Singapore Standard (SS 714:2025)

IMPLEMENTATION GUIDE

ver1.0 dated 27 June 2025

TABLE OF CONTENTS

1. ABOUT SINGAPORE STANDARD (SS714:2025)

1.1 This Singapore Standard was prepared by the Working Group on Data Protection Trustmark set up by the Technical Committee on Security and Privacy Standards under the purview of the Information Technology Standards Committee.

1.2 The Data Protection Trustmark (DPTM) certification was developed to support the digital economy strategy and for Singapore to stand out as a trusted data hub. The adoption of DPTM helps organisations strengthen their accountability and conformance to generally accepted personal data protection standards and best practices.

1.3 The DPTM will be a visible badge of recognition for an organisation's accountable data protection practices, in particular, for organisations to differentiate themselves from their competitors and increase their business competitiveness. DPTM will also assist companies to identify vendors and partners with sound data protection practices, facilitating more data exchanges to improve business outcomes.

1.4 Specifically, the standard aims to:

a) strengthen and demonstrate compliance with the Personal Data Protection Act (PDPA) and promote accountability by organisations;

b) enhance and promote consistency in data protection standards across all sectors;

c) provide a competitive advantage for businesses that are certified; and

d) encourage organisations to be transparent and accountable in their data protection practices and boost consumer confidence in their management of personal data.

1.5 This standard will cover the following topics and aspects of data protection:

a) Governance and transparency (Clause 6): Appropriate data protection policies and practices (such as risk assessment and data breach management plan) to be implemented for managing personal data, and the communication of these policies and practices to stakeholders.

b) Management of personal data (Clause 7): Appropriate procedures to obtain consent to collect, use and disclose data for appropriate purposes, and the notifications required for each step.

c) Care of personal data (Clause 8): Appropriate procedures to ensure information security, accuracy, completeness, retention and disposal of personal data.

d) Safeguarding individual's rights (Clause 9): Procedures for providing for withdrawal of consent, access and correction of personal data by individuals.

2. HOW TO USE THE IMPLEMENTATION GUIDE

2.1 This Implementation Guide ("IG") is designed to provide a guided approach to support organisations towards the implementation of accountable data protection policies and practices to meet the requirements of the Singapore Standard (SS714:2025) Certification scheme.

2.2 This implementation guide should generally be applicable for most organisations. However, considering the nature of business and the types of personal data handled could vary, organisations should implement practices that are appropriate and commensurate with the type of data that is to be safeguarded. In instances where the organisation implemented additional practices that are not mentioned in this guide, it may be useful to highlight to the assessors to facilitate compliance checking.

2.3 This document shall be read together with the PDPA, the relevant Advisory Guidelines and Guides published by Personal Data Protection Commission ("PDPC") and other relevant documents.

Structure of the Implementation Guide

2.4 The Singapore Standard Certification Framework comprises of 4 main clauses listed in 1.5, presented in the following structure:

a. **Implementation Guidance -** Provides more detailed information on concrete actions to take on the implementation of the requirements and meeting the control objectives.

   For each requirement, the organisation is required to explain and demonstrate clearly the policies, systems, processes and procedures relevant to the criteria and their implementation through written documents and samples of evidence. The organisation shall interpret the intent of the specific requirements in the context of the business and the type of personal data it possesses.

b. **Other Information** - Provides further information that may need to be considered, for example, good practices, legal considerations and references to other standards. This part is shown only if there is relevant and applicable information.

c. **Reference** – References to PDPA Advisory Guidelines / Guides and templates.

2.5 In this implementation guide, the following verbal forms are used:

a. "**shall**" indicates a requirement;
b. "**should**" indicates a recommendation;
c. "**may**" indicates a permission; and
d. "**can**" indicates a possibility or a capacity.

3. SINGAPORE STANDARD CERTIFICATION REQUIREMENTS

CLAUSE 6: GOVERNANCE AND TRANSPARENCY

6.1 Roles and responsibilities

6.1.1 Overall responsibility

The organisation shall bear overall responsibility for the establishment, implementation, and continued execution of all data protection policies and practices.

Implementation Guidance

a. The organisation shall ensure that the policies and practices are formally endorsed and approved by the management in accordance with the organisation's governance structure.

b. Organisations may meet this requirement in different ways, e.g., provide updated documented policies with appropriate management sign-off, notes of meetings on management approval on the policies and processes etc.

c. The management shall be responsible on the organisation's approach to handling personal data and provide leadership through:

- Appointing and empowering the Data Protection Officer (DPO).
- Approving the organisation's data protection policies and Data Protection Management Programme (DPMP).
- Providing strategic guidance on the implementation of data protection initiatives.
- Advocating data protection training.
- Commissioning Data Protection Impact Assessments (DPIA).
- 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

6.1.2 Appointment of a DPO

The organisation shall appoint one or more individuals to fulfil the role of DPO, responsible for ensuring the organisation's overall compliance with data protection obligations.

Implementation Guidance

a. Organisation shall appoint a DPO, preferably from senior management, who can effectively direct and oversee data protection initiatives and ensure that the organisation complies with the PDPA. The DPO can be supported by representatives from various organisational functions. Appointment of DPO can be through official appointment letter, organisation chart, DPO registration with PDPC etc. Organisation with manpower constraints may outsource operational

aspects of the DPO function to a service provider. However, the overall DPO function remains the management's responsibility.

b. Organisation shall clearly define and document the DPO's responsibilities through various means such as DPO appointment letter, data protection policy/manual, etc. Responsibilities of DPO should include, but not limited to the following:
   - Fostering organisation's personal data protection culture and communicating personal data protection policies to stakeholders.
   - Handling access and correction requests to personal data.
   - Managing personal data protection-related queries and complaints.
   - Conducting risk assessment exercises to flag out any potential data protection risks and put in place data protection policies to mitigate those risks.
   - Liaising with the PDPC on personal data protection matters, if necessary.
   - Mapping out organisation's personal data inventory.
   - Keeping up to date with data protection developments (e.g. through DPO registration with PDPC, sign up with DPO Connect, visit PDPC's website regularly, etc).

6.1.3 DPO training

The DPO shall periodically receive relevant training on data protection compliance (e.g., attend relevant courses, attain data protection certifications).

Implementation Guidance

a. The DPO shall be competent in data protection, someone who received relevant subject matter training(s) and/or obtained recognised data protection certification(s).

b. Organisation may meet this requirement in different ways, e.g. provide Statement of Attainment (SOA) to demonstrate that DPO has attended relevant personal data protection courses such as Fundamentals of the Personal Data Protection Act (PDPA) or other protection certification identified under the PDPC DPO Competency Framework and Training Roadmap.

Reference

- Guide to Accountability under the Personal Data Protection Act
- Guide to Developing a Data Protection Management Programme (Part I: Governance and Risk Assessment)
- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 21)
- PDPC - DPO Competency Framework and Training Roadmap

6.2 Establishment of appropriate data protection policies and practices

6.2.1 Implementation within the organisation

The organisation shall establish policies and practices for the management of personal data (including employee data). The subjects addressed by these policies and practices shall include, but are not limited to:

a) collection of personal data;
b) use of personal data;
c) disclosure of personal data;
d) purposes for collecting, using, or disclosing personal data; and
e) notification of purposes.

The policies and practices shall address different types of personal data.

Implementation Guidance

a. Organisation shall establish up-to-date data protection policies and practices to appropriately address all data protection requirements in compliance with the PDPA based on organisation's operations and business needs. These policies and practices should be developed as part of the organisation's corporate governance policies and implemented consistently.

b. The policies and practices shall apply to all personal data (e.g. employees, job applicants, customers, users etc) that the organisation holds (in both electronic and physical form). This includes managing different type of personal data including but not limited to those sensitive in nature and anonymised data.

c. Depending on the organisation's business, policies and practices including, but not limited to the following, should be established.
   - Employees: Internal data protection policy and notice.
   - Customers, Job Applicants etc: External data protection notices.
   - Third Party Vendors: Third party agreement for management of the organisation's personal data.

6.2.2 Implementation by third parties

Third parties engaged by the organisation (e.g., vendors, data intermediaries) to transact or process data shall demonstrate that the relevant policies and practices as described above are established within their organisation.

Implementation Guidance

a. Where the organisation engages third parties to handle or process personal data, organisation shall set personal data protection requirements and communicate to their third parties as clearly as possible.

   When handling personal data on the organisation's behalf, the third parties (e.g. data intermediary) are responsible for adhering to the Protection, Retention and Data Breach Notification Obligations under the PDPA. In this regard, organisation shall ensure binding

contractual agreement between the organisation and their third parties that highlight the responsibilities of third parties with regard to the processing of the personal data as well as compliance tracking should be in place.

b. Organisation may implement it in different ways, e.g. use standard contractual clauses in contracts and processing agreements with third party service vendors (e.g. cloud service providers) to ensure protection for personal data, use contractual clauses and retention schedules in contracts and processing agreements with third party service vendors to ensure proper disposal of personal data, etc.

Reference

- DP Notice Generator - Generate basic data protection template notices to inform their stakeholders (employees, customers, job applicants, etc.)

6.3 Monitoring compliance and review of policies and practices

6.3.1 Monitoring compliance

Compliance with data protection policies and practices shall be monitored in a structured and timely manner. The monitoring process shall extend, where relevant, to compliance by third parties engaged by the organisation (e.g., vendors, data intermediaries).

6.3.2 Outcomes of periodic monitoring

Outcomes of the periodic monitoring for compliance with policies and practices shall be reported to the management. Any gaps identified shall be addressed with remediation plans.

Implementation Guidance

a. Organisation shall have process to monitor compliance of data protection policies and practices regularly (e.g. annually) through activities such as:
   - Conducting an internal audit on a periodic basis.
   - Conducting a walk through and inspection.
   - Engaging an external party (on a periodic basis or as required) to evaluate implementation of data protection policies and processes.
   - Obtaining the Data Protection Trustmark or other relevant certifications.

b. Organisation shall conduct regular reviews/due diligence (e.g. every quarter or annually) to ensure third parties' compliance (e.g. through random spot-checks, request for an independent audit report, etc) of data protection and security policies, processes and practices.

c. Organisation shall ensure the outcome of the regular compliance monitoring, and any identified personal data protection non-compliance, gap analysis, and remediation plans are reported to the Management to get their support, direction and feedback.

Reference

- Guide to Developing a Data Protection Management Programme (Part IV: Maintenance)

6.3.3 Review and updates to policies and practices

The organisation shall review new data protection requirements, amendments, or additions to local data protection laws and international data protection guidelines and develop processes accordingly to maintain or improve compliance.

Developments or advancements in technology and business domains that affect data flow or systems should be evaluated for potential impact on the robustness of the organisation's policies and practices.

Significant changes in the organisation's collection, use, or disclosure of personal data should also necessitate a similar evaluation.

Where necessary, a DPIA should be conducted.

Implementation Guidance

a. Organisation shall establish process to conduct reviews of their data protection policies and practices at regular (e.g. annually) intervals or ad-hoc, if there are significant changes, to ensure suitability, adequacy and relevancy of the policies and practices. All changes shall be properly documented and endorsed by management.

b. The reviews should keep abreast of the changes and developments within (e.g. major re-organisation, new systems or processes, feedback from stakeholders, etc) and outside the organisation (e.g., amendment to relevant laws and regulations, issuance of new resources from the PDPC, data breaches in other organisations, international or industry guidelines, etc), to ensure that data protection policies and practices remains relevant and updated.

c. Organisations may also conduct a Data Protection Impact Assessment (DPIA) to provide assurance that the organisation's data protection practices are in line with new changes and that data protection risks are being managed effectively.

Reference

- Guide to Data Protection Impact Assessments

6.4 Processes for handling queries, complaints and special requests

6.4.1 Receiving queries, complaints and special requests

The organisation shall establish and document processes to receive and respond to queries or complaints arising with respect to the organisation's collection, use, or disclosure of personal data.

Specific processes shall also be implemented to handle requests from:

a) public agencies for the disclosure of personal data; and
b) courts and law enforcement agencies when required for investigations or proceedings under the prevailing law

Implementation Guidance

a. Organisation shall establish process to handle individual's queries and/or complaints including dispute resolution relating to data protection. The process may include how the organisation handles complaints, such as receiving, assessing, investigating, responding and taking corrective actions to address the complaints.

b. Organisation shall make the complaints handling process readily available to all relevant stakeholders such as:
   - Employees: Staff handbook, employees internal company memo, company intranet or other forms.
   - Customers/Job Applicants: Privacy notice on the organisation's website or other forms.

c. Organisation shall establish a process to respond to requests to disclose personal data to public agencies, courts and law enforcement agencies. The process should include the timeline to respond, steps to verify the authenticity of the requestor and an appropriate party in the organisation to respond to the public agencies.

6.4.2 Responding to queries, complaints and special requests

The organisation shall promptly respond to queries and complaints. Responses to complaints shall include an explanation of remedial actions where relevant.

Queries and responses shall be documented and retained for a reasonable period of time as determined by the organisation.

Implementation Guidance

a. Organisation shall ensure queries and complaints are handled effectively and promptly. The following guidelines should be considered:
   - Acknowledge and respond to complainant in a timely manner.
   - Include a register to keep track of the status and responses of the complaints.
   - Escalate and keep management informed on relevant data protection related complaints.
   - Update results of investigation and remediation within a reasonable timeframe.

Reference

- Develop a Process for Dispute Resolution

6.5 Processes to identify, assess and address data protection risks

6.5.1 Data Protection Impact Assessment (DPIA)

The organisation shall establish a process, such as a DPIA, to identify, assess, and address personal data protection risks to meet the organisation's operational functions, business needs, and processes. The management shall develop and approve action plans to mitigate identified risks and promptly implement them.

The DPIA shall be reviewed periodically to ensure it can identify current risks and determine appropriate mitigation measures.

Implementation Guidance

a. Organisation shall conduct Data Protection Impact Assessments (DPIA) to identify, assess and address personal data protection risks (including possible IT solutions and security on systems (e.g. public facing websites, Customer Relationship Management (CRM) systems, etc), functions (e.g. HR, Customer services, etc), and processes (e.g. procurement process) that involve the handling of personal data.

b. The DPIA process may include, but not limited to, assessing and conducting the risk and impact assessment, identifying the potential gaps after assessment, remediation efforts to address gaps, and implementing appropriate technical or other relevant measures to safeguard against data protection risks.

c. Organisation shall document the DPIA process including details of the action plans to be taken to address the identified risks and ensure that the proposed action plans are in line with the organisation's policies and practices:
   a. assess the realistic likelihood of the occurrence of the risk, determine the levels of risk and elaborate on how the risks are addressed.
   b. Specify the action owner(s) responsible to mitigate the risks.
   c. Provide the timeline for implementation measures to mitigate/eliminate the risks.
   d. Ensures that repeated DPIA produce consistent, valid and comparable results

c. The action owner shall implement and monitor the outcomes of the action plan, approved by management, to ensure that identified personal data protection risks are adequately addressed. When there is a change in risks associated with handling of personal data in the project, the existing DPIA (in particular the action plan outcomes) would need to be reviewed and updated where needed so that any new gaps or risks to individuals' personal data can be addressed.

Other Information

a. The PDPA requires organisations to conduct assessments to eliminate, reduce the likelihood or mitigate likely adverse effect to the individual when relying on deemed consent by notification, or legitimate interests' exception. (Note: the specific requirements for these assessments are provided in the regulations, as well as in the Advisory Guidelines on Key Concepts in the PDPA dated 1 Feb 2021).

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 21)
- Guide to Accountability under the Personal Data Protection Act
- Guide to Data Protection Impact Assessments
- Guide to Developing a Data Protection Management Programme (Part I: Governance and Risk Assessment & Part III: Processes)
- Data Protection Practices for ICT Systems

6.5.2 Data protection by design

The organisation shall take steps to ensure that data protection settings protect users by default. This means that the organisation shall:

a) implement data protection measures from the earliest possible design stage and throughout the operational lifecycle of a system, process, product, or service;
b) establish the necessary safeguards at each point of data collection, use, or disclosure;
c) make available to the user when data is collected for marketing purposes:
   i. opt-in consent rather than opt-out, and
   ii. data protection settings that are accessible and easy to understand.

Implementation Guidance

a. Organisations shall develop and implement processes to adopt Data Protection by Design (DPbD) where data protection measures are considered and incorporated from the start of the development of any product, service, system or process that involved processing of personal data. This may help organisations identify data protection issues early and increase awareness of data protection across the organisation.

b. Organisation should consider applying relevant DPbD best practices from the earliest possible design stage and throughout the operational lifecycle of a system or processes, such as

   a. Conduct DPIA to address data protection risks when the system or process is new and being designed, as there would be likely increased cost and effort to address data protection risks after the design of a process or system has been finalised or implemented.
   b. Minimise collection of personal data to ensure that the collection is for a lawful and reasonable purpose that is directly related to a function or activity of the organisation, and not excessive for the purpose.
   c. Collect information on personal identifiers (e.g. national identification number) when necessary (e.g. to accurately establish or verify the identity of the individual to a high degree of fidelity).
   d. Notify and explain clearly to individuals of the purposes and obtain their consent for collecting, using and disclosing their personal data, unless any exception applies.
   e. Implement good security measures and practices at every stage of the Software Development Lifecycle, and from the point that personal data is collected until it is purged from the system.
   f. Implement appropriate access control at the application to protect personal data (e.g. define user roles or groups and assign appropriate user access rights accordingly).
   g. Avoid loading production data (i.e. personal data) to test environments as testing environment is much less secure compared to production environments.
   h. Conduct vulnerability assessment and penetration testing.

c. Organisation should also consider building in DPbD to existing system or processes, such as:

   a. Conduct DPIA to review its existing system thoroughly, considering what personal data is being collected and whether the collection is completely necessary.

b. Implement relevant DPbD good practices to better protect personal data and reduce the risks identified.

d. Organisation shall implement data protection measures that integrate into processes and features of the systems to safeguard individuals' personal data by default. Examples include:

a. Adopting an opt-in consent rather than opt-out approach.
b. Giving individuals the option to customise settings with informative notices that are easily accessible, clear and easy to understand.
c. Requiring explicit action from the individual to indicate consent (e.g. checkbox should not be pre-ticked but to be selected by the individual).
d. Collecting personal data only when needed (e.g. provide the option for the individual to indicate his/her location when required rather than collecting it as default).

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 21)
- Guide to Accountability under the Personal Data Protection Act
- Guide to Developing a Data Protection Management Programme (Part II: Policy and Practices)
- Data Protection Practices for ICT Systems

6.6 Managing data breaches

6.6.1 Establishing the data breach management plan

The organisation shall establish a data breach management plan which includes the following:

a) A reporting structure of key relevant personnel in the organisation who are authorised to make time-critical decisions on the assessment and management of data breach incidents;
b) Arrangements for data intermediaries to notify the organisation of data breaches;
c) Timelines for reporting data breach incidents detected to the relevant personnel in the organisation;
d) A timeline for each action item;
e) Procedures for assessing whether the data breach meets the specified criteria for notification under the prevailing laws, regulations, or guidelines;
f) Notification process for affected individuals, and where required, relevant regulators or enforcement authorities.

The data breach management plan shall be communicated to all relevant internal and external stakeholders. The management shall ensure that all stakeholders are aware of their roles.

Implementation Guidance

a. Organisation shall develop data breach management processes to respond and address data breaches swiftly and in a systematic manner. The following guidelines should be considered when preparing a data breach management plan:

I. Define and monitor for data breach

a. There should be a clear explanation of what constitutes a data breach (suspected and confirmed) to assist employees in identifying and to respond promptly should one occur.
b. There should be measures (e.g. monitoring tools, real-time intrusion detection software, etc.) put in place to monitor and take pre-emptive actions to prepare for data breaches.

II. How to report a data breach internally

a. There should be a clear breach reporting process (through email or other mechanisms) under which the person(s) (e.g. DPO, breach response team, etc.) would be notified in the event of a data incident. This will ensure that employees know how and who to report the data breach to within the organisation when aware of a potential or real data breach.

III. How to respond to a data breach

a. There should be a strategy developed for containing, assessing and managing data breaches, which includes roles and responsibilities of the employees and data breach management team.
b. There should be contingency plans for possible data breach scenarios and measures to be taken or regular breach simulation exercises conducted to respond to data breach in a prompt and effective manner.

IV. Responsibilities of the data breach management team

a. There should be a data breach management reporting structure with relevant personnel assigned in the organisation who will make time-critical decisions on the assessment and appropriate response to manage the data breach incident.
b. There should be timelines for reporting/escalating data breach incidents to the responsible personnel in the organisation who should act on the information received according to their assigned roles. This will ensure that the organisation's response to the data breach will not be unnecessarily delayed.

b. When responding to data breach, organisation should consider taking the following steps (using the acronym of C.A.R.E):

I. Contain the data breach

a. An assigned individual or group should be immediately notified of all suspected/confirmed data breaches upon detection and conduct an initial appraisal of the data breach to determine its severity.
b. This will help the organisation decide on the immediate actions to be taken to contain the data breach as soon as possible to minimise potential harms from the breach. Immediate containment actions include:
    - Isolate the compromised system from the internet or network by disconnecting all affected systems.
    - Prevent further unauthorised access to the system. Disable or reset the passwords of compromised user accounts.
    - Establish whether the lost data can be recovered and implement further action to minimise any harm caused by the data breach.

c. Organisation should consider alerting the following bodies (e.g. Police, CSA, etc) if it suspects that criminal acts have been perpetrated and follow the requirements set out by its respective sectoral regulators (e.g. MAS, MOH, etc) for reporting of data breaches.

II. Assess the data breach

a. Assessment of data breaches should be conducted in a reasonable and expeditious manner and the steps taken documented in assessing the data breach.
   - Assessment of risks and impact of the data breach shall be done expeditiously (within 30 calendar days) to determine whether there could be serious consequences to affected organisations/individuals, as well as to assess whether the data breach is notifiable under the PDPA.
     - Depending on the outcome of assessment, the data breach may have to be notified to the PDPC and/or the affected individuals.
     - Understanding the extent and likely impact of the data breach will help the organisation identify and take further steps to limit the harm resulting from a data breach and prevent the recurrence of similar incidents.

III. Report the data breach

a. Depending on the outcome of assessment, the data breach may have to be notified to the affected individuals and/or the relevant regulators/enforcement authorities according to the requirements and timeframe for notification under the PDPA.
b. Organisation is to notify PDPC no later than 3 calendar days after the day the organisation determines that the data breach meets the notification criteria:
   - significant harm or impact to individuals (based on prescribed class of personal data for notification listed in the Advisory Guidelines on Key Concepts in the PDPA dated 1 Feb 2021), and/or
   - of a significant scale (i.e. more than 500 individuals affected).
c. Organisations must also notify affected individuals as soon as practicable after notifying PDPC, when a data breach is likely to result in significant harm or impact to them, regardless of the scale of the breach.
d. Notifying the data breach when the organisation is a DI:
   - Where a data breach is discovered by the organisation that is processing personal data on behalf and for the purposes of other organisations or public agencies, the organisation is required to notify other organisations or public agencies without undue delay from the time it has credible grounds to believe that the data breach has occurred.

IV. Evaluate the data breach

a. Organisation should review and learn from the data breach to improve its personal data handling practices and prevent the recurrence of similar data breaches. This can include:
   - Conduct a review including a root cause analysis of the data breach (e.g. implement fixes to system errors/bugs to prevent future disclosure of/access to personal data).
   - Develop a prevention plan to prevent similar data breaches in future.
   - Perform audit to ensure the prevention plan is implemented.

d. Organisation shall communicate to relevant internal and external stakeholders so that they are aware of their roles in the data breach management plan to ensure a quick and effective response to data breach incidents, such as:
    - Internal (Management): The composition and the roles and responsibilities of each member of the management team should be clear, such as who would be responsible for assessing the risks and making time-critical decisions on steps to be taken to contain and manage the data breach.
    - Internal (Employees): Each employee should be clear of his/her role in the event of a data breach. When an employee becomes aware of a potential or actual data breach, he/she should know how and who to report the data breach to within the organisation (e.g. specific individuals with expertise in handling data breaches, the DPO, senior management representative, data breach management team, etc). This should be communicated through training or information easily accessible and available (e.g. company intranet).
    - External (Data Intermediary): Where a data breach is discovered by a Data Intermediary (DI) that is processing personal data on behalf of and for the purposes of the organisation, the DI is required to notify the organisation without undue delay from the time it has credible grounds to believe that the data breach has occurred. Organisation shall ensure that the data breach notification requirement is included in the contractual agreement.

6.6.2 Implementing a data breach management plan

The organisation shall implement a data breach management plan based on the following :

a) A set of possible data breach scenarios, and for each scenario:
    i. the relevant personnel within the organisation to report the incident; and
    ii. the action plans for response, remediation and containment.

b) Procedures to assess the risks and impact of the data breach, including the identification of possible consequences to affected organisations or individuals

These plans should be subject to regular reviews and testing by the organisation.

Implementation Guidance

a. Organisation shall develop drawer plans on possible data breach scenarios or run regular breach simulation exercises to respond to data breaches in a prompt and effective manner.

b. Organisation should demonstrate through past breach incident(s), drawer plan or conduct periodic table-top exercise to test the data breach response plan to ensure the data breaches are handled according to the data breach management plan and process set out by the organisation.

c. The table-top exercise conducted should include process for organisation to take reasonable and expeditious steps to assess whether the data breach is notifiable to the PDPA and affected individuals.

d. Apart from data breach management plans, organisations may also consider developing crisis management, communications and business continuity plans to aid in their handling of data breaches and recovery from such incidents.

6.6.3 Remediation for data breaches

If the organisation has reported a breach within the last two years prior to seeking DPTM certification, a self-assessment shall be conducted for each reported breach to establish if the remediation is complete.

Implementation Guidance

a. If organisation encountered a data breach within the last 2 years of seeking certification, organisation shall provide information on the details of the data breach and the remediation required to mitigate or prevent the recurrence of similar data breaches in future.

b. Organisation may meet this requirement in different ways, e.g. demonstrate that the remediations are completed with management endorsement, conduct audits to ensure the remediations are implemented, review of existing policies, procedures and changes to reflect the lessons learnt from the data breaches, etc.

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 20)
- Guide on Managing and Notifying Data Breaches Under the PDPA
- Guide to Developing a Data Protection Management Programme (Part III: Processes)

6.7 Accountability

6.7.1 Accountability to public

The business contact information of at least one DPO shall be made publicly available and accessible.

Implementation Guidance

a. Organisation shall make DPO's contact information (e.g. email address, office number, mailing address, etc) available and easily accessible by the public via the organisation's website or forms

b. The contact details should be operational during Singapore business hours.

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Paragraph 21.6)

6.7.2 Accountability to external stakeholders

The organisation's public data protection policies shall be made available to external stakeholders (e.g., customers, third parties). The data protection policies, including relevant practices for protection and handling of personal data, shall be provided in a clear and accessible manner.

Implementation Guidance

a. Organisation shall communicate its data protection policies to all relevant external stakeholders, through various mechanisms such as:
   - Customers: Privacy notice on the organisation's website, service/product sign-up or other relevant forms, providing the data protection policy promptly when requested by customers.
   - Job Applicants: Privacy notice on the organisation's website, job application form/job portal or other relevant forms.
   - Third Party Vendors: Third party agreement on management of the organisation's personal data.

b. Organisation shall establish processes on how its data protection policies are communicated to external stakeholders upon request, through mechanisms such as email or physical copy, etc.

Reference

- Data Protection Notice Generator (https://apps.pdpc.gov.sg/dp-notice-generator/introduction).

6.8 Internal communication and training

6.8.1 Communication for awareness

There shall be processes in place to communicate data protection policies and practices to employees, and where relevant, third-party or temporary hires.

Updates to data protection policies and practices shall be promptly communicated to employees, and where relevant, third-party or temporary hires.

Implementation Guidance

a. Organisation shall communicate the policies and practices effectively to all employees to ensure that they are aware of their roles and responsibilities in handling personal data. Organisation may meet the requirement in various ways such as:
   a. Including data protection policies on the employment form.
   b. Employees' acknowledgement of the data protection policy by signing it.
   c. Providing easily accessibility of the data protection policy via the organisation's intranet/employees' handbook.Regular circulars to employees to generate awareness of personal data protection.Conducting data protection briefing to new staff via onboarding programme and refresher briefing for existing employees on data protection update via email, face-to-face.
   d. Conducting regular staff meeting or other relevant forms on data protection
   e. Conducting staff surveys to understand data protection awareness or feedback on data protection practices in the organisation.

b. Organisation shall establish processes and communicate updates to data protection policies to ensure employees and where relevant, third party hires and temporary hires are kept apprised in a timely manner, through mechanisms such as:
   a. Data protection policy via the organisation's intranet/employee's handbook.
   b. Regular circulars or emails to employees on updated policies.
   c. Ad-hoc briefing when there is a revision to the PDPA, PDPC guidelines or organisation's data protection policies and practices.
   d. Regular staff meeting or other relevant forms.

Reference

- Guide to Accountability under the Personal Data Protection Act
- Guide to Developing a Data Protection Management Programme (Part 1: Governance and Risk Assessment)

6.8.2 Training for internal stakeholders

The organisation shall provide relevant training to employees, and where relevant, third-party or temporary hires periodically, to increase awareness of and compliance with data protection policies and practices. Where necessary, refresher training courses shall be provided.

The organisation shall have training programmes, including but not limited to the following topics:

a) Data protection policies and processes
b) Procedure to handle queries and complaints related to personal data;
c) Data breach management plan; and
d) Security policies and processes

Implementation Guidance

a. Organisation shall have processes to provide the regular training to internal stakeholders (employees, third-party hires and temporary hires) on data protection policies and practices and ad-hoc training when there is a revision to the PDPA, PDPC guidelines or organisation's data protection policies and practices.

b. Organisation shall conduct ICT security awareness training regularly to keep employees updated on common topics such as password management, phishing/social engineering protection, corporate/personal device protection, reporting cyber incidents etc.

c. Organisation shall demonstrate the existence of a training programme where relevant trainings are provided to employees to educate on their responsibilities in the handling of personal data. These trainings should take place periodically and can be conducted by the organisation or by external vendors such as:
   - During on-boarding of new staff and refresher courses for employees on an ad-hoc/periodic basis (e.g. annually) when there is a revision to the PDPA, PDPC guidelines or organisation's data protection policies and practices.
   - Provide in-depth PDPA training specific to employees upon assignment to a specific job role or change in role/job scope.

- Obtain professional certification by DPO.

Reference

- Guide to Accountability under the Personal Data Protection Act
- Guide to Developing a Data Protection Management Programme (Part 1: Governance and Risk Assessment)

CLAUSE 7: MANAGEMENT OF PERSONAL DATA

7.1 Determining appropriate purpose

7.1.1 Assessing necessity

The organisation shall establish processes to determine that only personal data necessary to meet the specified purpose is collected.

The organisation shall collate the following information to limit collection to only necessary data:

a) Sources of personal data (e.g., directly from the individual or from third parties collecting on the organisation's behalf);
b) Types of personal data collected from individuals (e.g., customers, employees, contractors); and
c) Their respective purposes of collection

Implementation Guidance

a. Organisation shall have documented policies and processes to ensure personal data collected (directly or through a third party) is relevant and reasonable for the identified purposes and does not collect unnecessary personal data.

b. In collecting sensitive personal data, organisation shall consider whether alternative forms of personal data can be collected that can allow organisation to carry out its functions or to achieve the same purpose, as the potential adverse effect to individuals will be higher if the personal data is sensitive in nature. This is especially when sensitive personal data is collected from vulnerable individuals (e.g. minors, individuals with physical or mental disabilities, or other special needs, etc).

c. Organisation shall only collect information on personal identifiers (e.g. national identification number) when absolutely necessary. In instances where the collection of NRIC numbers is permitted under the law or when necessary to accurately establish or verify the identity of the individual to a high degree of fidelity, it should be properly documented. For example, instead of collecting NRIC number during the job application process, organisation should consider collection of name and date of birth and verify the individual's identity with the physical NRIC during the face-to-face interview.

d. Organisation shall clearly identify and document the types/source of personal data (including sensitive data where applicable) collected directly from individuals (e.g. customers, employees, contractors, etc), or from third parties collecting on organisation's behalf and their respective purposes for collection, use and disclosure of the personal data in the form of a data inventory map or data flow diagrams.

e. The data inventory map and data flow diagram should include information on the business purposes for collection, use and disclosure of personal data, the individuals and third parties who handle personal data under the organisation's possession or control, as well as a classification of

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

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 14)
- Guide to Developing a Data Protection Management Programme (Part III: Processes)
- Data Protection Practices for ICT Systems (Section: Policy and Risk Management for ICT Systems)
- PDPC Resources (Sample Personal Data Inventory Map Template)

7.1.2 Verification of purpose

The organisation shall establish a process to verify that the defined purposes are appropriate and consistent with the requirements of prevailing laws and regulations.

The organisation shall conduct regular reviews to ensure that the purposes for which personal data is collected remain necessary and appropriate.

Implementation Guidance

a. Organisation shall have a documented policies and processes to ensure that collection of personal data of an individual is only for purposes that a reasonable person would consider appropriate under the circumstances.

b. Organisation shall document and demonstrate that the collection of personal data is for a lawful and reasonable purpose that is directly related to a function or activity of the organisation, and not excessive for the purpose. Organisation should view the situation from the perspective of the individual and consider what is fair and reasonable.

c. Organisation shall conduct regular (e.g. annually) reviews on the organisation's need to collect, use or disclose personal data, for example, by reviewing the data inventory map on a regular basis to ensure personal data collected is necessary and appropriate for the purpose. The reviews should take into consideration the types of personal data collected in relation to the purposes identified.

7.2 Appropriate notifications

The organisation shall establish processes to provide the following information through clear, concise, and accessible notifications to individuals at the time of data collection:

a) The purposes of the data collection, to be notified on or before collecting their personal data;
b) The form of collection, whether the collection is carried out by the organisation itself or through third parties acting on the organisation's behalf;
c) Whether the collection of their data is necessary;
d) Reasons why data collection is necessary, such as:
   i. requirement by law,
   ii. requirement to provide the service;
e) Consequences of not providing the personal data necessary for a transaction or service

f) Whether the collected information may be disclosed to third parties; and
g) How individuals can exercise choice in the collection, use, or disclosure of their personal data.

Implementation Guidance

a. Organisation shall have documented processes to demonstrate that its collection, use and disclosure is limited to the purposes for which notification has been made to the individuals.

b. Organisation shall notify the individuals of the purposes for which their personal data would be collected, used and disclosed and obtained their consent on or before collecting their personal data, including why the personal data collected is necessary (to provide a service or required under applicable laws).

c. Organisation shall provide clear and concise notifications to individuals that their personal data, collected directly by the organisation or through third parties acting on behalf of the organisation, may be disclosed to third parties through mechanisms such as:
    a. Employees: Data protection notice in employment form, company intranet or other forms.
    b. Customers: Data protection notice on the organisation's website or other forms.
    c. Job Applicants: Data protection notice on the organisation's website, job application form or other forms.

d. Organisation shall provide clear notifications on how the individuals may exercise choice in the collection, use or disclosure of their personal data. For example:
    a. Individuals can provide consent to collect, use and disclose their personal data by agreeing with the data protection notice, terms of agreement, job application form, etc.
    b. Individuals are provided with information on how to withdraw consent in the data protection notice, job application form, etc.

e. Organisation shall indicate clearly the consequences of individuals not providing their personal data, such as the organisation is unable to provide the services, offer a job to the individual, or legal consequences.

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapters 7, 8, 9, 13 and 14)
- Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers
- Guide to Developing a Data Protection Management Programme (Part III: Processes)
- Data Protection Practices for ICT Systems (Section: Policy and Risk Management for ICT Systems)
- Guide to Notification

7.3 Appropriate consent

7.3.1 Obtaining consent

7.3.1.1 Valid or deemed consent

The organisation shall ensure valid or deemed consent is obtained from an individual for the collection, use, or disclosure of their data.

The ways in which consent can either be valid or deemed are:

a) by conduct;
b) by contractual necessity; or
c) by notification.

