Certified Data Protection Practitioner (CDPP)

Introduction

The Certified Data Protection Practitioner (CDPP) is built for professionals who are directly involved in the day-to-day handling, processing, and management of personal data. In most organisations, data protection failures do not happen because of poor policies, but because of gaps in operational understanding and execution. This programme addresses that gap.

CDPP equips participants with practical, role-based knowledge to apply PDPA requirements confidently in real working environments. The programme focuses on how personal data should be collected, used, stored, shared, and protected across functions such as HR, finance, marketing, operations, and IT. Participants will learn how to identify risks early, follow proper procedures, support the organisation's Data Protection Officer, and respond appropriately when incidents occur.

With 11 carefully structured modules, this programme balances legal awareness with operational clarity. It is suitable for managers, executives, system owners, compliance officers, and operational teams who play a critical role in protecting personal data but are not responsible for overall governance.

The CDPP programme turns data protection from a theoretical requirement into a practical capability, helping organisations reduce human error, strengthen internal controls, and demonstrate that reasonable steps have been taken to comply with the law.

Program Objectives

The Certified Data Protection Practitioner (CDPP) programme aims to equip participants with practical knowledge to support day-to-day compliance with personal data protection requirements. The programme is designed for professionals who handle or process personal data as part of their operational responsibilities and need a clear understanding of what compliant practice looks like in real working environments.

The focus of this programme is operational awareness, risk reduction, and consistent application of established data protection procedures.

Learning Outcomes

Upon completion of this programme, participants will be able to:

- Recognise personal data and sensitive personal data in their daily work activities
- Apply basic PDPA requirements when collecting, using, storing, and sharing personal data
- Follow organisational policies and procedures related to data protection and information security
- Identify potential data protection risks and escalate issues appropriately
- Support data controllers and Data Protection Officers in maintaining compliance

- Respond appropriately to suspected data incidents in accordance with internal procedures

Target Participants

Managers, executives, operational teams, system owners, compliance officers, and personnel directly involved in processing personal data.

Program Outline

DAY 1

Core Legal and Operational Foundation

Module 1: Introduction to PDPA and the 2024 Amendments

- Purpose and scope of the Personal Data Protection Act 2010
- Key changes introduced under the Personal Data Protection (Amendment) Act 2024
- Applicability of PDPA to private sector organisations in Malaysia
- Overview of organisational obligations and exposure

Module 2: Key Definitions and Risk Classification

- Personal data and sensitive personal data
- Biometric data and higher-risk data categories
- Roles of data controllers and data processors
- Meaning and implications of personal data breaches
- Understanding data-related risk exposure in operations

Module 3: Seven Principles of Personal Data Protection

- General Principle and lawful processing
- Notice and Choice Principle
- Disclosure Principle
- Security Principle
- Retention Principle
- Data Integrity Principle
- Access Principle and data subject rights

Module 4: Offences, Penalties, and Organisational Liability

- Common offences under the PDPA
- Enhanced penalties under the 2024 amendments

- Organisational and management liability
- Reputational and operational impact of non-compliance

DAY 2

Operational and Governance Responsibilities (Data Controller Perspective)

Module 5: Management Accountability and Oversight

- Accountability of data controllers under the PDPA
- Responsibilities despite outsourcing or delegation
- Oversight of internal teams and data processors
- Role of management in ensuring compliance

Module 6: Lawful Collection and Use of Personal Data

- Purpose limitation and lawful data collection
- Appropriate use of personal data in operations
- Managing employee, customer, and vendor data
- Avoiding misuse and over-collection of data

Module 7: Data Disclosure and Cross-Border Transfers

- Disclosure of personal data to third parties
- Managing data sharing arrangements
- Cross-border data transfer considerations
- Data portability requests and operational implications

Module 8: Contractual and Internal Risk Controls

- PDPA clauses in vendor and service contracts
- Internal approval processes for data-related activities
- Roles and responsibilities within operational teams
- Aligning operational practices with governance requirements

DAY 3

Operational Compliance (Data Processor Responsibilities)

Module 9: Security Principle as a Direct Obligation

- Security Principle under the PDPA
- Direct obligations of data processors
- Reasonable security measures in daily operations
- Shared responsibility between controllers and processors

Module 10: Operational Data Handling and Access Control

- Secure handling of personal data in daily work
- Access control and role-based permissions
- Common operational weaknesses and human error
- Managing risks in systems and shared platforms

Module 11: Incident Detection, Escalation, and Reporting

- Identifying early signs of data incidents
- Internal escalation and reporting procedures
- Coordination with data controllers and DPOs