their personal data for a particular purpose. The register could be used by the organisation to demonstrate that an individual had provided consent in the event of disputes or for verification purposes. The organisation may also be better able to monitor whether consent has been provided and/or withdrawn by an individual. Organisations should ensure that its consent register is up to date, in particular, when there may be revisions to its consent clauses. When there are changes an organisation's consent clauses, the scope of consent provided should be clearly recorded in the consent register (i.e. what is permitted for each version of the clause) along with the version of the consent clause that each individual had agreed to.

3.5.3 The registers should be updated and reviewed periodically, and when conducting a DPIA.

Risk Monitoring and Reporting

3.5.4 All risks, especially residual risks, should be monitored by organisations via regular reporting within the organisation's governance structure and through operational monitoring and reporting (such as through management reports). In this regard, the organisation's DPO should ensure that regular monitoring of identified risks is carried out and that data incidents and remediation measures are reported to the relevant authority. Organisations may wish to ensure that various feedback is provided at appropriate intervals of time by working level to senior management. The table below sets out some examples for consideration.

Frequency	Possible areas for feedback
Quarterly	• Changes to the organisation's personal data protection policies and practices • Results of DPIAs conducted and remedial plans • Status of or updates to identified risks, risk ratings and remedial plans • Emerging risks, risk ratings and remedial plans identified over the past quarter • Plans for data protection audits • Other important data protection issues, if any
Annually	• Personal data protection risk profile for the year • Summary of risk remediation plans and strategy

3.5.5 Overall, appropriate monitoring systems should be established to monitor occurrence of residual or ad-hoc risks, and internal reporting processes be put in place (e.g. data breach management plans can help with breach monitoring and management). Organisations should carry out periodic audits to ensure that all identified risks are addressed across time.

3.5.6 AITI highlights that organisations should ensure that they are able to demonstrate that they have in place accountability practices (e.g. monitoring processes and remediation plans). This may allow the organisation to qualify for the option of providing a voluntary undertaking in the case of a data breach, allowing for a better outcome compared to a full investigation being carried out by AITI.

3.6 Area 6: Review and Maintenance

Reviewing Data Protection Policies and Practices

3.6.1 Once data protection policies and practices are established, organisations should ensure that they are reviewed to ensure that they are up-to-date and tailored to their changing data protection practices and gaps, technological advancements and legislative changes. Where identified, gaps should be remedied and this should be supervised by the board and senior management. This helps to ensure that the organisation's risks continue to be managed effectively over time.

3.6.2 For example, the following types of review may be conducted on a periodic basis:

(a) Revising data protection policies and processes at specified time intervals.

(b) Batch review of minor incident occurrences (such as accidental disclosure of personal data to unauthorised employee and improper disposal of personal data).

(c) Revising systems or processes with a low level of impact on data protection (such as a change in the DPO's business contact information or email address for receiving access and correction requests).

3.6.3 Ad-hoc reviews such as the following should also be considered:

(a) Review of major incident occurrences (e.g. data breach incident affecting customers).

(b) Recent legislative and regulatory amendments.

(c) Occurrence of changes to the organisation (such as corporate restructuring, mergers and acquisitions, and changes to operations and processes).

3.6.4 When there are notable changes, organisations should conduct a DPIA to help identify, assess and address data protection risks that may emerge.

Establish an Audit Framework

3.6.5 Organisations are encouraged to a risk reporting and internal audit framework. This can help provide greater clarity regarding how they can manage personal data protection risks.

3.6.6 Their audit framework may provide for the following:

(a) Conducting an internal audit on a periodic basis.

(b) Conducting an ad-hoc inspections.

(c) Engaging an external service provider to evaluate implementation.

Monitor External and Internal Environment

3.6.7 To stay aware of changes and developments that take place within and outside the organisation, organisations may consider the following areas for monitoring:

	External Environment	Internal Environment
What to monitor?	• Amendments to the PDPO and subsidiary regulations issued thereunder. • Changes to sector-specific regulations. • New resources provided by AITI. • Data breaches that take place in other organisations. • Industry data protection best practices. • Newly-emerging technologies that may affect data protection risks.	• Systems or processes involving personal data that are either newly implemented or undergoing major changes. • New business engagement strategy or business model (or major changes thereto). • Feedback from internal and external stakeholders. • Data incidents and data breaches.
How to monitor?	• Subscribe to news reporting services to stay up-to-date on relevant legislative and regulatory developments. • Attend data protection conferences and training. • Subscribe to news reporting research and developments in the field of data protection.	• Conduct DPIAs on systems and processes involving personal data that are intended to be rolled out or to undergo major changes. • Assess the level of general data protection awareness and understanding of employees or obtain their feedback regarding the organisation's data protection practices. • Review feedback received from customers regarding the organisation's data protection practices.

Notify stakeholders regarding changes to Data Protection Policies and Practices

3.6.8 Organisations should keep its stakeholders updated regarding changes to their data protection policies or practices. In this regard, an organisation's data protection policies and practices should be made easily accessible to stakeholders such as through the following means:

(a) Update the information onto the organisation's website and push updates to customers through emails, newsletters or other CRM channels.

(b) Making such policies and practices available on the organisation's staff repository and sending regular staff update emails.

(c) Work with third-party organisations to ensure that the latter's staff who are handling the organisation's personal data are also adequately informed.

[END]

Annex A: Illustration on Training and Communication Initiatives in a Typical Employment Journey

	Training	Communication Initiatives	Target Staff
On-boarding	Briefing on the fundamentals of the PDPO	Access to the staff repository of data protection-related policies and processes	All staff
Assigned job scope	Thorough training on organisation's data protection processes		Staff handling personal data (e.g. IT, HR and Sales)
Change in job scope	Thorough training on specific data protection process, where required		
Ongoing	Refresher on PDPO fundamentals Briefings on specific data protection policies and processes, where required	Reminders and circulars regarding data protection policies and processes Update regarding changes to data protection policy on processes	All staff
Promotion	Thorough training on specific data protection process, where required		Staff with greater responsibility for data protection
Exit		Reminders regarding requirements for proper handling of personal data upon exit (such as proposal disposal)	Staff exiting the organisation

Annex B: Illustration of a Data Inventory Map

Data Inventory Map						
Part 1: Source, Location and Type of Personal Data						
No.	Database Name	Data Owner	Data Subject	Types of Personal Data	Storage Location	Security Measures
Part 2: Collection and Use of Personal Data						
	Purposes of Collection and Use	Legal Basis	Time and manner of collection	Other Data Users	Whether copies are made	Location of Copies
Part 3: Disclosure of Personal Data						
	External Recipients	Purpose of Disclosure	Legal Basis	Time and Manner of disclosure	Where transfer is overseas	
Part 4: Retention and Disposal of Personal Data						
	Retention Period	Disposal Method	Anonymisation of data	Department retaining anonymised data	Remarks (if any)	