Implementation Guidance

a. Organisation shall obtain consent from the individual in several ways – a) expressed consent (consent obtained in writing or recorded in a manner that is accessible), or b) deemed consent where consent is not explicitly given. Examples of expressed consent are through agreeing with the data protection notice, job/employment application form and opt-in for marketing communications, etc.

b. If organisation relies on deemed consent, it is required to demonstrate and document how the individual has deemed to consent to the collection, use or disclosure of his/her personal data through:
   a. Deemed consent by conduct, where individual voluntarily provides his/her personal data and the purposes are limited to those that are objectively obvious and reasonably appropriate from the surrounding circumstances (e.g. processing of payment where individual handed over credit card to the cashier to make payment).
   b. Deemed consent by contractual necessity, where consent may be deemed to be given for disclosure of the personal data from one organisation to another for the necessary conclusion or performance of a contract/transaction between the individual and the organisation he/she had originally provided the personal data to (e.g. processing of payment and delivery of e-commerce transaction).
   c. Deemed consent by notification, where consent may be deemed if the organisation (i) notifies the individual of the purpose of the intended collection, use or disclosure of his/her personal data, (ii) gives a reasonable period by which to opt-out of the collection, use or disclosure of his/her personal data for the purpose, and (iii) the individual does not opt-out within the period. Before the organisation may rely on deemed consent by notification, the organisation:
      i. Must conduct an assessment to ensure collection, use or disclosure of the personal data is not likely to have an adverse effect on the individuals.
      ii. Must not rely on deemed consent by notification for the purpose of sending direct marketing messages to the individuals.

Other Information

a. When conducting an assessment to eliminate or mitigate adverse effects, organisation may use the Assessment Checklist on Deemed Consent by Notification (provided in the Advisory Guidelines

on Key Concepts in the Personal Data Protection Act (Annex B)) to conduct the assessment. Please refer to the Personal Data Protection Regulations 2021 and Paragraphs 12.64 – 12.69 of the Advisory Guidelines on conducting the assessment.

7.3.1.2 Providing choices for type of consent

The organisation shall establish and document the processes that enable individuals to exercise choice in relation to their data's:

a) collection;
b) use; or
c) disclosure.

Implementation Guidance

a. Organisation shall establish processes for individuals to exercise choice in relation to the collection (and use or disclosure) of their personal data, such as providing consent through mechanisms like application form, online webform or mobile application, etc, and not obtain consent through providing false or misleading information or using deceptive or misleading practices.

7.3.1.3 Methods for providing choice

The organisation shall provide individuals with a means to specify the scope of consent for their personal data being collected.

Options provided for exercising choice shall be accessible and presented clearly and concisely. The following list provides examples of methods by which users can exercise choice:

a) Webforms,
b) Selection panels embedded within mobile applications, and
c) Hard-copy application forms.

Implementation Guidance

a. Organisation shall demonstrate that the mechanisms relating to how individual may exercise choice in the collection (use or disclosure) of their personal data are provided in a clear, comprehensible and accessible manner. For example:
    - Individuals can provide consent to collect, use and disclose their personal data by agreeing with the data protection notice, terms of agreement, job application form, opt-in for marketing communications, etc.
    - Individuals are provided with information that is clear and easily accessible to individual on how to withdraw consent to use and disclose their personal data on relevant avenues like data protection notice, job application form, etc. For example, the organisation can
        a) advise the individuals on the form and manner to submit a notice to withdraw their consent for specific purposes;
        b) indicate the person to whom, or the means by which, the notice to withdraw consent should be submitted; and
        c) distinguish between purposes necessary and optional to the provision of the products/services (that may include the service of the existing business relationship). Individuals must be allowed to withdraw consent for optional purposes without concurrently withdrawing consent for the necessary purposes.

7.3.2 Consent obtained via third parties

7.3.2.1 Validity of given consent from the individual

The organisation shall have appropriate measures and mechanisms in place to ensure that a person providing consent on behalf of an individual is acting validly on their behalf.

Implementation Guidance

a. Organisation shall establish a process to verify that necessary consent of the individual has been obtained from a person validly acting on behalf of the individual.

b. The process should include:
   a. Verifying the identity of person validly acting on behalf of the individual, e.g. individual signing the proxy form, etc.
   b. Notifying the purposes to the person acting on behalf of the individual for which the individual's personal data will be collected, used and disclosed.
      - Validating that the individual has given consent for those purposes. For example, when contacting the individual for the first time, the organisation should inform the individual that his/her personal data was disclosed by the person and verify that individual had provided consent to do so.

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Paragraphs 12.33 – 12.34)

7.3.2.2 Validity of obtained consent from third party sources

The organisation shall ensure that third-party sources of personal data have obtained valid consent, unless collection without consent is permitted under prevailing laws.

This shall include:

a) having processes in place to establish contractual agreements with third parties to ensure valid collection of personal data; and
b) exercising due diligence to ensure that the third-party source has obtained consent from individuals whose personal data may, for specified purposes, be:
   i. collected,
   ii. used, or
   iii. disclosed

Implementation Guidance

a. Organisations may collect personal data of an individual from third party sources such as vendor's marketing databases, third party referrals, authorised dealer processing application on behalf of the organisation and insurance/financial representatives collecting customers' data on behalf of the insurers.

b. Organisation shall establish contractual agreements with third parties to ensure valid collection of personal data such that necessary consent has been obtained from the individuals by the third

parties on the disclosure of their personal data to the organisation. For example, the contract with the third party indicates that the purpose of disclosure to the organisation is within the scope of the consent given by the individual to the third party, consent to be obtained for the necessary disclosure, etc.

c. Organisation may adopt one or more of the following measures to ensure that the third party source has obtained consent from individuals to collect, use or disclose their personal data for specified purposes:
   a. Establish contractual agreement to ensure collection, use or disclosure to the organisation is within the scope of the consent given by the individual to third party for specified purposes.
   b. Obtain confirmation in writing from third party on consent obtained from individuals.
   c. Obtain a copy of the document(s) containing or evidencing that consent has been obtained from individuals on the collection, use or disclosure of personal data to the organisation for specified purposes.
   d. Verify third party's terms of agreement/data protection notice with the individuals, to ensure consent has been obtained on the collection, use or disclosure of personal data to the organisation for specified purposes.

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 12)

7.3.3 New purposes for collection

The organisation shall establish processes to determine when there are new purposes for collection, use, and disclosure of personal data, and to update the notification accordingly to reflect these new purposes.

Where personal data collected is to be used or disclosed for new purposes, there shall be processes in place to notify individuals of the new purposes of use or disclosure, and to obtain consent for the use or disclosure.

Implementation Guidance

a. To determine if personal data can be used or disclosed for a new purpose without obtaining fresh consent, an organisation should find out:
   a. Whether the purpose is within the scope of the purposes for which the individual had originally been informed.
   b. Whether consent can be deemed to have been given by the individual in respect of use or disclosure for that purpose in accordance with Section 15 or 15A of the PDPA.
   c. Whether the purpose falls within the exceptions from consent in the First and Second Schedules to the PDPA.

b. If the purpose does not fall within the above 3 scenarios, organisation shall establish processes to notify individuals for use and disclosure of personal data for a different purpose from which it was first collected. Processes shall include:

a) Updating the notifications (e.g. through application forms, data protection notices on the organisation's website to reflect these new purposes).
b) Notifying and obtaining the individual's fresh consent for use and disclosure for the new purpose.

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapters 7, 8, 9, 13 and 14)
- Guide to Notification

7.4 Appropriate use

Where consent to collect data is obtained from an individual, the organisation shall have documented processes in place to ensure the use of personal data collected is consistent with the purposes for which the individual has given consent. The processes shall apply when the consent to collect data is obtained:

a) directly from the individual; and
b) through third parties acting on the organisation's behalf.

Implementation Guidance

a. Organisation shall establish processes to ensure use of personal data collected is consistent with the purposes for which the individual has given consent, such as validating the use of the personal data through the data inventory map or data flow diagram.

b. Organisation should document all personal data handled using the data inventory map or data flow diagram to understand the lifecycle of personal data in the organisation. Organisation can make use of the data inventory map to validate that the collection, use and disposal of personal data is consistent with the purposes for which the individual has given consent.

7.5 Appropriate disclosure

The organisation shall have documented processes in place to ensure any disclosure of personal data collected is consistent with the purposes for which the individual has given consent. These processes shall apply when consent to collect data is obtained:

a) directly from the individual; and
b) through third parties acting on the organisation's behalf.

The organisation shall exercise due diligence to ensure that third parties to whom it discloses personal data will not use or disclose the personal data for any purposes other than that for which consent has been obtained.

Implementation Guidance

a. Organisation shall establish processes to ensure disclosure of personal data collected is consistent with the purposes for which the individual has given consent, such as validating using the data inventory map or data flow diagram.

b. Organisation should document all personal data handled using the data inventory map or data flow diagram to understand the lifecycle of personal data in the organisation. Organisation can make use of the data inventory map to validate collection, use and disposal of personal data is consistent with purposes for which consent was given.

c. Organisation shall establish contractual agreements with third parties to ensure that third parties whom it discloses personal data to for a specified purpose will not use or disclose the personal data for other purposes for which it had not obtained consent. For example, a confidentiality clause can be included in the contract to ensure personal data disclosed will only be used within the scope of the agreement and not be used or disclosed for other purposes.

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 12)

7.6 Exceptions

If consent is not obtained, the organisation can collect, disclose, and use personal data when acting under exceptions as allowed by laws or regulations.

Where required, use of exceptions shall be made clear to users, either through the organisation's privacy policy or by other notification methods.

Implementation Guidance

a. Organisation shall have documented policies and processes on the collection, use and disclosure of personal data without consent (including collection from source other than the individual), specifying the permitted purposes in the First and Second Schedules to the PDPA.

b. If organisation relies on an exception to collect, use or disclose personal data without consent, organisation is required to demonstrate and document how it collects, use or disclose personal data pursuant to an exception under the PDPA or as required/authorised under any other written law. For example:
   a) Organisation may rely on vital interests (pursuant to Paragraph 2 under Part 1 of the First Schedule to the PDPA) of the individual for the purpose of contacting the next-of-kin or a friend of any injured, ill or deceased individual. Organisation shall provide notifications (e.g. in the form of a physical document, on the organisation's website, etc) on such collection, use or disclosure of personal data.
   b) Organisation may rely on the Legitimate Interests Exception (pursuant to Paragraphs 2 to 10 under Part 3 of the First Schedule to the PDPA) for collection, use and disclosure of personal data without consent for the purposes such as detecting or preventing illegal activities (e.g. fraud, money laundering, etc) or threats to physical safety and security, IT and network security, preventing misuse of services, and carrying out other necessary corporate due diligence*. Organisation shall conduct risk assessment to identify and mitigate adverse effects for certain uses of personal data such as for legitimate interests
   c) Organisation may rely on the Business Improvement Exception (pursuant to Part 5 of the First Schedule and Division 2 under Part 2 of the Second Schedule) to enable organisations to

use/disclose, without consent, personal data that they had collected is in accordance with the Data Protection Provisions of the PDPA. Examples of business improvement purposes are improving, enhancing or developing new goods or services, identifying goods or services that may be suitable for individuals, learning or understanding behaviour and preferences of individuals, etc. To rely on the exception, organisation shall ensure:

i. The business improvement purpose cannot reasonably be achieved without using the personal data in an individually identifiable form.
ii. The organisation's use of personal data for the business improvement purpose is one that a reasonable person would consider appropriate under the circumstances
iii. The organisations involved in the sharing are bound by contract, agreement or binding corporate rules requiring the recipient(s) of personal data to implement and maintain appropriate safeguards for the personal data.

** This would apply to organisations that intend to conduct further and necessary corporate due diligence on customers, potential customers and business partners in addition to existing statutory requirements. For instance, the collection, use and disclosure of personal data for the consolidation of official watch lists.*

Other Information

a. Organisation may use the Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Annex C) to conduct the assessment if they rely on the Legitimate Interests Exception. Please refer to the Personal Data Protection Regulations 2021 and Paragraphs 12.64 – 12.69 of the Advisory Guidelines on conducting the assessment.

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 12)
- Data Protection Practices for ICT Systems (Section: Policy and Risk Management for ICT Systems)

7.7 Overseas transfer

7.7.1 Measures to track data transfer

The organisation shall have documented processes, such as data inventories, data maps or other methods, in place to maintain a comprehensive overview of personal data transferred overseas. The following aspects of the transfer shall be documented:

a) Data fields transferred;
b) The locations the data is transferred to, including the:
   i. country,
   ii. city; and
c) The recipients of the transferred data.

7.7.2 Recipients of the data

The organisation shall ensure that the overseas recipient is able to provide a level of data protection comparable to the organisation's national requirements prior to transferring data overseas.

7.7.3 Transfer mechanisms

The organisation shall have documented processes in place to transfer data overseas using data transfer mechanisms permitted under applicable laws and regulations.

