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 questions	PDPC's Reference Advisory Guides/Guides
Principle 1: Governance and Transparency		
1	Does your organisation have policies and practices in place to manage personal data?	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act - Chapter 20 • Guide to Accountability under the Personal Data Protection Act • Guide to Developing a Data Protection Management Programme
2	Does your organisation communicate its data protection policies and practises to relevant internal and external stakeholders?	• Guide to Accountability under the Personal Data Protection Act • Guide to Developing a Data Protection Management Programme • Guide to Managing Data Intermediaries
3	Does your organisation regularly review and update data protection policies and practices, and monitor compliance of practices with these policies?	
4	Does your organisation receive and respond to queries on the collection, use and disclosure of personal data by your organisation?	• Guide to Developing a Data Protection Management Programme
5	Does your organisation conduct risk and impact assessments to identify, assess and address data protection risks?	• Guide to Accountability under the Personal Data Protection Act • Guide to Data Protection Impact Assessments • Guide to Developing a Data Protection Management Programme

		• Advisory Guidelines on Key Concepts in the Personal Data Protection Act – Chapter 2
6	Does your organisation take into account Data Protection by Design in the development of a product, service, system or process?	• Guide to Accountability under the Personal Data Protection Act • Guide to Developing a Data Protection Management Programme • Guide to Data Protection by Design for ICT Systems
7	Does your organisation have a data breach management plan? *The plan should include the following:* • *Personnel on management of data breach incident* • *Timeline for reporting data breach incident* • *Processes for notifying affected individuals/organisations and relevant regulators/enforcement authorities to comply with mandatory data breach notification requirements*	• Guide to Managing Data Breaches 2.0 • Guide to Developing a Data Protection Management Programme • Advisory Guidelines on Key Concepts in the Personal Data Protection Act – Chapter 3
8	Does your organisation have a Data Protection officer (DPO) who is well versed in your data protection policies and PDPA? Is the business contact information of the DPO made available to the public? *(DPO should also have received formal training on data protection compliance with the PDPA.)*	• Guide to Accountability under the Personal Data Protection Act • Guide to Developing a Data Protection Management Programme • Advisory Guidelines on Key Concepts in the Personal Data Protection Act - Chapter 20
9	Does your organisation conduct regular training to employees on company's data protection policies and practices?	• Guide to Accountability under the Personal Data Protection Act • Guide to Developing a Data Protection Management Programme
Principle 2: Management of Personal Data		
1	Does your organisation ensure that the personal data collected is necessary for the purpose, and individuals are notified of the purposes on or before the collection of their personal data? *(Organisation should also ensure collection of sensitive data is limited and necessary in its purposes.)*	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act - Chapters 7, 8, 9, 13, 14 • Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers

2	Does your organisation obtain consent for the collection, use or disclosure of personal data? *(This also includes* - *express consent or deemed consent, which the organisation relies on;* - *processes in place with 3rd parties on collection of personal data)*	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act - Chapter 2, 12 • Advisory Guidelines on the Personal Data Protection Act for Selected Topics (Chapter 8 on Data Activities Relating to Minors) • Advisory Guidelines on Requiring Consent for Marketing Purposes
3	Does your organisation ensure proper use and disclosure of personal data collected?	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act • Guide to Developing a Data Protection Management Programme
4	Does your organisation ensure that the transfer of data overseas is in compliance with PDPA? *[This includes 3rd party (e.g. data intermediary, agent) of the company handling the data transfer.]*	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act - Chapter 19
Principle 3: Care of Personal Data		
1	Does your organisation have appropriate security measures in place to prevent unauthorised access, collection and use of its personal data in its possession or under its control? *These security measures must be developed based on relevant risk assessments, type and sensitivity of personal data and likelihood and harm of unauthorised access, erasure or other use.* *Organisation should also ensure these security measures are regularly updated and communicated to relevant stakeholders.* *Organisation should also ensure processes are in place for 3rd parties to make reasonable arrangements to protect personal data.*	• Advisory Guidelines on the Key Concepts in the Personal Data Protection Act - Chapter 17 • Guide to Securing Personal Data in Electronic Medium • Guide to Disposal of Personal Data on Physical Medium • Guide on Building Websites for SMEs • 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

2	Does your organisation have appropriate data retention policies for different types of personal data? *(This also applies to 3rd parties in possession of its personal data.)*	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act - Chapter 18 • Guide to Disposal of Personal Data on Physical Medium • Advisory Guidelines on the Personal Data Protection Act for Selected Topics (Chapter 3 on Anonymisation) • Guide to Basic Data Anonymisation Techniques
3	Does your organisation have processes in place to handle unsolicited personal data?	• Organisation has appropriate policies and processes in place to handle unsolicited personal data (i.e. refers to personal information received by an organisation through no active means)
4	Does your organisation have processes in place to dispose of personal data? *(This also applies to 3rd parties in possession of its personal data.)*	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act - Chapter 18 • Guide to Disposal of Personal Data on Physical Medium • Guide to Securing Personal Data in Electronic Medium • Guide to Basic Data Anonymisation Techniques
5	Does your organisation ensure that its personal data is accurate, and that personal data disclosed to another organisation is accurate and complete? How does your organisation deal with inaccurate data?	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act - Chapter 16
Principle 4: Individual's Rights		
1	Does your organisation provide information on how individuals may withdraw consent on the use of their personal data and the consequences of withdrawing the consent?	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act - Chapter 12
2	Does your organisation provide information on how individuals can request access to their personal data and has a process in place to respond to their request?	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act - Chapter 15 • Guide to Handling Access Requests
3	Does your organisation provide information on how individuals can correct their personal data under its possession?	• Advisory Guidelines on Key Concepts in the Personal Data Protection Act - Chapter 15