Certified Data Protection Specialist (PDPS)

Introduction

The Certified Data Protection Specialist (PDPS) is designed for professionals who want to master personal data protection beyond basic compliance and become trusted experts within their organisations or advisory roles. As data protection obligations in Malaysia evolve and enforcement becomes more rigorous, organisations increasingly need specialists who can interpret the law, design robust governance frameworks, and anticipate risks before they become costly incidents.

This programme provides a comprehensive, end-to-end understanding of personal data protection under the Personal Data Protection Act 2010 and the Personal Data Protection (Amendment) Act 2024. Participants will gain the ability to connect legal requirements with real organisational practices, covering governance, operational controls, data breach management, cross-border data issues, and accountability mechanisms.

PDPS is ideal for senior HR and IT leaders, compliance and risk professionals, internal auditors, consultants, and advisors who are expected to guide organisations at a strategic level. By completing all 14 modules, participants develop the depth, confidence, and professional judgement required to design, assess, and improve data protection frameworks that can withstand regulatory scrutiny and business pressures.

This is not just a compliance course. It is a capability-building programme for professionals who want to be recognised as data protection specialists in a rapidly maturing regulatory environment.

Program Objectives

The Certified Data Protection Specialist (PDPS) programme aims to develop in-depth understanding and practical competence in personal data protection within the Malaysian regulatory context. The programme is designed to help participants interpret PDPA requirements, translate them into organisational policies and practices, and support informed decision-making related to data protection governance and risk management.

The programme focuses on building professional capability rather than conferring legal authority, enabling participants to contribute meaningfully to the design, review, and improvement of data protection frameworks within organisations.

Learning Outcomes

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

- Explain the key requirements of the Personal Data Protection Act 2010 and the 2024 amendments in an organisational context
- Distinguish between the roles and responsibilities of data controllers, data processors, and accountable officers

- Apply the seven data protection principles to organisational policies, processes, and systems
- Identify common data protection risks and propose appropriate controls and mitigation measures
- Support the development and review of data protection governance, documentation, and compliance practices
- Assist organisations in preparing for audits, regulatory enquiries, and incident management

Target Participants

Management, executives, officers, supervisors, operational staff, system users, and key personnel across departments who handle or influence personal data , senior professionals, consultants, compliance and risk officers, HR and IT leaders, internal auditors, and advisors who require a comprehensive understanding of personal data protection governance, operations, and accountability.

.

Program Outline

DAY 1

Core Modules – PDPA Fundamentals & Legal Obligations

Module 1: Introduction to PDPA and the 2024 Amendments

- Purpose and scope of the Personal Data Protection Act 2010
- Rationale for the Personal Data Protection (Amendment) Act 2024 (Act A1727)
- Terminology shift from Data User to Data Controller
- Applicability to private sector organisations in Malaysia
- Data subjects and fundamental rights

Module 2: Key Definitions under the Act

- Personal data vs sensitive personal data
- Biometric data as sensitive personal data
- Data controller, data processor, and legal relationships
- Meaning of personal data breach
- Data portability and its implications

Module 3: The Seven Principles of Personal Data Protection

- General Principle
- Notice and Choice Principle
- Disclosure Principle
- Security Principle
- Retention Principle
- Data Integrity Principle
- Access Principle

Special focus:

- Strengthened Security Principle under the 2024 amendments
- Shared responsibilities of data controllers and data processors

Module 4: Offences, Penalties, and Liability

- Criminal offences under PDPA
- Enhanced penalties under Act A1727
- Fines, imprisonment, and management liability
- Reputational and business risks
- Due diligence as organisational defence

DAY 2

Governance and Accountability

Module 5: Role and Accountability of the Data Protection Officer

- Mandatory appointment of DPO (Section 12A)
- Position of the DPO within the organisation
- Relationship with senior management
- Non-transferable accountability

Module 6: Governance and Compliance Documentation

- Personal data protection policies
- Standard operating procedures
- Records of data processing activities

- Risk assessment and internal controls

Operational Readiness and Continuous Improvement

Module 7: Personal Data Breach Management

- Identifying data breach incidents
- