DPTM	Singapore Standards (SS714:2025)
Principle 1 Governance and Transparency	**6 Governance and transparency**
1.1.1.1 Organisation has policies and practices to address data protection obligations 1. There are appropriate policies and practices in place, in accordance with relevant laws, sectoral and international guidelines, on the management of personal data (including employee data) by the organisation and third parties engaged by the organisation (e.g. vendors, data intermediaries), including collection/use/disclosure of personal data, purposes for collection/using/disclosing personal data, notification of purposes etc. The policies and practices include management of special categories of personal data such as personal data of a sensitive nature.	**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.
	6.2.2 Implementation by third parties Third parties engaged by the organisation (e.g. vendors and data intermediaries) to transact or process data shall demonstrate that the relevant policies and practices as described above are established within their organisation.
2 There is appropriate governance structure for management oversight and endorsement for the organisation's policies and practices on the management of personal data developed and implemented by the organisation	**5.2 Management review** The organisation's management shall ensure that: a) responsibilities and authorities for relevant roles are assigned and communicated within the organisation; b) outcomes of regular monitoring of compliance of practices with policies at planned intervals is reported to the management, including: i. any gaps identified, ii. actions to improve compliance, or iii. remediation plans to improve compliance; and

DPTM	Singapore Standards (SS714:2025)
	c) resources needed for compliance with the requirements are available.
3 The policies and practices are communicated to all relevant internal and external stakeholders to whom the policies and practices apply. 4 The policies and practices are easily accessible and provided in a clear and concise manner, clearly worded and easy to understand by recipients of the information	**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 hires or temporary hires. Updates to data protection policies and practices shall be promptly communicated to employees and where relevant, third-party or temporary hires.
1.1.1.2 Organisation regularly reviews and updates its policies and practices 1. There is a process in place to regularly review, update and obtain management endorsement for updates to the policies and practices. 2. Regular reviews and updates to the policies and practices may, where relevant, take into account compliance with relevant laws, sectoral and international guidelines. 3. Updated policies and practices are communicated to all relevant internal (e.g. employees) and external stakeholders (e.g. vendors, consumers) as soon as reasonably possible	**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.
1.1.1.3 Organisation monitors compliance of practices with policies 1. There is a process in place to regularly monitor compliance of practices with data protection policies in a structured and timely way. This includes, where relevant, compliance of the policies by third parties engaged by the organisation (e.g. vendors, data intermediaries).	**6.3 Monitoring compliance and review of policies and practices** **6.3.1 Monitoring compliance** Compliance of practices with data protection policies shall be monitored in a structured and timely way. The monitoring process shall extend, where

DPTM	Singapore Standards (SS714:2025)
2. Outcomes of regular monitoring of compliance of practices with policies, including any gaps identified and actions/remediation plans to improve compliance, is reported to management.	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.
1.1.2.1 Organisation receives and responds to queries and complaints that may arise with respect to the organisation's management of personal data 1. There are processes in place to receive and respond to queries or complaints that may arise with respect to the organisation's collection, use or disclosure of personal data. 3. There are processes in place to respond to requests to disclose personal data to public agencies, courts and law enforcement agencies when required for purposes of investigations or proceedings under the PDPA or other written law.	**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 to requests from: • public agencies for the disclosure of personal data; and • courts and law enforcement agencies when required for investigations or proceedings under the prevailing law.
1.1.2.1 Organisation receives and responds to queries and complaints that may arise with respect to the organisation's management of personal data 2. Queries and complaints received are responded to in a timely manner, and in relation to complaints, the response includes an explanation of remedial action where relevant. Queries and responses are documented and retained for a reasonable period of time.	**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 action where relevant. Queries and responses shall be documented and retained for a reasonable period of time as determined by the organisation.
1.1.3.1 Organisation identifies, assesses and addresses personal data protection risks 1. There are policies and practices in place to conduct risk and impact assessments, such as the Data Protection Impact Assessment (DPIA), to identify, assess and address data protection risks, to meet the	**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

DPTM	Singapore Standards (SS714:2025)
organisation's operational functions, business needs and processes, and to comply with the PDPA. 2. Recommended action plans are developed and approved by management to mitigate or address identified risks, and implemented in a timely manner.	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.
1.1.3.2 Organisation considers data protection across the various stages of the design and development of a product, service, system or process 1. There are policies and practices in place to take into consideration the protection of personal data from the earliest possible design stage and throughout the operational lifecycle of a system, process, product or service. The organisation has in place necessary safeguards at every point of collecting, using, or disclosing the personal data. 2. Organisation takes steps to ensure that data protection settings protect users by default. This includes adopting an opt-in consent rather than opt-out approach. and having data protection settings that are easily accessible, clear and easy to understand.	**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 option; and ii. data protection settings that are accessible and easy to understand.
1.1.4.1 Organisation has a data breach management plan 1. There is a data breach management plan and process in place to comply with mandatory data breach notification requirements that includes: • Data breach management reporting structure of key relevant personnel in the organisation who would make time-critical decisions on the assessment and management of a data breach incident. • Timelines for reporting data breach incidents detected to the relevant personnel in the organisation. • Possible data breach scenarios for reporting the incident to the relevant personnel in the organisation, and action plans for responding, remediating and containing the data breach for these scenarios.	**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.

DPTM	Singapore Standards (SS714:2025)
• Assessment of risks and impact of the data breach to determine whether there could be serious consequences to affected organisations/individuals. • Assessment is conducted in a reasonable and expeditious manner of whether the data breach meets the specified criteria for notification under the PDPA and any other relevant laws, regulations or guidelines. • Notifying the affected individuals and/or the relevant regulators/enforcement authorities in compliance with the relevant laws/regulations. • Arrangements for Data intermediary/intermediaries to notify the organisation of the data breach. 2. Breach incidents are handled according to the data breach management plan and process set out by the organisation. 3. Communicate and ensure that all relevant internal and external stakeholders are aware of their roles in the data breach management plan	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. **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. relevant personnel within the organisation to report the incident; and ii. 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.
	6.6.3 Remediation for data breaches If the organisation has reported a breach within last two years of seeking DPTM certification, a self-assessment shall be conducted for each reported breach to establish if the remediation is complete.

DPTM	Singapore Standards (SS714:2025)
1.1.5.1 Organisation has designated one or more individuals to be responsible for ensuring organisation's overall compliance with the data protection obligations. 1. Organisation has appointed one or more individual(s) as a Data Protection Officer (DPO) to ensure organisation's compliance with the data protection obligations. 2. The DPO has received relevant training on data protection compliance with the PDPA (e.g. attended data protection training, courses, or obtained data protection certifications). 3. The DPO has clearly defined responsibilities to carry out his/her role. These include: • Keeping up to date with organisation's data protection policies and practices. • Ensuring organisation's compliance with data protection obligations. • Developing processes to manage data protection related queries and complaints from the public	**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. **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. **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).
1.2.1.1 The business contact information of at least one DPO is made available to the public 1. The business contact information of at least one DPO is made available and easily accessible by the public. **1.2.2.1 Data protection policies are provided or made available on request to external stakeholders** 1. There are processes in place to communicate or make available organisation's data protection policies to external stakeholders (e.g. customers, third party contractors) regarding the organisation's practices and handling of personal data on request. The information is provided in a clear and easily accessible manner.	**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. **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.

DPTM	Singapore Standards (SS714:2025)
1.3.1.1 Employees are aware of organisation's data protection policies and practices 1. There are processes in place to communicate data protection policies and practices to employees, and where relevant, third party hires and temporary hires. 2. Updates to data protection policies and practices are communicated to employees and where relevant, third party hires and temporary hires are also kept apprised in a timely manner.	**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.
1.1.3.2 Organisation provides relevant training to all relevant internal stakeholders to increase awareness of and compliance with data protection policies and practices There are processes in place to train internal stakeholders (e.g. existing employees and new hires) on organisation's data protection policies and practices, such as when there are changes or updates to the data protection policies and practices. The processes may include regular briefings to refresh the employees' knowledge of the policies and practices. Where relevant, this includes training employees to respond to queries or complaints relating to the organisation's handling of personal data.	**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 complains related to personal data, c) Data breach management plan, and d) Security policies and processes.
Principle 2 Management of Personal Data	**7 Management of personal data**
2.1.1.1 Organisation ensures that the personal data collected is necessary for the purpose 1. There are processes in place to ensure that only personal data (including, where relevant, personal data of a sensitive nature) necessary to meet the specified purpose, is collected.	**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.

DPTM	Singapore Standards (SS714:2025)
4. Where the collection involves sensitive data, (e.g. data that may result in significant harm to an individual if breached), organisation has processes in place to limit the collection of such data to necessary purposes identified in its data protection policy. 5. Organisation has identified the sources of personal data (e.g. directly from the individual, third parties collecting on organisation's behalf), types of personal data collected from individuals (e.g. customers, employees, contractors) and their respective purposes of collection.	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.
2.1.1.1 Organisation ensures that the personal data collected is necessary for the purpose 2. These purposes are appropriate and consistent with requirements under the PDPA. 3. Organisation conducts regular reviews to ensure that purposes for which collection of personal data are still necessary and appropriate.	**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.
2.1.2.1 Organisation notifies individuals of the purposes for collecting their personal data on or before collecting their personal data 1. There are processes in place to provide clear and concise notifications to individuals regarding purpose(s) on or before collecting their personal data (whether the collection is carried out by the organisation itself or through third parties acting on the organisation's behalf). 2. At the point of collection of personal data, organisation provides clear and concise notifications to individuals that their personal information may be disclosed to third parties. 3. The information relating to how individuals may exercise choice in the collection, use or disclosure of their personal data is easily accessible and provided in a clear and concise manner, clearly worded and easy to understand.	**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;

DPTM	Singapore Standards (SS714:2025)
2.2.1.2 Organisation notifies individuals if collection of personal data is required or optional to provide the product or service 1. Organisation provides notification to individuals that indicates if collection of their personal data is obligatory (e.g. governed/required under applicable laws or required in order to provide the product/service) or voluntary 2. Organisation's notification to individuals clearly indicates the 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 may exercise choice in the collection, use or disclosure of their personal data.
2.2.2.1 Organisation notifies and obtains consent from individuals to use or disclose their personal data for new purposes 1. There are processes in place to determine when there are new purposes for the collection, use and disclosure of personal data and updates the notification accordingly to reflect these new purposes. 2. Where personal data collected is to be used or disclosed for different purpose(s), there are processes in place to notify individuals of the new purpose(s) of use or disclosure when obtaining consent for the use or disclosure.	**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 obtaining consent for the use or disclosure.
2.3.1.1 Organisation obtains individuals' consent for the collection (and use or disclosure, where relevant) of their personal data 3. Organisation obtains valid consent from individuals for the collection, use or disclosure of the personal data, including express consent or deemed consent (by conduct, by contractual necessity or by notification), which the organisation relies on.	**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

DPTM	Singapore Standards (SS714:2025)
	c) by notification.
2.3.1.1 Organisation obtains individuals' consent for the collection (and use or disclosure, where relevant) of their personal data 1. There are processes and mechanisms in place for individuals to exercise choice in relation to the collection (and use or disclosure, where relevant) of their personal data, and this may include the individual providing consent.	**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.
2.3.1.1 Organisation obtains individuals' consent for the collection (and use or disclosure, where relevant) of their personal data 2. These mechanisms are easily accessible and provided in a clear and concise manner, clearly worded and easy to understand by the individual.	**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.
2.3.2.1 Organisation ensures that the person providing consent on behalf of an individual is validly acting on behalf of that individual 1. There are appropriate measures and mechanisms in place to ensure / verify that the person providing consent on behalf of an individual is validly acting on behalf of an individual	**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.
2.3.2.2 Organisation ensures that third party sources of personal data, had obtained valid consent from individuals 1. There are processes in place to establish contractual agreements with third parties to ensure valid collection of personal data.	**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.

DPTM	Singapore Standards (SS714:2025)
2. Organisation exercises due diligence to ensure that the third party source has obtained consent from individuals to collect, use or disclose their personal data for specified purposes.	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.
2.4.1.1 Organisation restricts use of personal data to purposes for which consent had been obtained 1. There are processes in place for organisation to ensure use of personal data collected (whether directly from the individual or through third parties acting on your organisation's behalf) is consistent with the purposes for which the individual has given consent.	**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.
2.5.1.1 Organisation restricts disclosure of personal data to purposes for which consent had been obtained 1. There are processes in place for organisations to ensure disclosure of personal data collected (whether directly from the individual or through third parties acting on your organisation's behalf) is consistent with the purposes for which the individual has given consent. 3. Organisation exercises due diligence 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.	**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. 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. 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.

DPTM	Singapore Standards (SS714:2025)
Exception clauses from 2.3.1.1, 2.4.1.1 and 2.5.1.1 2.3.1.1 Where consent is not obtained, organisation collects personal data pursuant to an exception under the PDPA or as required/authorised under any other written law. 2.4.1.1 Where consent is not obtained, organisation uses personal data pursuant to an exception under the PDPA or as required/authorised under any other written law. 2.5.1.1 Where consent is not obtained, organisation discloses personal data pursuant to an exception under the PDPA or as required/authorised under any other written law.	**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.
2.6.1.1 Organisation ensures that personal data is only transferred to overseas recipients that provide a comparable standard of data protection in accordance with requirements under the PDPA 1. Organisation keeps track of the personal data that is transferred overseas and the recipient(s) of the transferred data.	**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.

DPTM	Singapore Standards (SS714:2025)
2.6.1.1 Organisation ensures that personal data is only transferred to overseas recipients that provide a comparable standard of data protection in accordance with requirements under the PDPA 2. Organisation has processes in place to transfer data overseas using data transfer mechanisms permitted under the Personal Data Protection Regulations. 3. Where the organisation engages a third party (e.g. data intermediary, agent) to transfer personal data out of Singapore on its behalf, it has policies, practices and measures in place to ensure that the third party is transferring personal data in compliance with the PDPA.	**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. **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.
Principle 3 Care of Personal Data	**8 Care of personal data**
3.1.1.1 Organisation implements security polices, practices and measures to protect personal data and regularly reviews them to ensure relevancy and currency 1. Organisation has in place appropriate security policies, practices and measures to secure personal data in its possession or under its control to prevent (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored, whether the protection of personal data is carried out by the organisation or a third party engaged by the organisation	**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 (eg data intermediary) is engaged to manage personal data, its practices are sufficiently secure to

DPTM	Singapore Standards (SS714:2025)
	at least meet the organisation's internal security policies, practices and measures (see 8.1.3).
2. These policies, practices and measures are developed based on relevant risk assessments and legal requirements, and may be in the form of physical, technical or administrative safeguards. They will assess the proportionality by taking into account the type and sensitivity of personal data, context in which the personal data is held, and the likelihood and severity of harm that could result from any form of unauthorised or accidental access, processing, erasure or other use. Where relevant, these considerations may also extend into the information systems and management such as website security testing (penetration testing and/or vulnerability assessments), network, software designs, information processing, storage, transmission and/or disposal.	**8.1.2 Developing security policies, practices and measures** These 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. **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 **8.1.4 Risk assessment of information systems and management processes** Where relevant, this risk assessment should 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;

DPTM	Singapore Standards (SS714:2025)
	f) data transmission; and g) data disposal.
3. Organisation has defined, and allocated security responsibilities and training in accordance with these security policies, practices and measures. 4. Organisation ensures that these security policies, practices and measures are regularly monitored, reviewed, updated and endorsed by the management and are communicated to all relevant internal and external stakeholders in a timely manner.	**8.1.5 Implementing security policies, practices and measures** The organisation shall define and allocate security responsibilities for these security policies, practices and measures. In addition, appropriate training (see 6.8) shall be conducted and provided to staff member on the practice of these security policies, practices and 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. **8.1.6 Updates to security policies, practices and measures** The organisation shall communicate all relevant security policies, practices and measures—including reviews and updates—promptly to internal and external stakeholders when necessary.
3.1.2.1 Organisation ensures that all third parties that the organisation has disclosed personal data to, or are engaged to process personal data on its behalf (i.e. data intermediaries), protect the personal data in accordance with the PDPA 1. Organisation has processes in place to establish contracts, with third parties to whom it discloses personal data, where the responsibilities of the third parties with respect to the personal data, are clearly defined.	**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.

DPTM	Singapore Standards (SS714:2025)
2. Third parties may determine their level and extent of security arrangements based on relevant risk assessments and legal requirements, and may be in the form of physical, technical or administrative safeguards. They will assess the proportionality by also taking into account the type and sensitivity of personal data, context in which the personal data is held, and the likelihood and severity of harm that could result from any form of unauthorised or accidental access, processing, erasure or other use. Where relevant, these considerations may also extend into the information systems, and management such as network, software designs, information processing, storage, transmission and/or disposal.	**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.
3. Organisation has processes in place to ensure these third parties are meeting their contractual obligations with respect to the personal data.	**8.2.1.3 Verifying compliance** The organisation shall have documented processes in place to verify that third parties engaged by the organisation are meeting their contractual obligations with respect to personal data.
4. Organisation has in place arrangements with these third parties to notify the organisation promptly when they become aware of an occurrence of breach of data protection or security of organisation's personal data, and to address/rectify the security failure as soon as practicable.	**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.
	8.2.3 Post-contract obligations Upon the expiry or cessation of the contract between third-party organisation and data owner, 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).

DPTM	Singapore Standards (SS714:2025)
	The appropriate course of action to be taken shall be verified with the organisation prior to the expiry or cessation of the contract.
5. Organisation maintains a record of third parties to whom they disclose personal data and the purposes, contracts/requirements and applicable time period for the contract/agreement.	**8.2.4 Record keeping** The organisation shall maintain a record of third parties to whom they disclose personal data, including: a) purposes; b) contracts; c) requirements; and d) applicable time period for the contract/agreement.
3.1.3.1 Organisation verifies the effectiveness of security measures on a periodic basis 1. Organisation has in place appropriate policies and processes to verify effectiveness of security measures regularly or when risk assessment outcomes change, to protect personal data from unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. These should include, but not limited to: (a) conducting regular ICT scan and test such as penetration testing and or vulnerability assessments on the organisation's system and website (b) making appropriate modifications to security policies, practices and measures on a periodic basis, taking into consideration verification results performed and new and changing threats and vulnerabilities in current or newly developed systems. (c) reporting verification results of security measures to management.	**8.1.7 Verifying the 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.

DPTM	Singapore Standards (SS714:2025)
	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. **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. The modifications should address new and changing threats and vulnerabilities in current or newly developed systems.
3.2.1.1 Organisation sets out specific retention periods for various sets or types of personal data in its possession or under its control 1. Organisation has processes to implement an appropriate data retention policy setting out any mechanisms, approaches and retention periods for various sets or types of personal data in its possession or under its control, and where relevant, to third parties that the personal data is disclosed to. 2. The policy ensures that personal data is retained only for as long as necessary for the purpose for which it was collected, and there is a legal or business purpose for its 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 in its possession or under its control. 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.

DPTM	Singapore Standards (SS714:2025)
3.2.1.2 Organisation provides information to individuals about the retention of their personal data 1. Organisation has processes in place to provide to individuals upon request, information about the duration and the purposes for which their personal data is retained by the organisation. 2. Organisation has processes in place to provide to individuals, upon request, information about how the organisation will destroy all personal data once the retention period is over.	**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.
3.2.1.3 Organisation ceases to retain unsolicited personal data 1. Where relevant, organisation has processes in place to cease retention, use or disclosure of personal data it did not solicit and is unable to determine if such data can be collected.	**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.
3.2.1.4 Organisation regularly reviews the retention periods of personal data in its possession or control to ensure relevancy and currency 1. Organisation has in place processes to periodically and systematically review the retention policies and periods to ensure that only personal data necessary for its business or legal purposes are retained. 2. Organisation conducts ad-hoc reviews of the retention periods e.g. when there are significant changes to business operations, products or services.	**8.3.4 Review of personal data retention policies and periods** The organisation shall have documented processes to periodically and systematically review their 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.

DPTM	Singapore Standards (SS714:2025)
3.3.1.1 Organisation disposes of, destroys or anonymises personal data when it is no longer necessary to retain it for any business or legal purpose in a manner that the data cannot be recovered or re-identified 1. Organisation has in place appropriate processes to cease retention of documents containing personal data, or remove the means by which the 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 retention of the personal data, and b) retention is no longer necessary for legal or business purposes.	**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.
2. Organisation determines appropriate data disposal, destruction or anonymisation methods. Where personal data is disposed of or destroyed, organisation takes appropriate measures to ensure the personal data cannot be recovered. In the case of anonymised personal data, organisation takes appropriate measures to ensure that individuals cannot be re-identified.	**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. **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.
3. Where third party service providers are engaged to dispose, destroy or anonymise personal data, organisation takes reasonable measures to ensure that the personal data is not disclosed to unauthorised parties during the entire disposal, destruction or anonymisation process.	**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.

DPTM	Singapore Standards (SS714:2025)
3.4.1.1 Organisation ensures that personal data under its possession or control is accurate and complete for the intended purposes of use or disclosure 1. Organisation has processes in place makes reasonable effort to verify that personal data under its possession or control is accurate and complete for the purposes of making decisions that affects individuals to whom the personal data relates.	**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 affects individuals to whom the personal data relates.
3. Where there are reasonable grounds for believing that personal data to be used to make a decision affecting the individual is inaccurate, incomplete or out-dated, organisation has mechanisms to ensure the inaccurate/incomplete/out-dated personal data is corrected before using it to make the decision.	**8.5.2 Corrections for 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 which is: a) inaccurate; b) incomplete; or c) out-dated
2. Organisation exercises due diligence to ensure that personal data obtained from third party sources is accurate and complete.	**8.5.3 Maintaining data accuracy and completeness with third parties** Organisation shall exercise due diligence to ensure that personal data obtained from third party sources is also accurate and complete.
3.4.2.1 Organisation ensures the accuracy and completeness of personal data that may be disclosed to another organisation 1. Organisation has processes in place to ensure any personal data it discloses to another organisation is reasonably accurate and complete for the intended purposes. **3.4.1.1 Organisation ensures that personal data under its possession or control is accurate and complete for the intended purposes of use or disclosure**	**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.

DPTM	Singapore Standards (SS714:2025)
4. Where relevant, organisation may communicate the corrections to third parties whom the personal data was disclosed.	
3.4.2.1 Organisation ensures the accuracy and completeness of personal data that may be disclosed to another organisation 2. Where third party organisations to whom the personal data was disclosed (e.g. data intermediaries, service providers, agents) become aware of personal data that is inaccurate, incomplete or out-dated, the organisation has processes or mechanisms to ensure it is informed as soon as practicable.	**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) out-dated.
Principle 4 Individuals' Rights	**9 Safeguarding individual rights**
4.1.1.1 Organisation makes available information on how individuals may withdraw consent 1. Organisation makes available information on how individuals may withdraw consent provided for a purpose (e.g. through data protection policy on corporate website, terms and conditions affixed in physical forms that collect consent). The information relating to choice is easily accessible and provided in a clear and concise manner, clearly worded and easy to understand.	**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 which are: a) clear; b) concise; and c) easy to understand

DPTM	Singapore Standards (SS714:2025)
	These instructions shall be readily available to the individuals, for example through: a) a data protection policy on the organisations' website; or b) terms and conditions affixed in forms that collect consent.
2. Organisation informs individuals clearly the likely consequences of withdrawing consent, either before or upon receiving the notice of withdrawal, before giving effect to the withdrawal of consent	**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.
4.1.1.2 Organisation ensures proper handling of withdrawal of consent requests 1. The organisation has a process in place for receiving, reviewing and effecting withdrawal of consent requests within a reasonable timeframe.	**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.
2. Organisation takes into account the amount of time needed to give effect and the manner in which notice of consent withdrawal was given, and the timeframe for giving effect to the withdrawal of consent is communicated clearly to the requesting individuals.	**9.1.3.2 Communications regarding withdrawal of consent** The organisation shall clearly communicate the timeframe for giving effect to the withdrawal of consent is to the requesting individuals. Determining the timeframe shall be based on: a) amount of time needed to give effect; and b) manner in which notice of consent withdrawal was given.
3. When giving effect to withdrawal of consent, organisation has processes in place to cease and to inform its data intermediaries or third parties to cease, to collect, use or disclose the personal data of the individual.	**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.

DPTM	Singapore Standards (SS714:2025)
4.2.1.1 Organisation makes available information on how individuals may request for access to their personal data 1. Organisation makes available information on how individuals may request for access to their personal data. The information provided is easily accessible, clearly worded and easy to understand for recipients of the information.	**9.2.1 Provisions for individuals' access to their personal data** The organisation shall make available information on how individuals may request for 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.
4.2.1.2 The organisation ensures proper handling of access requests 1. Organisation has processes in place for receiving, reviewing and responding to individual's requests to access their personal data under the organisation's possession or control and how the personal data may have been used or disclosed within a reasonable timeframe. These should include: a) Verification of the requesting individual's identity b) Upon request, providing confirmation that organisation holds personal data about the requesting individual. c) Estimated timeframe to process and address the access request (taking into consideration that organisation must provide access to the personal data within 30 days after receiving the request; if unable to do so, the organisation to inform the individual in writing within 30 days of the time by which it will be able to respond to the request). d) Providing a written estimate of any associated fees imposed for providing access to the personal data and based on the format either requested by the individual or provided by the organisation. e) Process for rejecting access requests, including 1) providing a response to the requesting individual even if organisation is not providing access to the requested personal data or other requested information; 2) providing the reason for the rejection; and 3)	**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) providing a written estimate of any associated fees imposed for providing access to the personal data based on the format requested by the individual or provided by the organisation.

DPTM	Singapore Standards (SS714:2025)
preserving a complete and accurate copy of the personal data requested pursuant to an access request for a prescribed period after rejection of the request. 2. Organisation keeps a record of all access requests received and processed, documenting clearly whether the requested access was provided or rejected.	**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. **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 in the access request for a prescribed period after rejection of the request. **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.
4.3.1.1 Organisation makes available information on how individuals may request for correction of their personal data 1. Organisation makes available information on how individuals may request for correction to their personal data under its possession or control. The information provided is easily accessible, clearly worded and easy to understand for recipients of the information.	**9.3 Provisions for corrections** **9.3.1 Request for correction process** The organisation shall have documented processes in place to process an individuals' request to correct their personal data. These processes 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:

DPTM	Singapore Standards (SS714:2025)
	a) accessible; b) clear; and c) easy to understand.
4.3.1.2 Organisation ensures proper handling of correction requests 1. Organisation has processes in place for receiving, reviewing and responding to individuals' requests to correct their personal data under its possession or control, upon confirming the individual's identity, and unless it is satisfied on reasonable grounds that a correction should not be made, to make the correction as soon as practicable. These should include: a) Verification of the requesting individual's identity b) Upon request, providing confirmation that organisation holds personal data about the requesting individual c) Estimated timeframe to process and address the correction request d) If individual consents, to send corrected personal data to other relevant organisations e) Process for rejecting correction requests 2. Organisation also has processes for individuals to raise objections if dissatisfied with the refusal to correct their personal data. Where no correction is made, organisation annotates the correction that was requested but not made.	**9.3.3 Handling correction requests** The organisation shall have documented processes for handling an individuals' request to correct their personal data. The processes should 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. **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.