OVERVIEW OF CERTIFICATION REQUIREMENTS

The certification requirements are based on parameters including relevance to enhanced PDPA, international standards (e.g. APEC CBPR/PRP requirements) and industry best practices. They are organised around 4 Principles, and each Principle is framed by a set of assessment criteria with controls under each criterion. The 4 Principles and illustrative assessment criteria are outlined below:

Principle 1: Governance and Transparency

Appropriate Policies and Practices

- Establish data protection policies and practices
- Establish queries, complaints and dispute resolution handling processes
- Establish processes to identify, assess and address data protection risks
- Establish a data breach management plan
- Appoint Data Protection Officer (DPO)

Accountability

- Make available business contact information of the DPO to the public
- Provide information on personal data protection policies to external stakeholders

Internal Communication and Training

- Communicate data protection policies and practices to all employees
- Implement data protection training for all relevant internal stakeholders

Principle 2: Management of Personal Data

Appropriate Purpose

- Ensure collection of personal data is for purposes that are clear and appropriate in the circumstances

Appropriate Notification

- Ensure notification of the purposes for the collection of personal data, on or before the collection of personal data
- Ensure notification of new purposes before the use or disclosure of personal data

Appropriate Consent

- Ensure that consent for the purposes has been obtained on or before collecting the personal data
- Ensure that consent for personal data with special considerations has been obtained

Appropriate Use and Disclosure

- Ensure the use of personal data is for purposes for which consent has been obtained
- Ensure the disclosure of personal data is for purposes for which consent has been obtained

Compliant Overseas Transfer

- Ensure appropriate personal data transfer policies are implemented as required under law

Principle 3: Care of Personal Data

Appropriate Protection

- Ensure reasonable security policies and practices are implemented
- Ensure third parties make reasonable security arrangements to protect personal data
- Ensure testing of security measures

Appropriate Retention and Disposal

- Ensure personal data retention policies are implemented
- Ensure appropriate implementation of processes and methods for the disposal, destruction or anonymisation of personal data when there are no longer legal or business purposes to retain the personal data

Accurate and Complete Records

- Ensure personal data for use or disclosure is accurate and complete
- Ensure personal data disclosed to a third-party organisation is accurate and complete

Principle 4: Individuals' Rights

Effect Withdrawal of Consent

- Ensure provision for the withdrawal of consent for the collection, use or disclosure of individuals' personal data

Provide Access and Correction Rights

- Ensure provision for individuals' access to their personal data in the organisation's possession or under its control on request
- Ensure provision for individuals' correction of their personal data in the organisation's possession or under its control on request

Note:

Organisations shall have written documentation on policies, processes and practices for data protection. Organisations must also demonstrate that their data protection policies, processes and practices are implemented and practised on the ground.