Implementation Guidance

a. Organisation shall keep track of the personal data transferred overseas and the recipient(s) of the transferred data. This includes transferring personal data overseas to another company within the same corporation for centralised corporate functions, or to a DI for data processing.

b. Organisation shall document information such as the type of personal data, recipient and country where the personal data is transferred to using the data inventory map or vendor/third party list.

c. Organisation shall establish processes to ensure that the recipient organisation (including third parties such as service provider, DI, agent, or another company in the same group) is bound by legally enforceable obligations to provide a comparable standard of protection under the PDPA.

d. Legally enforceable obligations may include the recipient organisation holding a "specified certification" such as Asia Pacific Economic Cooperation Cross Border Privacy Rules ("APEC CBPR") System, and the Asia Pacific Economic Cooperation Privacy Recognition for Processors ("APEC PRP") System, or the recipient organisation is under:
   a) Any relevant data protection related law.
   b) Any other legally binding instrument, contract or binding corporate rules that imposes a standard of protection that is comparable to that under the PDPA, and which specifies the countries and territories to which the personal data may be transferred under the contract.

7.7.4 Transfer via a third party

Where a third party (e.g., data intermediary, agent) is engaged to transfer personal data overseas on its behalf, the organisation shall establish measures to verify that the third party complies with prevailing regulations during the transfer.

Implementation Guidance

a. Organisation shall put in place processes to ensure that the third party third party (e.g. data intermediary, agent) engaged to transfer personal data out of Singapore on its behalf, only transfers data to locations with comparable data protection regimes or has legally enforceable obligations to ensure a comparable standard of protection under the PDPA to comply with the Transfer Limitation Obligation. For instance, impose obligations that ensure adequate protection in the relevant areas in their processing contract.

b. Organisation which engages a Cloud Service Provider as a DI to provide cloud services shall comply with the Transfer Limitation Obligation in respect of any overseas transfer of personal data when using the cloud services. This is regardless of whether the CSP is located in Singapore or overseas.

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 19)

- Guide on ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows
- Advisory Guidelines on the Personal Data Protection Act for Selected Topics (Chapter 8)

CLAUSE 8: CARE OF PERSONAL DATA

8.1 Appropriate protection

8.1.1 Required security policies, practices and measures

The organisation shall have appropriate security policies, practices, and measures in place to secure personal data in its possession or under its control, to prevent:

a) unauthorised actions including:
   i. access,
   ii. collection,
   iii. use,
   iv. disclosure,
   v. copying,
   vi. modification,
   vii. disposal; and
b) the loss of any storage medium or device on which personal data is stored.

The organisation shall ensure that where a third party (e.g., data intermediary) is engaged to manage personal data, its practices are sufficiently secure to at least meet the organisation's internal security policies, practices, and measures (see 8.1.3).

Implementation Guidance

a. Organisation shall have security policies, practices and implemented appropriate security arrangements to protect personal data in its possession or under its control to prevent (a) unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored.

b. When engaging a third party (e.g data intermediary), organisation shall ensure appropriate protection and retention of the personal data processed by its third party through a contract, using standard contractual clauses in contracts and processing agreements with third party organisations to ensure protection for personal data. Refer to 8.2 for requirements under Working with Third Party.

8.1.2 Developing security policies, practices and measures

Security policies, practices, and measures shall be developed based on relevant risk assessments and can be in the form of:

a) physical safeguards;
b) technical safeguards; or
c) administrative safeguards

Implementation Guidance

a. Organisation shall implement appropriate security measures to ensure its information security objectives are met. Security measures are mechanisms implemented to prevent, detect, rectify or

minimise security risk to assets and can be classified as administrative, physical and technical measures. The following are examples of the types of security measures:

Administrative measures refer to policies, processes, or guidelines setting out an organisation's information security objectives. For example:

a) Requiring employees to be bound by confidentiality obligations in their employment agreements.
b) Implementing robust policies and procedures (with disciplinary consequences for breaches) regarding confidentiality obligations.
c) Conducting regular training sessions to staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data.
d) Ensuring only appropriate amount of personal data is held, as holding excessive data will increase the efforts required to protect personal data.

Physical measures refer to mechanisms used to prevent or detect unauthorised access to physical areas or assets. For example:

a) Marking confidential documents clearly and prominently.
b) Storing confidential documents in locked file cabinet systems.
c) Restricting employees' access to confidential documents on a need-to-know basis.
d) Ensuring proper disposal of confidential documents that are no longer needed, through shredding or similar means. The measures for secure disposal should be proportional to the sensitivity of that information.
e) Installing appropriate physical security perimeters and entry measures, such as fences, security gantries, biometric door access, etc.

Technical measures refer to the use of information technologies to protect assets. For example:

a) Ensuring computer networks are secure, such as equip networks with defence devices eg firewalls to protect your computer network connected to the Internet
b) Monitor, encrypt and restrict communications between environments to only authenticated and authorised connections
c) Restrict access to specified external IP addresses and ensuring remote desktop is used behind a secure virtual private network ("VPN")
d) Adopting appropriate access controls based on the sensitivity of the data.
e) Establishing an appropriate password policy, with at least 8 alphanumeric characters. Implementing protection systems such as anti-virus systems, intrusion detection systems, firewalls, etc.
f) Encrypting personal data to prevent unauthorised access. For example, consider database repositories encryption or encrypt datasets containing sensitive personal data
g) Use a one-time password ("OTP") or 2FA/MFA for admin access to sensitive personal data records or large volumes of personal data.
h) Ensure that personal data in your organisation's possession are regularly backed up according to the backup policy
i) Activating self-locking mechanisms for the computer screen if the computer is left unattended for a certain period.

j) Installing appropriate computer security software and using suitable computer security settings.
k) Conducting website security testing to help detect web vulnerabilities such as penetration testing and/or vulnerability assessments.
l) Applying secure connection technologies or protocols, such as TLS, to websites and web applications that handle personal data. For example, use HTTPS instead of HTTP
m) Using the right level of email security settings when sending and/or receiving highly confidential emails.
n) Updating computer security such as installation of latest software patches regularly.
o) Ensuring that IT service providers are able to provide the requisite standard of IT security.

For more security measures, refer to the PDPC Guide on Data Protection Practices for ICT Systems

8.1.3 Risk assessment approach for security policies

The organisation shall assess the likelihood of harm that can result from any form of unauthorised access, processing, erasure or other use, taking into account the context in which the personal data is held.

The security policies, practices, and measures shall assess the severity of harm that can result from any form of unauthorised or accidental access, processing, erasure or other use, based on the:

a) type of personal data;
b) sensitivity of personal data; and
c) volume of personal data.

Implementation Guidance

a. Organisation shall demonstrate and document that the security arrangements implemented are reasonable and appropriate under the circumstances, supported by relevant risk assessment or based on legal requirement. This should include institute a risk management framework to identify security threats to repositories or datasets containing personal data, assess the risks involved and determine the controls to mitigate or minimise such risks.

b. They should be assessed by taking into consideration the nature of the personal data, how the personal data has been collected (i.e. physical or electronic) and the possible impact to the individual if an unauthorised person obtained, modified or disposed the personal data. For example, in the employment context, it would be reasonable to expect a greater level of security for highly confidential employee appraisals as compared to more general information about the projects an employee has worked on.

c. When assessing whether information security arrangements are adequate, organisation should consider the following factors:
   a) Nature of the personal data held by the organisation and the possible harm that might result from a security breach.
   b) Size of the organisation and the amount and type of personal data it holds.
   c) Who within the organisation has access to the personal data.

d) Whether the personal data is or will be held or used by a third party on behalf of the organisation.

8.1.4 Risk assessment of information systems and management processes

Where relevant, risk assessment shall include information systems and information management processes, such as but not limited to:

a) website/web application security testing (penetration testing and/or vulnerability assessments);
b) network security;
c) software design;
d) information processing;
e) data storage;
f) data transmission; and
g) data disposal.

Implementation Guidance

a. Organisation shall conduct relevant risk assessments to identify, assess and address personal data protection and security risks based on the organisation's systems and implement appropriate technical or other relevant measures to safeguard against data protection risks. For example:
   - Conduct regular security scan or penetration test to detect vulnerabilities and non-compliance with organisational standards
   - Encrypt or password protect emails or documents containing personal data
   - Implement measures to ensure that system logs are reviewed regularly for security violations and possible breaches.
   - Use network proxies to restrict employee access to known malicious websites

8.1.5 Implementing security policies, practices and measures

The organisation shall define and allocate security responsibilities for security policies, practices, and measures. In addition, appropriate training (see 6.8) shall be conducted and provided to employees on implementing these measures.

The organisation shall ensure that these security policies, practices and measures are regularly:

a) monitored;
b) reviewed;
c) updated; and
d) endorsed by the management.

Implementation Guidance

a. Organisation shall assign security responsibilities to relevant stakeholders in accordance with its security policies and with the details documented. Examples of security responsibilities include:
   a) Overall accountable for the development, implementation and management of the data protection programme.
   b) Carry out specific information security processes and management activities, including establishing, enforcing and updating Information and Communications Technology (ICT)

security policies, standards and procedures, and establishing end user policies to prevent misuse of ICT systems.

c) Conduct compliance audits to ensure adherence with the information security policies and practices.

b. Organisation shall communicate to relevant stakeholders on their security responsibilities and provide the necessary training to ensure they can carry out the roles effectively. Organisation shall put in place processes to monitor the awareness level of the employees. Examples of communication channels include:

a) Employees: Security Policy signed by employees, regular briefing or staff training through various training programmes (i.e. courses or online videos).

c. Organisation shall monitor and conduct regular (e.g. annually) reviews to update security policies, practices and IT security measures to ensure they are up-to date. The updates shall be documented and endorsed by management.

d. The reviews should keep abreast of the changes and developments within (e.g. new systems or processes, feedback from stakeholders, etc) and outside the organisation (e.g. emerging new technologies, revisions to relevant laws and regulations, international or industry guidelines, etc).

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 17)
- Data Protection Practices for ICT Systems
- Guide to Printing Processes for Organisations
- Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data
- Guide to Managing Data Intermediaries

8.1.6 Updates to security policies, practices and measures

The organisation shall communicate relevant security policies, practices, and measures—including reviews and updates—promptly to internal and external stakeholders when necessary.

Implementation Guidance

a. Organisation shall establish processes to communicate security policies, practices, and measures, including updates promptly to relevant internal and external stakeholders to ensure they are kept apprised, through mechanisms such as:

- Employees: Providing easily accessibility of the security policy via the organisation's intranet/employees' handbook, regular circulars to employees to generate awareness of security practices and measures
- Third Party Vendors: Agreements with third party vendors on their security responsibility to ensure reasonable security arrangements are in place to protect personal data.

8.1.7 Verification on effectiveness of security measures

8.1.7.1 Scope of verifications

The organisation shall have appropriate policies and processes in place to test and verify the effectiveness of security measures regularly, or when risk assessment outcomes change, to protect personal data from:

a) unauthorised access;
b) collection;
c) use;
d) disclosure;
e) copying;
f) modification;
g) disposal; or
h) similar risks

8.1.7.2 Processes for verification

The organisation's policies and processes for testing and verifying security effectiveness should include, but not be limited to, the following activities:

a) Regular ICT scans and tests such as penetration testing; and/or
b) Vulnerability assessment on the organisation's system and website.

The level of testing shall be commensurate with the type, sensitivity and volume of personal data collected. Some types of data can require extensive testing.

Implementation Guidance

a. Organisation shall establish policies and processes and conduct reviews to verify the effectiveness of the security measures implemented (i.e. administrative, technical and physical measures as set out in 8.1.1) on a regular basis.

b. Examples of security measures:
   - Performing periodic security patching to fix potential vulnerabilities.
   - Conducting periodic penetration testing or vulnerability assessments on IT applications and databases to identify and help address cyber security vulnerabilities.
   - Conducting internal ICT audits or engaging an independent auditor to assess effectiveness of the security safeguards.
   - Applying prompt remedial actions to detect security vulnerabilities and any non-compliance with established policies and procedures.
   - Implementing measures to ensure ICT system logs are reviewed regularly for security violations and possible breaches, etc.

c. It is important to ensure the level of testing for security measures commensurate with the volume and sensitivity of the personal data being collected and processed. For example:
   - Type of data: Basic contact information might need less rigorous testing compared to financial or health data.
   - Sensitivity: Highly sensitive data like medical records, biometric information, or financial details typically require more extensive testing to ensure robust protection.

- Volume: Large datasets generally pose a greater risk if breached, thus warranting more comprehensive testing.
- Regulatory requirements: Certain types of data are subject to specific regulations (e.g., PCI DSS, MAS TRM, etc.) which may dictate minimum testing standards.

8.1.7.3 Management review of security measures

The results of the tests shall be reported to the management upon verification by the testing team. The organisation shall make appropriate modifications to security policies, practices, and measures periodically, based on the results of the tests.

These modifications should address new and changing threats and vulnerabilities in current or newly developed systems.

Implementation Guidance

a. Organisation shall make appropriate modifications and update its security policies, practices and measures based on the verification results from the security measure reviews and report the verification results and modifications to the management through an audit report or action plan.

Reference

- Data Protection Practices for ICT Systems (Section: SOP/IT Operations)

8.2 Working with third parties

8.2.1 Engagement phase

8.2.1.1 Defining responsibilities

The organisation shall have a clearly defined process for establishing contracts with third parties to whom it discloses personal data, or who are engaged to process personal data on its behalf (e.g., data intermediaries), that clearly defines the responsibilities of the third party with respect to the personal data.

Implementation Guidance

a. Organisation shall establish contractual agreements with its third parties to whom personal data is transferred to, to ensure reasonable security arrangements are in place and responsibilities to protect personal data are clearly defined. Contractual agreements with the third parties may include:
   a) Appointing an individual(s) to be responsible for overall compliance with the data protection requirements.
   b) Defining the purpose of collection, use and disclosure of the personal data limited to fulfilling its obligations and providing the services required in the agreement.
   c) Creating policies and procedures for the handling of personal data and complying with their contractual obligations.
   d) Giving the organisation the right to monitor the compliance of the third party relating to the contractual terms.

e) Restricting the third party from further transferring or disclosing organisation's personal information without the explicit written instruction or approval of the organisation.
f) Seeking evidence or declaration from the third party that it has processes in place (e.g. perform risk assessments) to assess sub-contractor's data handling practices and ensure it complies with the data protection requirements stipulated in the contract.
g) Making reasonable security arrangements to meet the required level of protection of the personal data (to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks).

b. When engaging a CSP, organisation shall review the service provider's data processing or equivalent agreements and security policies to ensure they meet the standards of protection in processing personal data as DIs (e.g. industry standards like ISO27001, Tier 3 of the Multi-Tiered Cloud Security (MTCS) Certification Scheme, etc).

8.2.1.2 Aligning requirements

The organisation shall verify that data managed by the third party undergoes an equivalent level of risk assessment and be protected by appropriate safeguards by the third party (see 8.1.2 and 8.1.3) throughout the entire duration of their contract.

Implementation Guidance

a. Organisation shall establish processes such as seeking evidence or declaration from third parties that the security arrangements (in the form of physical, technical or administrative safeguards) in place are reasonable and appropriately supported with relevant risk assessment or based on legal requirement. For example:
   a) Require third parties to provide list of security arrangements supported with relevant risk assessment.
   b) Conduct due diligence through questionnaire or checklist to assess if their security arrangements are reasonable and appropriate.
   c) Include appropriate security arrangements in the contract agreements with third parties.
   d) Check third parties' track record, for example to consider whether the third parties' data protection and security practices are subject to regular external reviews and validation, such as the Data Protection Trustmark ("**DPTM**") Certification or other forms of certification.

b. When assessing whether third parties' security arrangement (in the form of physical, technical or administrative safeguards) are adequate and proportionate to the type of the personal data disclosed to them, organisation shall consider the following factors:
   a) Nature of the personal data disclosed/handled by the third parties and the possible harm that might result from a security breach.
   b) Volume and sensitivity of personal data disclosed/handled by the third parties.

Other Information

a. For outsourcing of IT operations, an organisation may consider security measures such as regular security patching which keep security measures current against external threats. Other security measures are conducting regular penetration tests on IT applications and databases to fix

potential vulnerabilities. For good practices on protecting electronic personal data, refer to the PDPC's Guide to Securing Personal Data in Electronic Medium.

8.2.1.3 Verifying compliance

The organisation shall have documented processes in place to verify that third parties engaged by the organisation meet their contractual obligations with respect to personal data.

Implementation Guidance

a. Organisation shall establish processes to ensure third parties abide by their contractual obligations, such as:
   a) Ensuring third parties have created policies for complying with their contractual obligations with respect to personal data.
   b) Ensuring third parties are complying with their own policies for handling personal data.
   c) Reviewing and auditing third parties' policies and procedures with respect to handling of personal data.

b. Examples of how organisation can evaluate its third parties:
   a) Third party provides self-assessments through questionnaire or checklist to ensure compliance with the contractual obligations.
   b) Third party self-certifies that its practices meet the organisation's requirements based on internal audits or other procedures.
   c) Third party provides audit or similar report, certification assessed by an independent auditor.
   d) Organisation performs audits and on-site inspections of the third party to verify that the third party (particularly DI) is carrying out its roles and responsibilities properly, especially when processing large amount of sensitive personal data over long periods.
   e) While audits and inspections are put in place to monitor and evaluate the third parties' operations, simulations and table-top exercises should be considered to test out the effectiveness of ad-hoc incident reporting and remediation plans.
   f) Regular meetings with key members of the third parties to ensure that its operations are going according to contractual arrangements and the agreed SOPs.
   g) Proactive monitoring of third parties includes reviewing document database logs and system logs, and monitoring access, to identify possible unauthorised access or disclosure.

8.2.2 Contractual obligations

8.2.2.1 Breach notifications

The organisation shall have arrangements in place with third parties engaged by the organisation to notify the organisation promptly when they become aware of a security breach affecting the organisation's personal data.

8.2.2.2 Rectification actions

Third parties engaged by the organisation shall address and rectify the security failure as soon as practicable.

Implementation Guidance

a. Organisation shall establish and document the processes with third parties (i.e. DIs, vendors, etc) to notify organisation in the event of a data breach and rectify the security failure as soon as practicable when they are aware of the breach of data. The contractual agreement shall:
   a) Establish an escalation process with third parties to notify organisation without undue delay from the time they are aware that the data breach has occurred.
   b) Include breach notification obligation and requirements to cover incident investigation and management and for third parties to assist organisation in containing/assessing the breach.
   c) In the event of a data breach, organisation should put in place drawer plans for data breach management for their third parties to take remedial actions to address the data breach.

8.2.3 Post-contract obligations

Upon the expiry or cessation of the contract between the third-party and the organisation, the third-party shall either retain the data securely for the stipulated retention period or securely dispose of the data held (see 8.3 and 8.4).

The appropriate course of action to be taken shall be verified with the organisation prior to the expiry or cessation of the contract.

Implementation Guidance

a. Organisation shall establish the retention period of data processed by third-party organisation. The contractual agreement shall
   - Establish the stipulated retention period or whether the data should be securely disposed or anonymised by the third-party organisation.
   - In the event of a change in third party, the organisation should ensure that any data migration or transfers of data from one third party to another is done in a secure manner.

Other information

Under exit management, organisation should ensure all work done by the third party is fully documented and handed over upon completion of the project. For IT-related projects such as data migration, the documentation could include information such as the database mapping, extraction, transformation and loading scripts, verification test scripts and test results.

8.2.4 Record keeping

The organisation shall maintain a record of third parties to whom it disclosed personal data, including:
   a) purposes;
   b) contracts;
   c) requirements; and
   d) applicable time period for the contract or agreement.

Implementation Guidance

a. Organisation shall document and keep track of all third parties whom personal data are disclosed to. This includes disclosing personal data to another company within the same group for centralised corporate functions, a service provider for provision of services, or to a DI for data processing.

b. Organisation shall document the name of vendors, contractual period, type of personal data, and country (if any data transferred overseas) of the personal data transferred/disclosed to using data inventory map or vendor/third party list.

Reference

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Paragraphs 6.15 - 6.34)
- Data Protection Practices for ICT Systems (Section: SOP/IT Operations)
- Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data
- Guide to Managing Data Intermediaries

8.3 Appropriate retention

8.3.1 Data retention policies

8.3.1.1 Scope of data retention policies

The organisation shall implement an appropriate data retention policy for each set or type of personal data it possesses or controls. For each data set or type, the data retention policy shall define:

a) mechanisms for tracking and monitoring the data retention period to ensure policy compliance;
b) approaches for the secure permanent disposal of data by the organisation or data intermediary offering destruction services; and
c) retention periods, including retention by a third party such as data intermediary or agent.

8.3.1.2 Purposes of data retention

The data retention policy shall ensure that:

a) personal data is retained only for as long as necessary for the purpose for which it was collected; or
b) there is a legal or business purpose for its retention.

Implementation Guidance

a. Organisation shall establish a data retention policy and set out its approach to retaining personal data. The retention periods for various types of personal data shall be based on the purposes for which the personal data was collected and other legal or business purposes. For example:
   a) Personal data may be retained so long as one or more of the purposes for which it was collected remains valid.
   b) Personal data must not be kept by an organisation on a "just in case" basis where the purposes have not been notified to the individual.
   c) Other legal or business purposes such as personal data is required for an ongoing legal action; to comply with the organisation's obligations under other applicable laws; to carry out its business operations, such as to generate annual reports, or performance forecasts; for research, archival, historical, artistic or literary purpose(s) that benefits the wider public or a segment of the public.

b. Organisation shall document the retention period with its respective purposes in the retention schedule, data inventory map, or other appropriate forms. Organisation should have appropriate retention periods for different types of personal data.

c. Organisation shall implement processes to ensure it ceases to retain personal data or documents containing personal data in its possession or under its control (including personal data disclosed to third parties), as soon as the purpose for which personal data was collected is no longer being served and retention is no longer necessary for legal or business purposes.

d. Organisation shall clearly define, document and inform via contractual agreements or other available means on the data retention periods, data disposal methods and mechanisms for various sets and types of personal data disclosed to third parties (e.g. DIs, vendors etc), so that third parties can cease to retain personal data when the purpose of the data is no longer being served and retention is no longer necessary for legal or business purposes.

Reference:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 18)
- Data Protection Practices for ICT Systems (Section: ICT Controls)

8.3.2 Provision of information to individuals

The organisation shall have documented processes in place to provide to individuals, upon request, with information about the duration and the purposes for which their personal data is retained.

The organisation shall have in place a process to provide confirmation to individuals, upon request, that it no longer retains their personal data.

Implementation Guidance

a. Organisation shall implement processes to communicate to all individual's information about the duration and the purposes for which their personal data is retained and disposed by the organisation once the retention period is over. Organisation should also have a mechanism to allow individuals to query about its data retention policy.
   a) Employees: Data protection policy signed by employees, staff handbook, company intranet or other forms.
   b) Customers: Privacy notice on the organisation's website, DPO contact details on the organisation's website or other forms.
   c) Job Applicants: Privacy notice on the organisation's website, DPO contact details on the organisation's website or other forms.

b. Organisation shall provide contact details of the DPO for individuals to request for information about the retention and disposal of their personal data on its website or in its policies (e.g. data protection policy signed by employees).

Reference:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 18)

8.3.3 Unsolicited personal data

Where unsolicited data has been collected and the organisation is unable to determine if its collection use, disclosure, or retention is appropriate, the organisation shall have documented processes in place to cease:

a) retention;
b) use; and
c) disclosure of the data.

Implementation Guidance

a. Organisation shall establish a policy and implement processes to cease retention, use or disclosure of personal data it did not solicit, such as:
   a) Deleting unsolicited personal data or document containing personal data received via organisation's generic email immediately.
   b) Performing regular housekeeping of personal data in system databases or relevant documents after reviewing the purposes.
   c) Anonymisation of personal data such that the individual can no longer be identified directly or indirectly by the organisation.

8.3.4 Review of personal data retention policies and periods

The organisation shall have documented processes to periodically and systematically review its personal data retention periods to ensure that only personal data currently necessary for its business or by law are retained.

The organisation shall conduct ad-hoc reviews of the retention periods when there are significant changes to business operations, products, or services.

Implementation Guidance

a. Organisation shall have a policy to review the personal data it holds on a regular and ad-hoc basis to determine if the personal data is still necessary for business or legal purposes. The review process should be documented and endorsed by management.

b. The reviews should keep abreast of the changes and developments within (e.g. new systems or processes, feedback from stakeholders, etc) and outside the organisation (e.g. emerging new technologies, revisions to relevant laws and regulations, international or industry guidelines, etc).

