DPTM Certification Checklist

This checklist provides a broad outline based on abridged DPTM certification requirements to help organisations gauge their readiness before applying for the DPTM certification.

Organisations should review their data protection regime using the checklist and having a "yes" answer to all the questions is an indication that the organisation is ready to apply for DPTM.

However, kindly note that answering "yes" to all questions on this checklist **may not necessarily equate to meeting all the DPTM requirements.**

The DPTM assessment will also require the organisation to demonstrate and provide evidence for the following:

- Documented data protection policies and processes; and
- Demonstrate that data protection policies and processes are implemented and practised on the ground.

	Checklist	Yes	PDPC's Reference Advisory Guides/Guides/Templates
Principle 1: Governance and Transparency			
A: Establish data protection policies and practices			
1	Organisation shall have data protection policies and practices approved by management, setting out the organisation's approach to managing personal data (include management of special categories of personal data such as personal data of a sensitive nature) for various stakeholders such as:		• Advisory Guidelines on Key Concepts in the Personal Data Protection Act • Guide to Accountability under the Personal Data Protection Act
	• Employees - Internal data protection policy and notice	☐	• Data Protection Notice Generator (https://apps.pdpc.gov.sg/dp-notice-generator/introduction)
	• Customers, Job applicants, visitors etc - External data protection notices	☐	
	• Third party vendors - Third party agreement for management of the organisation's personal data	☐	• Guide to Managing Data Intermediaries • Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data

2	Organisation shall publish and communicate the data protection policies to relevant internal and external stakeholders through appropriate platforms such as:		• Guide to Accountability under the Personal Data Protection Act • Guide to Developing a Data Protection Management Programme (Part II: Policy and Practices)
	• Customers - Privacy notice on the organisation's website, service/product sign-up form or other forms	☐	• Data Protection Notice Generator (https://apps.pdpc.gov.sg/dp-notice-generator/introduction)
	• Employees - Data protection notice on employment form, data protection policy signed by employees, regular staff meeting or other forms	☐	
	• Job applicants - Privacy notice on the organisation's website, Job Application Form/Job portal or other forms	☐	
	• Vendors - Third party agreements or other forms	☐	• Guide to Managing Data Intermediaries • Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data
3	Organisation shall have documented policies and processes to review, update and monitor compliance of data protection policies and practices, such as:		• Guide to Accountability under the Personal Data Protection Act • Guide to Developing a Data Protection Management Programme (Part IV: Maintenance)
	• Process to review data protection policies periodically and obtain management approval for any policy revisions	☐	
	• Process to monitor internal parties' (i.e. employees) compliance with the data protection policies and practices	☐	
	• Process to monitor external parties' compliance with the data protection policies and practices	☐	

B: Establish queries, complaints and dispute resolution handling processes			
4	The organisation shall have documented policies and processes on how it receives and responds to queries/complaints on the collection, use and disclosure of personal data, such as:		• Guide to Developing a Data Protection Management Programme • Develop a Process for Dispute Resolution
	• Procedure on how it handles queries/complaints on the collection, use and disclosure of personal data	☐	
	• Mechanisms on how the individual (e.g. employees, job applicants, customers etc) may submit queries/complaints (e.g. electronic or non-electronic means) to the organisation	☐	
C: Establish processes to identify, assess and address data protection			
5	The organisation shall have documented policies and processes on how it performs risk and impact assessments (e.g. Data Protection Impact Assessment) on its operational functions, business needs and processes which involve personal data.	☐	• 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 I: Policy and Practices & Part IV: Maintenance)
6	The organisation shall document the DPIA conducted and ensure appropriate action plans that are endorsed by management are implemented to address the identified data protection risks.	☐	• Guide to Data Protection Impact Assessments
7	The organisation shall demonstrate Data Protection by Design through documented process and/or other evidence that data protection measures are considered and built into the systems and/or components that involve the processing of personal data as they are being developed.	☐	• Data Protection Practices for ICT Systems

D: Establish a data breach management plan			
8	The organisation shall establish a data breach management plan and communicate it to relevant employees and external stakeholders. The data breach management plan should include:		• 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)
	• Roles and responsibilities of data breach management team	☐	
	• Timeline for reporting data breach incidents	☐	
	• Processes for notifying affected individuals/organisations and relevant regulators/enforcement authorities	☐	
	• Processes for third parties to notify organisation in the event of a data breach	☐	
	• Drawer plans for likely data breach scenarios to better help organisation manage and respond in the event of a data breach	☐	
E: Accountability			
9	The organisation shall appoint a competent DPO (e.g. received formal training) responsible for the organisation's data protection regime and compliance with the PDPA.	☐	• 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)
10	The DPO shall have defined roles and responsibilities, with his contact information easily accessible (e.g. privacy notice on organisation's website) to facilitate queries.	☐	
F: Internal Communication and Training			
11	The organisation shall put in place training programmes and/or other measures to ensure all staff (e.g. employees, new hires, contract staff, etc) are aware of the organisation's data protection obligations.	☐	• Guide to Accountability under the Personal Data Protection Act • Guide to Developing a Data Protection Management Programme (Part I: Governance and Risk Assessment)

Principle 2: Management of Personal Data			
A: Appropriate Purpose			
1	The 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 individuals are notified of the purposes on or before the collection of their personal data.	☐	• 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 Notification
B: Appropriate Consent			
2	The organisation shall have clear and accessible notifications on the purpose on or before the collection of personal data through mechanisms such as Data Protection Notice on the website, employee notice etc.	☐	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapters 7, 8, 9, 13 and 14) • Guide to Notification
3	The organisation shall have processes in place to obtain fresh consent from individuals to use or disclose their personal data for new purpose(s).	☐	
C: Appropriate Use and Disclosure			
4	The organisation shall have documented policies and processes on:		• Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 12) • Guide to Notification • Advisory Guidelines on the Personal Data Protection Act for Selected Topics (Chapter 7) • Advisory Guidelines on Requiring Consent for Marketing Purposes • Guide to Developing a Data Protection Management Programme (Part III: Processes)
	• obtaining consent from the individuals on the collection, use or disclosure of their personal data	☐	
	• collection, use and disclosure of personal data of the individuals without consent (i.e. organisation relies on Exceptions to the Consent Obligation)	☐	
	• obtaining valid consent of the individuals from third parties' sources	☐	

5	The organisation shall maintain a Data Inventory Map to document and track personal data flows in the organisation, to ensure personal data is used and disclosed in accordance with the purposes stated in the notifications and consented by the individuals at the point of collection.	☐	• Guide to Developing a Data Protection Management Programme (Part III: Processes)
D: Compliant Overseas Transfer			
6	The organisation shall establish processes to assess and ensure that the personal data that is transferred overseas is accorded a standard of protection that is comparable to that under the PDPA.	☐	• 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
7	If the organisation engages a third party to transfer personal data overseas, a contract shall be established, including appropriate measures to ensure compliance with the Transfer Limitation Obligation.	☐	
Principle 3: Care of Personal Data			
A: Appropriate Protection			
1	The organisation shall document and implement appropriate protection measures to prevent unauthorised access, collection and use of its personal data in its possession or under its control, which may include:		• 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
	• establishing an information security policy	☐	
	• implementing appropriate administrative, technical and physical safeguards, based on relevant risk assessments, probability and severity of the identified threats and the sensitivity of the information	☐	
	• establishing processes to ensure security measures are regularly tested for effectiveness e.g. vulnerability assessment, penetration tests etc, updated and communicated to relevant stakeholders	☐	

	• establishing contractual agreements with third parties to whom personal data is transferred to, to ensure reasonable security arrangements to protect personal data are in place	☐	
B: Appropriate Retention and Disposal			
2	The organisation shall have a data retention policy and retention schedules for all personal data in its possession.	☐	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 18)
3	The organisation shall implement processes to communicate the data retention policy to all stakeholders and upon request by any stakeholders.	☐	
4	The organisation shall have documented policies and processes on how it ceases to retain unsolicited personal data.	☐	
5	The organisation shall have documented policies, processes and mechanisms for the disposal, destruction or anonymisation of all personal data held by the organisation and its third parties.	☐	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 18) • Data Protection Practices for ICT Systems • Guide to Basic Data Anonymisation Techniques • Advisory Guidelines on the Personal Data Protection Act for Selected Topics (Chapter 3)
6	The organisation shall implement measures (with appropriate contractual provisions) to ensure outsourcing of disposal, destruction or anonymisation of personal data by third party service providers is in accordance with data protection obligations.	☐	
C: Accurate and Complete Records			
7	The organisation shall have documented policies and processes:		• Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 16)
	• to verify and ensure personal data under their possession is accurate and complete for the intended purposes of use or disclosure	☐	
	• for correction of inaccurate, incomplete and out-dated personal data	☐	

	• to communicate corrections to third parties (e.g. data intermediaries and/or other service providers) to whom the personal data was disclosed	☐	
Principle 4: Individual's Rights			
A: Effect Withdrawal of Consent			
1	The organisation shall have documented policies and processes on how it handles requests for withdrawal of consent for collection, use and disclosure of personal data.	☐	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 12)
2	The organisation shall provide information on how individuals may withdraw consent, the consequences of withdrawing the consent, and the mechanism by which to withdraw consent.	☐	
B: Provide Access and Correction Rights			
3	The organisation shall have documented policies and processes on how it handles and responds to access requests, including verifying the identity of requester, response time required and appeal process if access request is rejected.	☐	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 15) • Guide to Handling Access Requests
4	The organisation shall provide information to individuals on the mechanism for access requests and keep records of all requests.	☐	
5	The organisation shall have documented policies and processes on how it handles and responds to correction requests, including verifying the identity of requester, response time required and appeal process if correction request is rejected.	☐	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Chapter 15)
6	The organisation shall provide information to individuals on the mechanism for correction request and keep records of all such requests.	☐	

---End---