AITI Authority for Infocommunications Technology Industry of Brunei Darussalam

PERSONAL DATA PROTECTION ESSENTIALS INFOKIT

January 2026 | Version 1.0

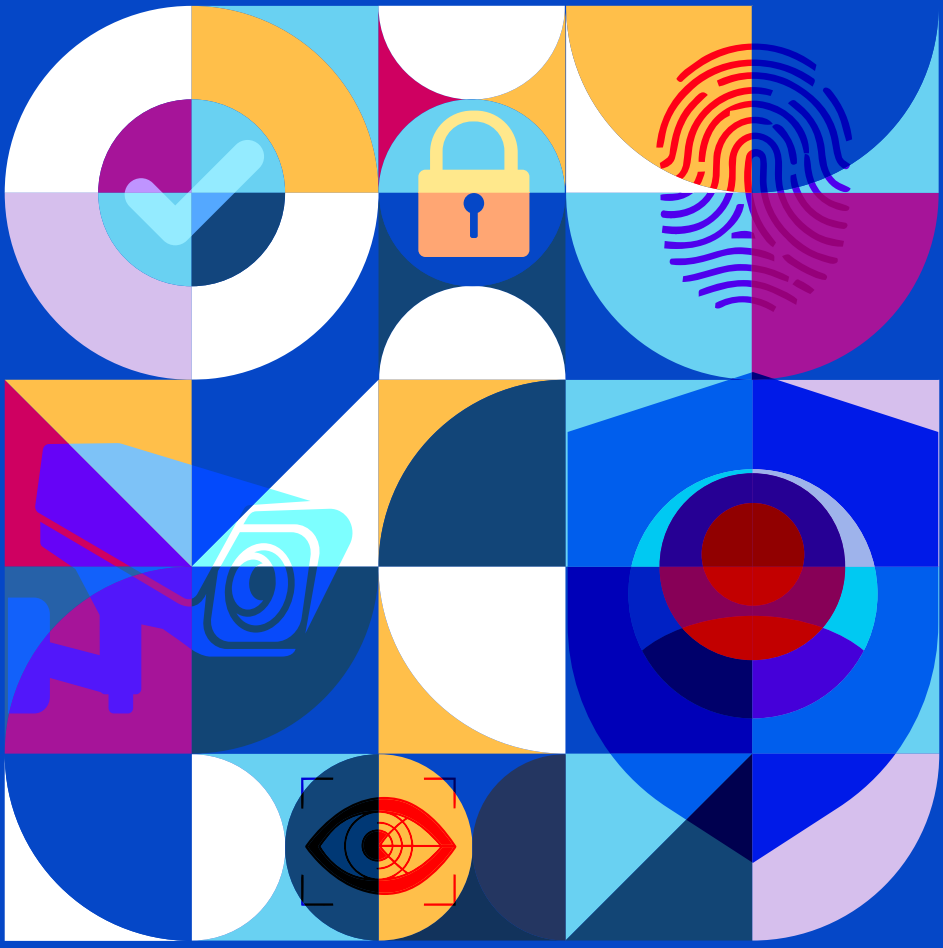


Table of Contents

About

The Personal Data Protection Essentials Infokit has been developed by the Authority for Infocommunications Technology Industry of Brunei Darussalam (AITI) to provide a practical guide for organisations to hold accountability in the personal data entrusted to them.

This Infokit contains information on how organisations can take reasonable steps to ensure appropriate personal data protection policies, processes and practices are implemented with considerations of **the five (5) essential steps.**

It includes general guidance in the form of illustrations, checklists, sample clauses and notices, based on frequently asked questions arising from industry engagement and general enquiries.

NOTE: The tools provided in this Infokit serve as a basic guide and are for illustrative purposes only. Organisations intending to use the tools should assess its own data protection lifecycle and customise it according to its business needs.

Personal Data Protection Order, 2025

The Personal Data Protection Order, 2025 (PDPO) aims to govern private sector organisations' collection, use, disclosure and processing of personal data of individuals, such as their employees or customers.

Identification Card

Passport

Mobile Number

Thumbprint

Home Address

CCTV Image

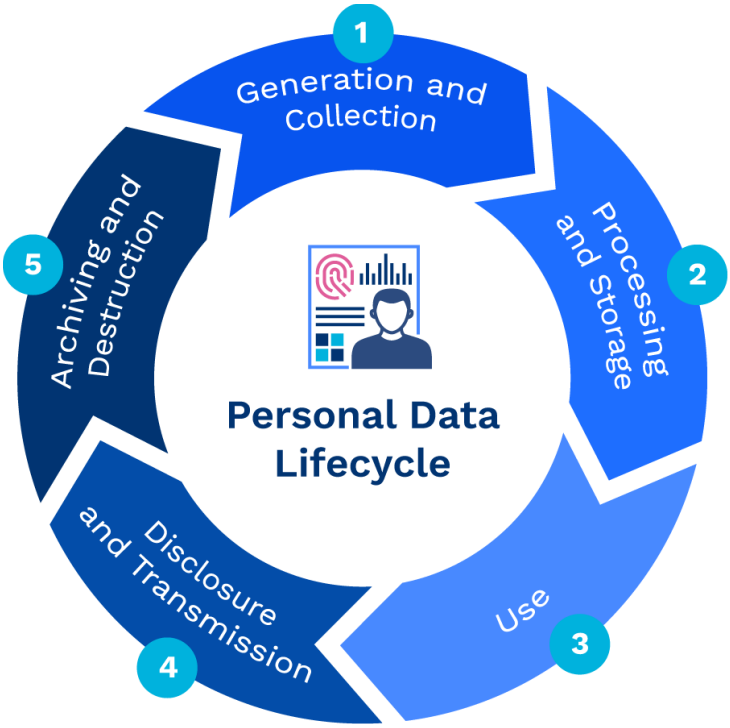
The Role of the Authority

AITI

Authority for Infocommunications Technology Industry of Brunei Darussalam

Authority for Infocommunications Technology Industry of Brunei Darussalam (AITI) is the Authority that administers and enforces the PDPO.

Personal Data Lifecycle



The flows of personal data generally begin from individuals as data subjects sharing their personal data to the organisation requesting for it. The management of personal data continues with the relevant organisation(s) concerned, either as the **data controller** and/or as **data processor**.

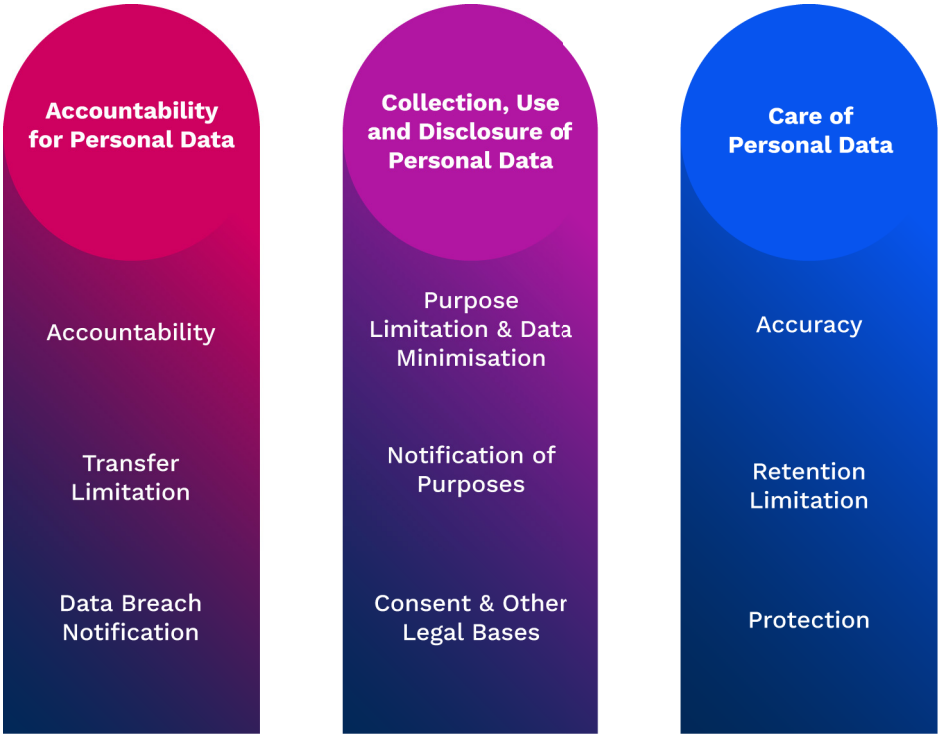
Data Controller: Organisations which have **direct control** over the means and purposes for processing of the personal data.

Data Processor: Organisations which **process personal data on behalf of** another organisation or a public agency.

Data Protection Obligations

In general, the PDPO confers upon private sector organisations obligations through the following data protection provisions:

- **Accountability of Personal Data:** Organisations must hold accountability for the personal data entrusted to them.
- **Collection, Use and Disclosure:** Organisations should limit such activities based on what is reasonable and appropriate.
- **Care of Personal Data:** Organisations must take reasonable steps to protect personal data and retain only when necessary.



5 ESSENTIAL STEPS TO GET STARTED

STEP 1:

Demonstrate Accountability

STEP 2:

Document Data Flows

STEP 3:

Develop Data Protection Policies and Practices

STEP 4:

Establish Appropriate Processes and Controls

STEP 5:

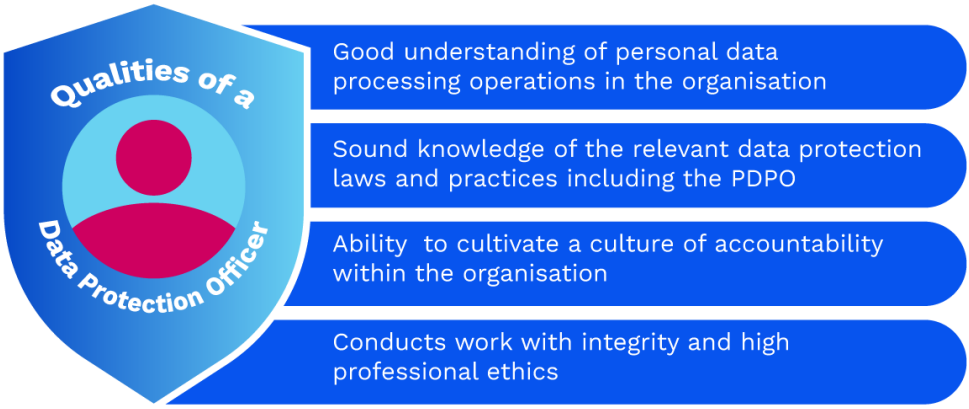
Respond to Individuals Effectively

STEP 1
DEMONSTRATE ACCOUNTABILITY

Organisations must be able to take responsibility for the management of personal data entrusted to them. This can be done by ensuring all employees are informed on their roles in safeguarding personal data and that data protection policies, processes and practices are in place.

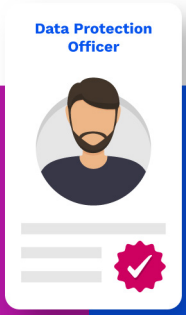
A crucial step to demonstrate accountability would be through the appointment of a **Data Protection Officer (DPO)**. The DPO plays an important role in **facilitating compliance to the PDPO** and in setting the tone for the overall management of personal data.

Organisations should assess the suitability of a DPO candidate in accordance to the **complexity of its operations within the personal data lifecycle.**



Note: Organisations may appoint an existing employee or new hire or outsource the function to an external entity altogether. Larger organisations may also find it suitable to appoint more than one individual to form a DPO team.

Upon appointment of the DPO, organisations should brief the individual of the roles and responsibilities in order to facilitate assessment on data protection matters.



Expectations on Organisations

1. Empower the DPO with clear roles and responsibilities, including developing and/or updating data protection policies and practices.
2. Provide training to the DPO to be able to perform their roles and responsibilities.
3. Inform all staff on the business contact information of the appointed DPO and their role in PDP-related queries and complaints.
4. Ensure the DPO communicates and coordinates with relevant staff and third-party organisation on data protection matters.

Expectations from the Authority

1. Inform AITI on the appointed DPO's business contact information.
2. Publish data protection policies and make business contact information available publicly.
3. Represent the organisation in AITI's stakeholder consultation and events.
4. Facilitate data breach incident reports and investigation.

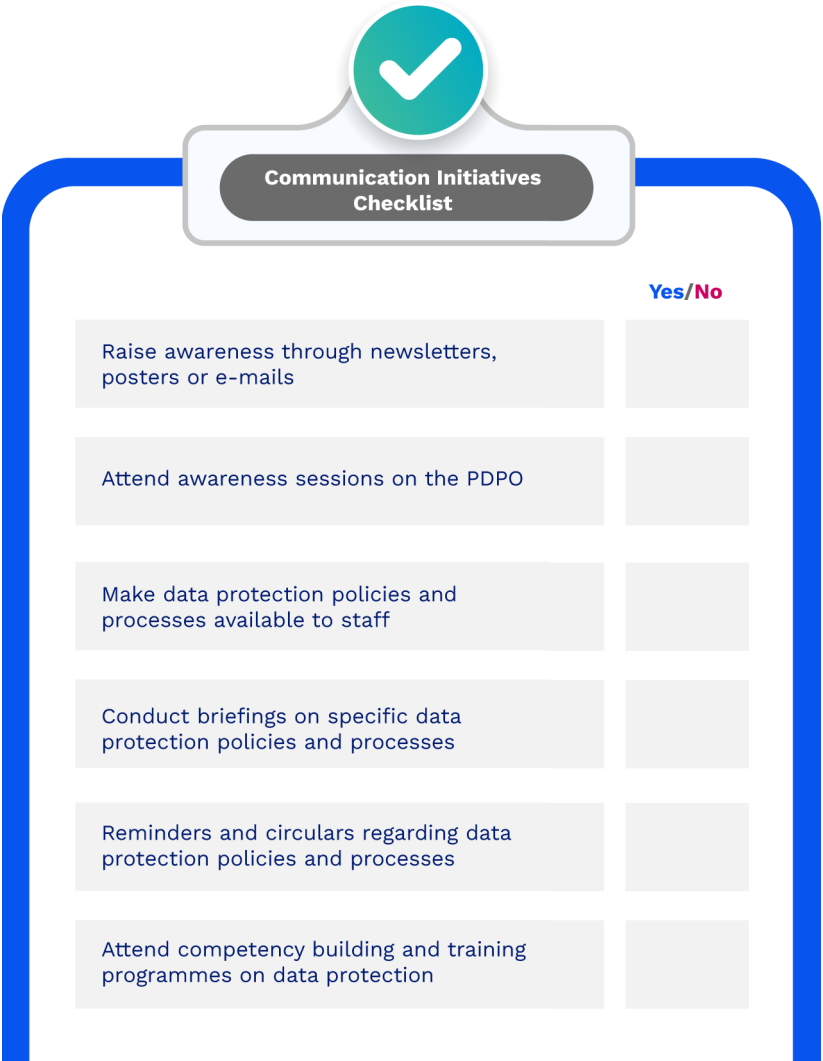
NOTE: The responsibility for complying to the PDPO still remains with the organisation and is not transferred to the appointed DPO.

For more information, refer to AITI's Guide on Appointment of Data Protection Officers.

Illustration on Accountability - Communicating Data Protection Policies, Processes and Practices

Organisations should ensure its employees possess adequate knowledge to handle data protection matters through appropriate channels and processes.

This can be facilitated by the DPO, whereby communication initiatives can be tailored based on the job scopes of the employees in attendance.



STEP 2

DOCUMENT DATA FLOWS

Organisations should aim to **identify the types of personal data** it processes, **document the flows** of the personal data lifecycle of any systems or processes and **assess the potential risks**. Upon completing such activities, organisations can rectify any data protection gaps or implement suitable controls, where necessary. The DPO may facilitate this by coordinating with the relevant project managers.

General Considerations When Documenting Data Flows
Types of personal data collected
Purposes for collection, use and disclosure
How/where personal data is collected (source)?
Where personal data is stored (including copies)?
Who uses or has access to the personal data?
Parties to whom the personal data is disclosed/transferred
Mode of overseas transfer (if any)
How long personal data is retained/archived?
How personal data will be disposed?
Who is responsible to ensure compliance at each stage?

Illustration on Data Inventory Map

A Data Inventory Map can guide organisations in mapping their data assets and capture the flow of personal data within the data lifecycle of a system or process. This would begin from the collection of personal data to its deletion or disposal. It includes noting the roles and responsibilities of assigned staff involved in managing personal data, including internal departments and external third-party organisations.

Steps		Sample Data Inventory Map [For illustration purposes only]		
1	**Source, Location and Type of Personal Data**	**Data Owner**	**Data Subject**	**Types of Personal Data**
		ProjectTeam_HR, Organisation A	Applicant 1 to Applicant 50	Full name, IC number, Contact number, Date of birth
2	**Collection and Use of Personal Data**	**Purposes of Collection and Use**	**Legal Basis**	**Time and Manner of Collection**
		Interview and Hiring for Marketing Role	Consent	Upon submission of job application form
3	**Disclosure of Personal Data**	**Other Recipients**	**Purpose of Disclosure**	**Time and Manner of Disclosure**
		Officer A (Marketing Dept) and Officer B (Business Dept)	To assess candidates for interview of Marketing Role	Upon shortlisting of suitable candidates
4	**Retention and Disposal of Personal Data**	**Retention Period**	**Anonymisation of Data**	**Department Retaining Anonymised Data**
		Retain successful candidate's data	Anonymisation of unsuccessful candidates' data	Retain anonymised data for internal statistics

Illustration on Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) can guide organisations in reviewing various data protection risks arising within the personal data lifecycle. This can be assessed periodically by identifying the risks and taking measures to mitigate these risks such as changing the system or operational process.

Sample Data Protection Impact Assessment
[For illustration purposes only]

STEP 1 Identify the Need for a DPIA	Organisation B has deployed an online recruitment management system for job applications in the past month. It has the personal data of 500 individuals. The purpose of the system is to interview potential candidates to fill in the open roles in the organisation. It includes processing personal data of new graduates and experienced professionals.
STEP 2 Describe the Data Processing Involved	The types of personal data processed include information requested from the job application form such as Full Name, Contact Number, IC Number, Date of Birth and CV. The collection of personal data begins upon the submission of the form. Upon shortlisting of potential candidates, the personal data of the applicant will be disclosed to the interview panel. Only successful candidates' personal data will be retained for employment purposes.
STEP 3 Assess compliance measures and necessity	The processing of personal data is required to select the appropriate candidate for the interview process and this is stated in the privacy policy. The organisation has taken steps towards data minimisation on the application form by placing the required fields (*) to be filled for the necessary information only.
STEP 4 Identify and Assess Risks	A potential harm includes the lack of clarity on access controls and the authorised personnel for the project. A data breach resulting in the lack of such measures can cause significant harm to individuals and damage to reputation of the organisation.
STEP 5 Identify measures to reduce or mitigate risk	To reduce such risks, Organisation B has taken steps to hold accountability by laying out appropriate processes and controls such as (i) set clear roles and responsibilities of the project team members and (ii) restrict the disclosure to specified authorised personnel only.

For more information, refer to AITI's Template on DPIA and Guide on Developing a Data Protection Management Programme.

STEP 3

DEVELOP DATA PROTECTION POLICIES AND PRACTICES

Upon capturing the flows of personal data and/or assessing the risks of processing such personal data, organisations should ensure appropriate internal and external data protection policies and practices are in place. The DPO may facilitate this with relevant teams within the organisation and ensure it will be communicated effectively upon publishing.

General Considerations of Data Protection Policy

What is the purpose of the policy?	Who is the intended audience of the policy?
What types of personal data are collected, used, disclosed and processed?	Are there processes concerning the handling of queries, feedback, access request and disputes?
What is the duration of data retention or manner of disposal?	How will data incidents and breaches be handled?
Are there measures to ensure third-party organisations protect personal data?	How will data incidents and breaches be handled?
How will the organisation notify AITI and/or affected individuals in the event of a data breach?	How often is the policy reviewed?

Organisations should consider publishing policies in simple language, ensuring they are easily accessible and designed to help individuals understand what they are consenting to.

Illustration of External Data Protection Policy

An External Data Protection Policy provides clarity regarding the organisation's purposes for collection, use and disclosure of personal data **for external stakeholders** such as customers and business partners.

Sample Data Protection Policy [For illustration purposes only]		
No.	**Content**	**Remarks**
1	General Disclaimer	*Organisation C ("we") collects, uses, discloses and processes personal data in accordance with the Personal Data Protection Order 2025 ("PDPO"). This Policy explains how we process personal data while meeting the requirements of the PDPO*
2	Types of personal data collected	*We may collect the following types of personal data about you when reasonably required for any of the following purposes specified in this Policy: (a) Full Name, (b) Mobile Number, (c) Home Address*
3	Methods of collection of personal data	*We may collect personal data about you when you purchase a product from us on our website*
4	Purpose of collection and use of personal data	*We may collect and use your personal data to provide the product you have ordered from our website*
5	Purpose of disclosure of personal data	*We may disclose your personal where reasonably required for any of the purposes specified to third party service providers*
6	How the personal data is protected	*We shall protect personal data in our possession or under our control by making reasonable security arrangements to prevent loss, unauthorised access, collection, use and disclosure, copying, modification, disposal or similar risks.* *We will ensure that any transfers of personal data outside of Brunei is protected to a standard or protection that is comparable to the PDPO*
7	Amendments	*We may amend or update this Policy from time to time. You may refer to our website (at https://OrganisationC.com.bn/dppolicy) for the latest version*
8	Information about the DPO	*Any queries, requests for access to or correction of personal data, withdrawal of consent and complaints relating to your personal data may be sent to us to [The Data Protection Officer] at dpo@OrganisationC.com.bn*
9	Date Issued	*27 January 2026*

For more information, refer to AITI's Template on Data Protection Policy.

Illustration on Consent Clauses for Registration Forms

For Organisations offering Membership Applications

Sample Consent Clause for Membership Form

By submitting this form, you agree that Organisation D may collect, use and disclose personal data for the following purposes in accordance to the Personal Data Protection Order, 2025 and our data protection policy (https://OrganisationD.com.bn/dppolicy):

1. The processing of the membership
2. The administration of the membership

Name: _____

Signature: _____

Date: _____

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

For Organisations Conducting Lucky Draw

Sample Consent Clause for Lucky Draw

By submitting this form, you agree that Organisation E may collect, use and disclose your personal data for the following purposes in accordance with the Personal Data Protection Order, 2025 and Organisation E's data protection policy (https://OrganisationE.com.bn/dppolicy):

1. To contact you and verify your identity for the administration of prizes in relation to the lucky draw.

Name:_____ Mobile Number: _____

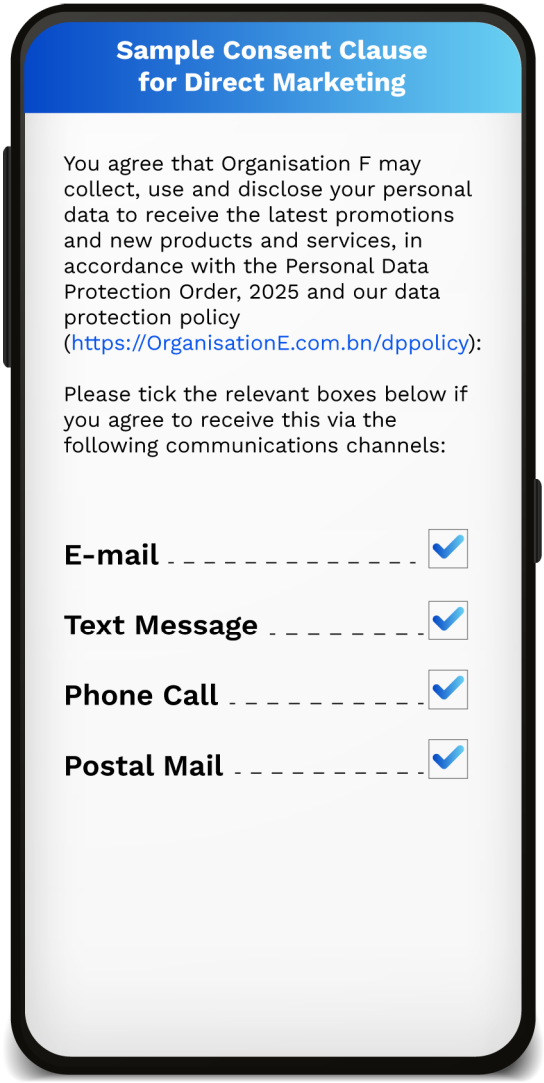
Last three (3) Digits of IC: _____ Date: _____

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

TIP: When collecting personal data, organisations should consider principles of data minimisation and only request for personal data that is necessary in order to provide the product or service.

Illustration on Consent Clauses for Direct Marketing

For Organisations which would like to send customers Marketing Materials.



TIP: Organisations should in general obtain express consent from individuals to receive any direct marketing messages and provide the means to opt-into receiving such messages. This is typically presented with check boxes.

Illustration of Notices for Photography, Video and CCTV Recording

Informing individuals when photography, video, and audio recording will occur at an event the organisation is hosting.

Sample Personal Data Protection Notice for Events

Such notice can also be stated early on at the registration form.

Informing individuals when closed-circuit televisions (CCTVs) are in place to monitor the organisation's premises and recording image of visitors.

Sample Personal Data Protection Notice for CCTV Use

These notices should state the purpose of CCTV usage, be clearly printed and placed in areas that are easily visible.

Illustration on Internal Data Protection Policy – Processing of Individuals Access Request

An Internal Data Protection Policy provides clarity regarding the organisation's data protection obligations under the PDPO **for internal stakeholders** (such as permanent and temporary employees) and elaborates on their roles and responsibilities on data protection process and practices.

Sample of Organisations Handling Access Requests
[For illustration purposes only]

No.	Considerations	Sample Process
1	Channel to receive requests	*The request of access of customers personal data will be facilitated by the DPO and it can be done by signing in the individual's account at (https://www.OrganisationG.com.bn/User) and submitting the request form or by e-mail at dpo@OrganisationG.com.bn*
2	Charging Access Fee	*The general fee for the request of access is published on the official website and upon the acknowledgement e-mail to the individual.*
3	Ascertaining Identity	*To verify the validity of request and individual's identity, the individual will take steps to answer a set of security questions.*
4	Response timeframe	*The DPO will acknowledge the request of access within three (3) working days.* *Upon payment of the access fee, the DPO will facilitate such requests with the relevant project team and provide the information within thirty (30) working days, unless any exception applies.*
5	Obtaining specific information	*The DPO will inform the relevant project team, who will locate the requested personal data (where appropriate) and facilitate in producing a summary report based on the personal data requested.*
6	Keeping records of access and correction requests	*The DPO will keep records of all access request it receives and/or processes.*

Illustration on Data Breach Response Plan

A Data Breach Response Plan provides clarity regarding the measures which the organisation will take in order to respond quickly and effectively in the event of a personal data breach incident and its notification to AITI. The DPO can facilitate the implementation of the plan alongside a project team consisting of relevant departments.

General Considerations of a Personal Data Breach Response Plan
[For illustration purposes only]

1 Contain the data breach

Upon detection of confirmed personal data breach within Organisation H's system, the DPO is notified immediately and conducts initial appraisal with the relevant project team detailing (i) cause of the data breach, (ii) number of affected individuals, (iii) types of personal data involved (iv) affected systems and (v) remediation action(s).

The DPO will facilitate the recording of the details of the data breach in an Incident Record Log.

2 Assess and determine if it is a notifiable data breach

Upon containment of the data breach, the organisation must conduct an in-depth assessment on the success of its containment action(s) taken, the effectiveness of any technological protection and determine if it is a notifiable data breach within 30 (thirty) days.

The DPO will facilitate organisation's assessment such as detailing the (i) context of data breach, (ii) ease of identifying individuals from the compromised data and (iii) circumstances of the data breach.

3 Report to AITI and/or the affected individuals

Upon organisation's assessment that it meets the threshold of a notifiable breach under the PDPO, the DPO will submit the data breach report and any supporting documents to AITI through the online form provided.

Depending on the context of the data breach, the organisation will also report to other authorities and/or directly to the affected individual, where relevant.

4 Evaluate response to the data breach

The DPO and the relevant project team continues to review its personal data handling practices to prevent the recurrence of similar data breaches.

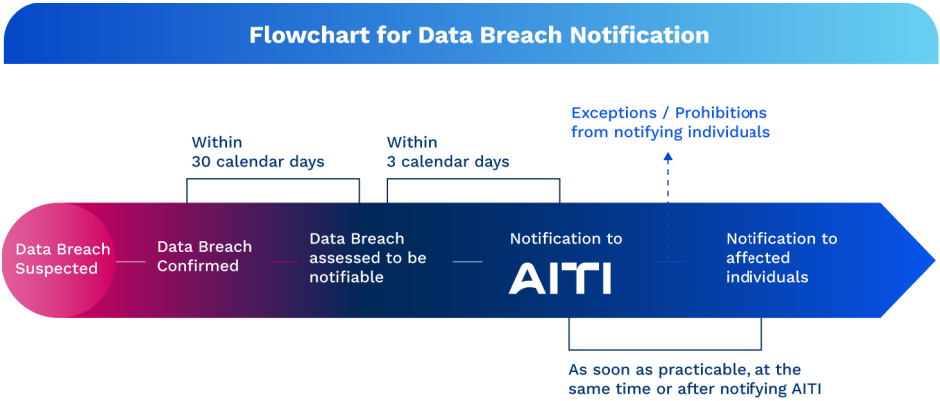
Periodic reviews of existing procedures will be done to reflect the lessons learnt and recommendations of training requirements to respond or prevent breaches effectively.

NOTE: Organisations may have security policies in place which describe and establish requirements for how the organisation protects its computer systems, networks and data. Such policies can be amended to include the Data Breach Response Plan to incorporate how the organisation protects personal data.

Illustration on Data Breach Notification to AITI

Where an organisation has reason to believe that a data breach has occurred, the organisation must conduct an assessment on whether it is a notifiable data breach to AITI within thirty (30) days.

Upon determining that a data breach is notifiable, the organisations must notify AITI within three (3) days and to the affected individuals, where reasonable.



Organisations must provide to AITI information such as the facts of the data breach, data breach assessment, contact details of the DPO and any supporting documents on the Data Breach Notification form provided on https://pdp.aiti.gov.bn

NOTE: Data Processors should notify the relevant organisation from the time it has credible grounds to believe that a data breach has occurred. The organisation engaging the data processor remains responsible to notify AITI and/or affected individuals.

Voluntary Undertaking

Upon submitting the data breach notification form, organisations may request to invoke a voluntary undertaking to AITI as an opportunity to demonstrate that it has existing accountable policies and practices in place and show commitment to implement their remediation plan in relation to the incident within a specified time.

General Considerations of Voluntary Undertaking

- Describing the incident which the organisation is involved in.
- Measures the organisation will take to rectify the cause(s) of the incident within a specified time.
- Measures to reduce recurrence of the incident and putting in place appropriate policies and processes.
- A remediation plan detailing how compliance of the PDPO may be achieved in relation to the incident.
- Acknowledgment that the voluntary undertaking may be published by AITI.
- Acknowledgment to provide related reports to AITI, when requested.

NOTE: Where organisations do not comply with the terms of its voluntary undertaking, AITI will resume with full investigations of the incident and/or impose any other enforcement outcome it deems fit.

For more information, refer to AITI's Template on Incident Record Log and Advisory Guidelines on Key Concepts of the PDPO.

STEP 4
ESTABLISH APPROPRIATE PROCESSES AND CONTROLS

Human error remains one of the biggest causes of data breach whereby the organisation has not established clear processes and controls for its employees or third-party personnel, leading to unrestricted access or misuse, jeopardising its security posture.

Some common cybersecurity attacks include:

Phishing

Cybercriminals posing as legitimate representatives of reputable organisations with the intent to trick employees into disclosing personal data resulting in data breach, identity theft and financial loss. Tactics include lucrative statements and sense of urgency through fake calls, SMS and e-mail.

Malware

Cybercriminals deceiving employees with the intent to infiltrate and infect computers to compromise device, disrupt service, steal data or monitor user activities. Tactics include viruses, ransomware and spyware through malicious links and documents.

Denial-of-Service (DoS) Attack

Cybercriminals disrupting a network's service to make it unavailable to its intended and legitimate users. Tactics include flooding the network with useless traffic until it overwhelms the resources and crashes the system through the exploitation of vulnerable devices.

Organisations should take reasonable steps to address any identified data protection risks and mitigate it through appropriate process and controls.

It should conduct due diligence and review its processes and controls regularly within the organisation and any third party organisations involved. The DPO may facilitate this with relevant teams within the organisation and ensure it will be communicated effectively once established.

General Considerations of Establishing Appropriate Processes and Controls

Standard Operating Procedures (SOPs)

Establish relevant procedures for the secured processing of any personal data and monitor its compliance to the PDPO by ensuring reasonable security measures are in place to prevent any unauthorised access or misuse.

Legally Enforceable Mechanisms

Ensure data protection requirements are clearly communicated and documented. Any transfers of personal data should be bound by written agreements which covers sufficient measures to comply with any applicable data protection laws.

Illustration on Data Protection Processes – Access Controls

In order to ensure that personal data stored can only be accessed by authorised persons, organisations must implement authentication and authorisation processes in ICT systems. As good practice, organisations should **set appropriate access control rules, access rights and restrictions for specific user roles.**

General Considerations of Access Controls through Authentication
[For illustration purposes only]

No.	Authentication	Example
1	Determine a suitable authentication method for accessing personal data based on the risk to the individual in case of a data breach.	*Organisation J uses multi-factor authentication to access personal data that is considered sensitive.*
2	Determine a suitable maximum number of attempts allowed for a user to authenticate his or her identity based on the type of data to be accessed.	*The organisation determined that the assigned staff can have a maximum number of two (2) attempts to authenticate their identity for the access of personal data that is considered sensitive.*
3	Implement account lockout when the maximum number of attempts is reached.	*At the third attempt, it sets controls to lock the accounts to prevent any dictionary or brute-force attacks.*
4	Update any default passwords set at the earliest possible opportunity.	*All staff are advised to update any default password as soon as possible.*
5	Ensure strong passwords are used for authentication and has a length of at least 8 characters.	*All staff are advised to create strong passwords containing at least 1 numeric character, 1 uppercase character and 1 special character.*
6	Password used for authentication is encrypted or hashed, where relevant.	*Organisation J encrypts all passwords during its transmission and storage.*
7	Frequent update of passwords based on the risk of access to the type of data.	*The assigned staff will be asked to change their password every three (3) months to access personal data that is considered sensitive.*
8	Discourage users from using the same password across different systems or applications.	*All staff are advised not to use the same password for all systems.*

General Considerations of Access Controls through Authorisation
[For illustration purposes only]

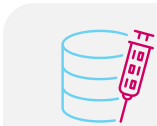
No.	Authorisation	Example
1	Implement authorisation mechanisms and processes to ensure the person accessing the system has appropriate access rights to data requested within the system.	*Organisation K designated only selected assigned staff to have the appropriate access rights to the system with personal data that is considered sensitive.*
2	Define user roles or groups for systems that enable access rights to personal data.	*The organisation clearly defines access rights for the selected assigned staff and their role in relation to the data.*
3	Grant a user only the necessary access rights to personal data within systems to fulfil their role or function.	*It ensures the selected assigned staff only has access to the necessary personal data based on their roles.*
4	Track and review usage of accounts and their associated access rights regularly.	*It regularly reviews the usage of accounts of selected assigned staff and associated access rights. It has removed access of one (1) staff upon their transfer to a different role within the organisation.*
5	Implement anti-password sharing policies.	*All staff are advised to conduct due diligence in managing their passwords and to not store passwords in public web folders or on display at their desks.*
6	Log all successful and failed access to system.	*Organisation K documents all logins on the system to detect any unauthorised attempts to gain access to them.*

For more information, refer to AITI's Guide to Data Protection Measures.

General Considerations on Security Measures for Databases, Websites and Web Applications

When selecting a database product, organisations should consider their security requirements as different database products tend to have different security features. It should consider identifying the types of personal data to be stored and the risk of adverse impact to the individual if such data was compromised.

Some **common form of attacks** on databases on website and web applications include:



SQL Injection Attacks

Cybercriminals sending malicious database instructions as users input from a website or web application to database, allowing them to access, modify and delete data.

Cross-site Scripting (XSS)

Cybercriminals causing website or web application to be deceived into activating malicious programs, allowing them to deface websites and redirect users to malicious websites or hijack user activities.

Buffer Overflow Attacks

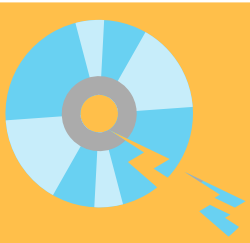
Cybercriminals using malicious programs to send more data to a temporary data storage area, allowing them to corrupt or overwrite the data held in the buffer.

General Considerations on Security Measures for Databases, Websites and Web Applications
[For illustration purposes only]

- Review the types of personal data held in databases and store them in encrypted form.
- Strictly control users direct access to the database, including remote administrator(s).
- Do not allow ‘backdoors’ that allow bypass of user authentication to access personal data.
- Back up databases and ensure that such backups are protected.
- Log database activities and access to personal data.
- Perform web application scanning and source code analysis to help detect web vulnerabilities.
- Perform data validation on user input to prevent buffer overflow attacks, injection attacks and XSS attacks.
- Apply secure connection technologies or protocols, such as TLS, to websites and web applications that handle personal data.For example, use HTTPS instead of HTTP.
- Avoid using unpublished links to files containing personal data stored on website or a web application as this may still be discoverable.
- Use a web application firewall (“WAF”) to defend against typical web application attacks such as SQL injection and XSS attacks. WAFs can act as another layer of security in addition to the application code level.

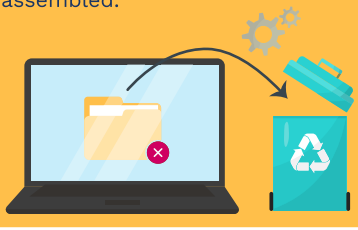
General Considerations on Methods of Disposal of Personal Data

Organisations should set clear retention periods for various types of personal data and dispose anything that is no longer needed for its original purpose or for any business or legal purpose. Hence organisations must ensure that the personal data is **disposed or destroyed in a manner that cannot be recovered or disclosed.**



For Physical Documents: The simple breaking of DVD(s) or tearing of paper documents alone may not destroy personal data completely if it can still be retrieved or pieces can be reassembled.

For Electronic Documents: The simple deletion of any files in a computer may not destroy the personal data completely if can still be retained and recovered.



To ensure such personal data are not at risk, the following methods show good practices of disposal and destruction.

General Considerations on Methods of Destruction

- Using a shredder to cut the documents into small pieces which cannot be reassembled.
- Using dedicated software that can overwrite selected files or the entire storage device and perform secure deletion of personal data or storage media.
- Using specialised hardware appliances that cater for the destruction (such as a degausser machine) or incineration.
- Physically destroy the storage device by crushing, drilling or shredding it.

Alternatively, organisations may anonymise the personal data and keep it for further uses, where appropriate.

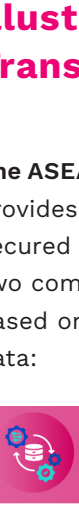
General Checklist on Security Measures

Organisations should ensure appropriate and reasonable **organisational, physical and technical security measures are in place** to protect personal data across the lifecycle. Establishing appropriate security measures will aim to maintain the **confidentiality, integrity and availability** of personal data and protect them from data breaches.

General Checklist on Security Measures	
1 Appoint data protection officer(s) and set clear roles and responsibilities	
2 Conduct data inventory map and/or data protection impact assessment	
3 Develop or update data protection policy, handbook, manual and related contracts	
4 Set retention period and methods of disposal	
5 Communicate duty of confidentiality/ policies for employees	
6 Regularly monitor for any data breaches	
7 Evaluate the software applications used/will be used for personal data	
8 Establish process for regular testing, assessment and evaluation of effectiveness of security measures	
9 Limit access to personal data and lay out authentication processes, encryption and other technical security measures	
10 Destroy or anonymise personal data if it is no longer needed for any purpose	
11 Conduct regular trainings or seminars on data protection	
12 Review processes regularly and document all activities on data protection	
13 Respond to data breaches effectively and document the incident	

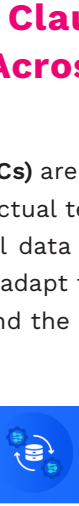
Illustration on Contractual Clauses for the Transfer of Personal Data Across Borders

The ASEAN Model Contractual Clauses (MCCs) are a voluntary standard which provides guidance through template contractual terms and conditions for the secured transfer and exchange of personal data across borders. There are two common scenarios where parties may adapt their contractual provisions based on the nature of the relationships and the purposes of the transfer of data:



Controller-to-Processor Transfer (C-P):

When an organisation exports and transfers data to another organisation which processes the data on behalf, including onward transfers to other organisations.



Controller-to-Controller Transfer (C-C):

When an organisation exports or transfers data to another organisation which processes the data for its own purpose and may have full control of the data upon receipt.

The details of transfer and the personal data involved can be documented in an Appendix to the contract, which may include description of the data subjects involved and the purposes for the transfer of personal data.

NOTE: When using the ASEAN MCCs, parties may modify the contractual terms in accordance to its business requirements and any amendments or added clauses should not contravene the data protection obligations under the PDPO.

For more information, refer to ASEAN Model Contractual Clauses for Cross Border Data Flows.

General Considerations of Contractual Clauses for Obligations on Personal Data Protection
[For illustration purposes only]

Obligations of Data Exporters (C-P, C-C) (The organisation which transfers personal data)
The transfer is made in accordance with applicable data protection laws.
Technical and operational measures are implemented to ensure secured transfer of personal data.
Responding to enquiries and requests of access or correction within reasonable time frame.
Where reasonable, the Data Subject has been notified and given consent.

Obligations of Data Importer (C-P, C-C) (The organisation which receives the personal data)
Processing of personal data only in compliance with Data Exporter's instructions.
No disclosure or transfer of personal data unless permitted by Data Exporter or other written law.
Any disclosure of transfer of personal data to third parties to be bound by similar obligations imposed by the data exporter to the data importer.
Communication to Data Exporter for any enquiries and requests of access or correction of personal data and promptly provide assistance required or assign a focal point.
Return or cease to retain personal data upon completion and/or termination of contract.
Reasonable security measures are in place and consistent with applicable data protection laws.
Notification to the Data Exporter of any occurrence of Data Breach without undue delay and within a reasonable time period.
Promptly notify and consult Data Exporter on any investigation of the transferred data, unless prohibited under law.

Obligation of both Data Exporters and Data Importers (C-C)
Appropriate steps have been taken to determine level of potential risks of data breaches and considered suitable security measures to undertake.
Appropriate controls and adequate security standards shall apply to storage and processing of personal data.

General Considerations for Data Sharing Agreement with Third Party Organisations

When engaging another third-party organisation(s) to provide services relating to the sharing or processing of personal data, organisations should ensure they communicate their data protection requirements clearly and enter into agreements which can ensure reasonable measures are in place to protect personal data.

General Considerations for Data Sharing Agreement with Third Party Organisations

- Parties to the agreement
- Purposes of Data Sharing
- Types of Personal Data to be shared
- Term of the duration of the agreement
- Operational details of the sharing or transfer of personal data
- Description of the security measures and method for protection, retention and/or disposal of personal data
- Name of personnel involved in the processing of personal data
- Any other relevant terms and conditions

Data Sharing Agreements can contain the terms and conditions between two or more parties which sets out the services provided and the obligations of the parties in relation to the PDPO.

For more information, private sector organisations processing personal data on behalf of government organisations may refer to MTIC's Guidelines of Personal Data Sharing.

STEP 5
RESPOND TO INDIVIDUALS EFFECTIVELY

Organisations are expected to establish processes to receive and effectively respond to individuals giving reasonable notice to withdraw their consent, requests for access and/or correction of the personal provided and reports on complaints of alleged breaches of the data protection provisions.

In particular, organisations should be clear on **how individuals can submit such requests or report a complaint.** These can be **facilitated by the appointed DPO** through their official business contact information and organisations may publish this through any of the following methods:

Official website or media channels

Any data protection notices or policy statements

On-premise notices

A dedicated contact form addressed to the DPO

Sample Clause on Data Protection Policy

Any queries, requests for access to or correction of personal data, withdrawal of consent and complaints relating to your personal data may be sent to us to [The Data Protection Officer] at dpo@OrganisationK.com.bn

Illustration on Responding to Withdrawal of Consent

Organisations should aim to respond accordingly to an individual's notice to withdraw prior consent for the collection use or disclosure of his/her personal data, unless any exception applies.

Expectations from the Authority
Organisations to determine official channels of how individuals can give reasonable notice of withdrawal of consent.
Organisations to inform individual of likely consequences of withdrawing his/her consent.
Organisations to acknowledge the request within ten (10) days to effect the withdrawal notice.
If it requires more than ten (10) business days, inform the individual when he/she can expect the withdrawal to take effect.
Organisations to stop using his/her personal data after the withdrawal and cease to retain if there is no business or legal purposes to do so.
If the individuals opts out of receiving direct marketing, ensure such messages will no longer be sent by the end of thirty (30) days.
Third parties should be informed of the withdrawal of consent and personal data will no longer be disclosed to such parties from effective date of withdrawal.

Sample Clause for Withdrawal of Consent from Direct Marketing
[For Illustration Purposes Only]

I hereby withdraw my prior consent for Organisation L to use my personal data, to send me the latest promotions, advertisements, and information about new products and services as follows:

*Please tick the relevant boxes below to indicate the communication channels for which consent is withdrawn.

☑ Email ☑ Text Message ☐ Phone Call ☑ Postal Mail

This withdrawal of consent is made in accordance with the Personal Data Protection Order, 2025 and Organisation L's data protection policy (https://organisationL.com.bn/dppolicy).

I understand that it may take up to thirty (30) working days for this withdrawal to be fully processed, and I may receive pre-scheduled communications during this period.

Full Name: _____ Signature: _____ Date: _____

Illustration on Responding to Access and Correction

Organisations should aim to respond accordingly to an individual's request for access or correction to their personal data, unless any exception applies.

Expectations from Authority
Organisations to determine official channels of how individuals can make access or correction request.
Organisations to exercise due diligence and undertake reasonable measures to verify the identity of the requestor or his/her representative.
Organisations to provide or correct information as soon as reasonably possible, within thirty (30) days.
Organisations may charge a reasonable fee to cover the processing cost for the request.
If it requires more than thirty (30) days, inform the individual when he/she can expect the information to be provided.

Sample Application Form to Request for Access on Personal Data
[For Illustration Purposes Only]

Under the Personal Data Protection Order, 2025, you are entitled to request for access on the personal data that Organisation M has and how the personal data has been used and disclosed over the past year. Upon completion of the form, you can submit it to DPO@OrgansitionM.com.bn

Name of requestor: _____

Contact Number: _____

Email Address: _____

Please indicate the types of personal data you are requesting for, when you provided it to us and state your purposes for accessing the personal data.

Type of Personal Data	Date Provided	Purpose of Access

I understand that Organisation M may charge a reasonable fee for the processing of an access request. I also understand that Organisation M may take steps to verify my identity before processing this request.

This request is made in accordance with the Personal Data Protection Order 2025 and Organisation M's data protection policy (https://organisationM.com.bn/dppolicy).

Illustration on Responding to Complaints of Individuals

Organisations should aim to respond accordingly, address any data protection concerns and seek any amicable resolution directly with the individual, where reasonable.

General Considerations of Handling Complaints of Individuals

- Organisations to determine official channels of how individuals can give reasonable notice of withdrawal of consent.
- Provide clarification on reasons for the organisations actions
- Address concerns of individual, where reasonable
- Keep records of all correspondences with the individual
- Respond within ten (10) days of receiving the complaint
- If it requires more than ten (10) days, inform the individual when he/she can expect to get a response

NOTE: AITI encourages individuals who have concerns about the ways in which an organisation has handled their personal data to first approach the organisation to seek an amicable resolution of the matter before considering to report a complaint to the Authority.