Reference:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 18)
- Data Protection Practices for ICT Systems (Section: ICT Controls)

8.4 Appropriate disposal

8.4.1 Triggers for disposal

The organisation shall have appropriate processes in place to cease retention of documents containing personal data, or remove the means by which personal data can be associated with particular individuals, as soon as it is reasonable to assume that:

a) the purpose for which the personal data was collected is no longer served by its retention; and
b) retention is no longer necessary for legal or business purposes.

Implementation Guidance

a. Organisation shall implement processes to cease retention of personal data and/or documents containing personal data (including those held by agents/DIs) when the purpose for which the personal data was collected is no longer served by retention of the personal data, and retention is no longer necessary for legal or business purposes. For example:
   a) Return documents to the individuals once there are no business or legal purposes for the storage of these documents.
   b) Transfer the document to another person on the instructions of the individual.
   c) Anonymise the personal data (e.g. pseudonymisation, aggregation, replacement, data reduction, data suppression, data shuffling, masking, etc) to ensure that it cannot be re-identified.
   d) Locate and remove or redact specified personal data about an individual (e.g. removing credit card numbers after the transaction is complete).
   e) Destroy personal data stored on paper by shredding, pulping or disposing them in an appropriate manner. The measures for secure disposal should be proportional to the sensitivity of that information.
   f) Perform physical disposal of hard disks or other known methods of destruction of storage media, such as degaussing and incinerating, when secure deletion, erasure or deletion of personal data stored on the electronic media is not possible.

8.4.2 Methods to cease to retain personal data

The organisation shall determine appropriate methods for data:
a) disposal;
b) destruction; or
c) anonymisation.

8.4.3 Preventing data recovery

Where personal data is disposed of or destroyed, the organisation shall take appropriate measures to ensure that it cannot be recovered.

Implementation Guidance

a. Organisation shall implement appropriate data disposal, destruction or anonymisation methods to ensure documents are completely destroyed, disposed or deleted in an irretrievable manner, and anonymised data does not identify any particular individual. Examples of data disposal, destruction or anonymisation methods include:
   a) Hard copies documentation: Destroy the documents using a shedder (e.g. cross-cutting instead of straight-cut shredder should be used. For shredding of personal data on paper, the DIN 66399 standard recommends the use of at least a level P-3 cross-cut shredder, which shreds paper into particle size of maximum 320mm^2)

b) CD-ROMs, DVDs & Tapes: Destroy CD-ROMs, DVDs or tapes by cutting them up with scissors or using devices designed to shred them.
c) USB, Hard Drives: The hardware (USB, Hard Disk) must be physically destroyed (e.g. degaussing, etc) after secured deletion of the data.
d) Data in shared folders: Organisation shall implement clean folder policy, perform an inventory for all files containing personal data and delete old data that is longer required (especially unstructured files) at periodic intervals.
e) Voice recordings/video images: All recordings should be deleted from the system after a reasonable timeframe (e.g. 24 months).
f) Personal data stored on mobile devices: Conduct periodic reviews of all personal data on devices and delete old data that is longer required.
g) Anonymisation of data: Where there is a need to keep the data beyond the retention period, review and anonymise records to prevent re-identification to an individual. Refer to PDPC's Advisory Guidelines on the Personal Data Protection Act for Selected Topics (Chapter 3) for more techniques on anonymisation.

8.4.4 Disabling traceability

Where personal data is anonymised, the organisation shall take appropriate measures to ensure that individuals cannot be traced and identified based on the remaining information.

Implementation Guidance

a. When determining whether a dataset is anonymised, the organisation should consider whether there is a possibility that an individual can be identified from the dataset when it is combined with other information that the data recipient has or is likely to have access to, by carrying out an assessment of the risk of re-identification.

b. For data to be considered anonymised, the following measures should be considered:
   (i) All direct identifiers should be removed
   (ii) All indirect identifiers that can be used to re-identify individuals when matched with publicly available or proprietary information that the organisation knows the data recipient has access to, should be altered or removed to prevent re-identification from the data.
   (iii) Additional safeguards4 may be implemented by the data recipient to restrict access and use of the anonymised data to reduce the risks of disclosure and thus risks of re-identification.
   (iv) Stringent internal safeguards should be implemented on the set of information (e.g., identity mapping tables or other datasets containing linkable information) that can be used to re-identify individuals from the anonymised data.
   (v) Periodic review should be conducted, particularly where anonymised data is disclosed over a period of time in an ongoing relationship, to ensure that the risk of re-identification from the anonymised data is minimised and acceptable.

More information

Refer to PDPC's Advisory Guidelines on the Personal Data Protection Act for Selected Topics (Chapter 3) for more techniques on anonymisation.

8.4.5 Disposal by third parties

Where third-party service providers are engaged to dispose of, destroy, or anonymise personal data, the organisation shall ensure that the personal data is not disclosed to unauthorised parties during the entire process.

Implementation Guidance

a. Organisation shall establish contractual agreements with third party service providers that provide personal data disposal/anonymisation services to comply with the obligations under the PDPA, which should include:
   a) Having requirements or standards for proper secure disposal of personal data once the retention period is over.
   b) Requiring an undertaking from the third party service providers not to attempt to re-identify the anonymised data or further disclosure of the anonymised data to another organisation.
   c) Having third party service providers take reasonable measures to protect the personal data from disclosure to unauthorised parties during the entire disposal and/or anonymisation process.
   d) Ensuring that transfer complies with the Transfer Limitation Obligation under the PDPA where the paper (or physical medium) containing personal data is transferred overseas to be destroyed or recycled.

b. Organisation shall implement measures to ensure that the personal data is not disclosed to unauthorised parties during the entire disposal, destruction or anonymisation process. For example:
   a) Assess the service provider's overall processes and safeguards during transport, storage, and actual destruction.
   b) Assess whether containers are locked or secured during transit, whether policies for accident and incident reporting are in place, and whether the shredding/incineration/pulping facility has physical security.
   c) Keep records of collection and destruction confirmation.
   d) Supervise or document all collection (or handover) of waste items (e.g. paper documents).
   e) Witness the actual destruction, or even follow the third party's disposal vehicle, especially when sensitive personal data is involved.
   f) Ensure that the anonymisation techniques (e.g. pseudonymisation, aggregation, replacement, data reduction, data suppression, data shuffling, masking, etc) applied to the data set are robust and legal safeguards are in place to prevent attempts to re-identify and further disclose the anonymised data.

Reference:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 18)
- Data Protection Practices for ICT Systems (Section: ICT Controls)
- Advisory Guidelines on the Personal Data Protection Act for Selected Topics (Chapter 3)

8.5 Accuracy and completeness

8.5.1 Ensuring accuracy and completeness

The organisation shall have documented processes in place to ensure that reasonable effort is made to verify that data under its possession or control is both accurate and complete for the purposes of making decisions that affect the individuals to whom the personal data relates.

Implementation Guidance

a. Organisation shall have documented processes to verify and ensure personal data under its possession is accurate and complete for the intended purposes of use or disclosure, such as:
   a) Record personal data accurately which it collects (whether directly from the individual or through another organisation).
   b) Ensure personal data it collects includes all relevant parts thereof (so that it is complete).
   c) Take appropriate (reasonable) steps under the circumstances to ensure the accuracy and correctness of the personal data.
   d) Consider whether it is necessary to update the information.

b. Organisation should take reasonable steps to ensure the accuracy and correctness of the personal data, such as:
   a) Use systems or IT applications to validate information accuracy or adequacy during collection and when the information is stored, for example,
      - missing @ in email or insufficient digits of NRIC/mobile number or incompletion of mandatory fields will not be accepted.
      - provide users with a self-management facility (CRM), where possible, allow users to manage their personal data without requiring employee assistance to minimise human error.
      - periodically reminding users to view their details and acknowledge that they are correct through self-management facility.
   b) Require the individual to provide verbal or written declaration that the personal data provided is accurate and complete for example, via job application form, during interview, before submission of sign-up for new services, etc.
   c) Request individual to provide supporting documents (e.g. photo identification at job interview) in order to verify the information.

8.5.2 Corrections of data

Where there are reasonable grounds for believing that an individual's personal data is incorrect, the organisation shall have mechanisms to ensure the data is corrected before using it to make any decisions regarding that individual. Incorrect personal data includes any data that is:

a) inaccurate;
b) incomplete; or
c) out-dated.

Implementation Guidance

a. Organisation shall implement processes to ensure inaccurate/incomplete/out-dated personal data is corrected before using it to make the decision. For example:

a) Inform individual on any inaccurate/outdated personal data and require individual to provide updated data with supporting documents for verification of the accuracy of the personal data before using it.
b) Use systems or IT applications (e.g. CRM, HRM system, etc) to alert individual to update or review his/her personal data periodically to ensure information in the system is always up to date.

8.5.3 Maintaining data accuracy and completeness with third parties

The organisation shall exercise due diligence to ensure that personal data obtained from third-party sources is also accurate and complete.

Implementation Guidance

a. Organisation shall take appropriate steps to ascertain the accuracy and completeness of personal data it collects from third party sources. For example:
   c) Obtain confirmation from the third-party source that it had verified the accuracy and completeness of that personal data.
   d) Require an undertaking from the third party or through contractual agreement to ensure that personal data disclosed to the organisation is accurate and complete.

Reference:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 16)
- Data Protection Practices for ICT Systems (Section: ICT Controls)

8.5.4 Personal data disclosed to a third party organisation

8.5.4.1 Accuracy and completeness

The organisation shall have documented processes in place to make reasonable effort to ensure that any personal data it discloses to another organisation is accurate and complete for the intended purpose.

Where corrections have been made, the organisation may communicate these corrections to third parties to whom the personal data was disclosed.

Implementation Guidance

a. Organisation shall implement processes and mechanisms to ensure the accuracy and correctness of the personal data before disclosing to another organisation, such as:
   a) Use latest supporting documents to validate whether the data is accurate and up to date before disclosing personal data.
   b) Use systems or IT applications to validate information accuracy or adequacy where the information is stored.
   c) Use CRM, HRM systems to alert individual to update his/her personal data periodically to ensure information in the system are up to date before use or disclose to any third parties.
   d) Validate with individuals on the accuracy and currency of their personal data before any disclosure.

b. Organisation shall have a policy and documented processes to inform relevant third parties whom the personal data was disclosed to on the corrections to the personal data. Corrections can be communicated to third parties through the following mechanisms:
   a) Notify third parties (e.g. via email) on changes or deletion of personal data, if required, where there is inaccurate, incomplete or out of date information.
   b) Use systems or IT applications (e.g. CRM) to notify and share updated individual's personal data through the centralised system used by the organisation and the third parties (e.g. authorised reseller, agents/sales representatives use organisation's CRM system to manage their customers data, etc).

8.5.4.2 Corrections of data

When third-party organisations to whom the personal data was disclosed (e.g., data intermediaries, service providers, agents) identify personal data that is incorrect, they shall inform the organisation as soon as practicable. Incorrect personal data includes any data that is:

a) inaccurate;
b) incomplete; or
c) outdated.

Implementation Guidance

a. Organisation shall implement processes or mechanisms for third parties to notify the organisation as soon as practicable on any inaccurate personal data disclosed to them. Mechanisms could include:
   a) Obligations to notify the organisation on any inaccuracy, in the contractual agreement established with the third parties.
   b) Specify requirements in the Code of Conduct or Standard Operating Procedures documentation to ensure that third parties to whom personal data are disclosed to inform the organisation on any inaccurate, incomplete or outdated personal data.

Reference:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 16)
- Data Protection Practices for ICT Systems (Section: ICT Controls)

CLAUSE 9: SAFEGUARDING INDIVIDUAL RIGHTS

9.1 Withdrawal of consent

9.1.1 Provisions for the withdrawal of consent

The organisation shall have a documented process for allowing individuals to withdraw consent for their personal data to be:

a) collected;
b) used; and
c) disclosed.

9.1.2 Communicating the provisions for withdrawal of consent

9.1.2.1 Instructions regarding withdrawal of consent

The organisation shall provide instructions that are:

a) clear;
b) concise; and
c) easy to understand

These instructions shall be readily available to the individuals, for example through:

a) a data protection policy on the organisation's website; or
b) terms and conditions affixed in forms that collect consent.

Implementation Guidance

a. Organisation shall have a policy and documented processes to inform individuals about their right to withdraw consent through data protection notices or other mechanisms, in a clear, concise and accessible manner. The information should:
   a) Advise the individuals on the form and manner to withdraw their consent for specific purposes (e.g. click on an "unsubscribe" link within an electronic direct mailer for withdrawal of marketing communication, email organisation for withdrawal request or fill in a consent withdrawal form which can be found in the organisation's website, etc.).
   b) Inform the person to whom, or the means by which, the notice to withdraw consent should be submitted.
   c) Distinguish between necessary and optional purposes for the provision of the products/services. Individuals must be allowed to withdraw consent for optional purposes without concurrently withdrawing consent for the necessary services provided by the organisation.

b. Organisation shall make withdrawal of consent information readily available to all relevant stakeholders, such as:
   a) Employees: Staff handbook, HR portal, company intranet or other forms.
   b) Customers: Privacy notice on the organisation's website, marketing electronic direct mailer sent to individuals, service agreement with the individuals, customer's portal, or other forms.

c) Job Applicants: Data protection notice on the job application form or organisation's website, or other forms.

9.1.2.2 Providing information on consequences

The organisation shall inform individuals of the likely consequences of withdrawing consent before confirming and implementing the withdrawal.

Implementation Guidance

a. Organisation shall have documented policies to inform the individual of the likely consequences of withdrawing consent before giving effect to the withdrawal of consent through:
   a) Employees: Staff handbook, HR portal, company intranet or other forms.
   b) Customers: Privacy notice on the organisation's website, marketing electronic direct mailer sent to individual, service agreement with the individual, customer's portal, or other forms.
   c) Job Applicants: Data protection notice on the job application form or organisation's website, or other forms.

b. Upon receiving a notice of withdrawal, organisation should have a process to verify the identity of the individual and clearly inform the likely consequences of withdrawing consent, even if the consequences are set out in the service contract between the organisation and the individual or in the privacy notice on the organisation's website.

c. Examples of consequences for withdrawal of consent:
   a) Organisation would cease to collect, use or disclose the individual's personal data for the purpose specified by the individuals.
   b) Organisation may not be able to continue providing services to the individual.
   c) Legal consequences.

Reference:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Paragraphs 12.38 – 12.54)

9.1.3 Managing requests for withdrawal of consent

9.1.3.1 Execution timeframe

The organisation shall have a documented process in place for execution of the following within a reasonable timeframe:

a) Receiving;
b) Reviewing; and
c) Effecting requests for withdrawal of consent.

9.1.3.2 Communications regarding withdrawal of consent

The organisation shall clearly communicate the timeframe for giving effect to the withdrawal of consent to the requesting individuals. Determination of the timeframe shall be based on:

a) Amount of time need to give effect; and
b) manner in which notice of consent withdrawal was given.

9.1.3.3 Effecting the withdrawal

When giving effect to withdrawal of consent, the organisation shall have documented processes in place to cease its own collection, use, or disclosure of the individual's personal data, and to inform its data intermediaries or other third parties to do the same.

Implementation Guidance

a. Organisation shall have documented policies and implemented processes on how it handles requests for withdrawal of consent for collection, use and disclosure of personal data. The processes should include:
   a) Notifying individual on the timeframe for giving effect to the withdrawal of consent (e.g. 10 business days from the day the organisation receives the withdrawal notice).
   b) Informing the individual of the likely consequences of withdrawing consent on receipt of the withdrawal notice.
   c) Not prohibiting an individual from withdrawing consent if there are no legal consequences arising from such withdrawal.
   d) Ceasing to collect, use or disclose the individual's personal data upon withdrawal of consent.
   e) Informing its DIs and agents about the withdrawal and ensuring that they cease collecting, using or disclosing the personal data for the various purposes.
   f) Keeping records of all withdrawal requests received and processed, clearly documenting the outcome of the requests.
   g) Retaining the documents and records in accordance to the organisation's retention policy.

Reference:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Paragraphs 12.38 – 12.54)

9.2 Access rights

9.2.1 Provisions for individuals' access to their personal data

The organisation shall make available information on how individuals can request access to their personal data. The information provided shall be:

a) accessible;
b) clear; and
c) easy to understand.

9.2.2 Handling requests for access

The organisation shall have documented processes in place for receiving, reviewing, and responding to individuals' requests to access their personal data held or controlled by the organisation.

Implementation Guidance

a. Organisation shall have documented policies and processes to inform individuals on their right to request for access to their personal data through data protection notices or other mechanisms, in a clear, concise and accessible manner. The information should:

a) Advise the individual on the form and manner to submit a request to access their personal data including electronic or non-electronic means (e.g. email organisation for access request or fill in an access request form).
b) Inform the person to whom, or the means by which the access request should be submitted to.

b. Organisation shall make access request information readily available to all relevant stakeholders, such as:
   a) Employees: Staff handbook, employees' data protection notice, employee self-help portal, company intranet or other forms.
   b) Customers: Privacy notice on the organisation's website, service agreement with the individual, or other forms.
   c) Job Applicants: Data protection notice on the job application form or organisation's website, or other forms.

Reference:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 15)
- Guide to Handling Access Requests
- Data Protection Practices for ICT Systems (Section: ICT Controls)

9.2.3 Processing the access requests

Upon receiving requests from individuals to access personal data held or controlled by the organisation, the organisation shall have documented processes to:

a) verify the requesting individual's identity;
b) provide confirmation (upon request) that it holds personal data about the requesting individual;
c) provide an estimated timeframe to process and address the access request;
d) inform the individual in writing within 30 days of receiving the request if it is unable to provide access, and provide an expected timeframe for response; and
e) provide a written estimate of any associated fees for providing access to the personal data based on the format requested by the individual or provided by the organisation.

9.2.4 Nature of disclosure

The organisation shall have documented processes in place for informing, upon request, an individual on how their personal data has been used or disclosed.

Implementation Guidance

a. Organisation shall have documented policies and implemented processes on how it receives, reviews and responds to individual's requests to access his/her personal data within a reasonable timeframe. The processes should include:
   a) Providing individual the available avenues to request for access to his/her personal data (e.g. online feedback form, physical forms downloaded from the website, request via email, phone calls or walk-in, or employee self-help portal, etc).
   b) Soliciting sufficient details on the personal data the individual would like to access as part of the request (e.g. type of personal data and reason for requesting for access).

c) Upon receiving the request, organisation should exercise due diligence and adopt appropriate measures to verify an individual's identity and provide confirmation that organisation holds the personal data about the requesting individual.
d) In situations where a third party is making an access request on behalf of an individual, organisation should ensure that the third party has the legal authority to validly act on behalf of the individual.
e) Providing a response to an access request as soon as reasonably possible from the time the access request is received. If the organisation is unable to respond to an access request within 30 days after receiving the request, the organisation shall inform the individual in writing within 30 days by when it will be able to respond to the request.
f) Providing individual in writing the estimated fee imposed for providing access to the personal data (if any).

9.2.5 Rejecting requests for access

Where the organisation is rejecting a request for access, it shall:

a) provide a response to the requesting individual for access to the requested personal data or other requested information;
b) provide reasons for the rejection; and
c) preserve a complete and accurate copy of the personal data requested pursuant to an access request for a prescribed period after rejection of the request.

Implementation Guidance

a. When rejecting a request for access, organisation shall inform the individual the reason(s) where it has valid grounds not to provide access. For example, information could reasonably be expected to threaten the safety or physical or mental health of an individual other than the requesting individual, or individual refusal to pay the service fee process an access request, etc.

b. Organisation shall preserve a complete and accurate copy of the personal data requested for (a) at least 30 calendar days after rejection of the request, or (b) until the individual has exhausted his/her rights to apply for a reconsideration request to PDPC or appeal to the Data Protection Appeal Committee, High Court or Court of Appeal, whichever is later.

9.2.6 Documenting access requests

The organisation shall keep a record of all access requests received, indicating whether the access was provided or denied.

Implementation Guidance

a. Organisation shall keep a record of all access requests received and processed, document clearly information on whether the request for access was provided or rejected.

b. Record should include relevant details such as requestor name, date of request, reason for requesting, all correspondences between the individual and organisations, outcome and status of the request, etc.

Reference:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 15)
- Guide to Handling Access Requests
- Data Protection Practices for ICT Systems (Section: ICT Controls)

9.3 Provisions for corrections

9.3.1 Request for correction process

The organisation shall have documented processes in place to process an individual's request to correct their personal data. These procedures shall encompass:

a) receiving;
b) reviewing; and
c) responding to requests;

9.3.2 Providing information regarding corrections

The organisation shall make available information on how individuals can request correction of their personal data under its possession or control. The information provided shall be:

a) accessible;
b) clear; and
c) easy to understand.

Implementation Guidance

a. Organisation shall have documented policies and processes on how individuals may request for correction to their personal data through its data protection notice or other mechanisms, in a clear, concise and accessible manner. The information should:
   a) Advise the individual on the form and manner to submit a request to correct his/her personal data including electronic or non-electronic means (e.g. email organisation for correction request or fill in a correction request form).
   b) Inform the person to whom, or the means by which the correction request should be submitted to.

b. Organisation shall make correction request information readily available to all relevant stakeholders, such as:
   a) Employees: Staff handbook, employees' data protection notice, employee self-help portal, company intranet or other forms.
   b) Customers: Privacy notice on the organisation's website, service agreement with the individual, or other forms.
   c) Job Applicants: Data protection notice on the job application form or organisation's website, or other forms.

Reference:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 15)

9.3.3 Handling correction requests

The organisation shall have documented processes for handling an individuals' request to correct their personal data. The processes shall include the following:

a) Verification of the requesting individual's identity;
b) Determining that the information in question is under the organisation's:
   i. possession, or
   ii. control;
c) Providing, upon request, confirmation that organisation holds personal data about the requesting individual;
d) The estimated timeframe to process and address the correction request;
e) If individual consents, sending corrected personal data to other relevant organisations; and
f) The procedures for rejecting correction requests.

9.3.4 Executing corrections

Corrections to personal data should be made as soon as practicable, unless the organisation is satisfied on reasonable grounds that a correction should not be made.

Implementation Guidance

a. Organisation shall have documented policies and implemented processes on how it receives, reviews and responds to individual's requests to correct his/her personal data as soon as practicable. The process should include:
   a) Providing individual the available avenues to request for correction to his/her personal data (e.g. online feedback form, physical forms downloaded from the website, request via email, phone calls or walk-in, or employee self-help portal, etc).
   b) Soliciting sufficient details on the personal data the individual would like to correct as part of the request (e.g. type of personal data and supporting documents for update of data).
   c) Upon receiving the request, organisation should exercise due diligence and adopt appropriate measures to verify an individual's identity and provide confirmation that organisation holds the personal data about the requesting individual.
   d) In situations where a third party is making a correction request on behalf of an individual, organisation should ensure that the third party has the legal authority to validly act on behalf of the individual.
   e) Provide a response to the correction request as soon as reasonably possible from the time the access request is received. If an organisation is unable to respond to a correction request within 30 days after receiving the request, the organisation shall inform the individual in writing within 30 days by which it will be able to respond to the request.
   f) Not charging any fee to correct the personal data.
   g) Responding to correction request by correcting the personal data, or by informing the individual the reason where it has valid grounds not to make correction.
   h) Sending the corrected personal data (if individual consents) to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction request was made, unless the other organisations do not need the corrected personal data for any legal or business purpose.

i) Keeping a record of all correction requests received and processed, documenting clearly whether the request for correction was provided or rejected. Record should include relevant details such as requestor name, date of request, reason for requesting, reason of rejection (if any), all correspondences between the individual and organisations, outcome and status of the request, etc.

9.3.5 Objections to correction made

The organisation shall have documented processes for individuals to raise objections if they are dissatisfied with a refusal to correct their personal data. Where no correction is made, the organisation shall record the correction that was requested but not made.

Implementation Guidance

a. Organisation shall inform the individual the reason where it has valid grounds not to make correction. For example, opinion data kept solely for an evaluative purpose, any examination details such as results conducted by an education institution, a document related to a prosecution if all proceedings related to the prosecution have not been completed, etc.
b. Where no correction is made, organisation shall explain to the individual why it has decided that the correction should not be made, provide individuals a mechanism to raise objections and annotate reason why the correction, though requested, was not made.

Reference:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 15)
- Data Protection Practices for ICT Systems (Section: ICT Controls)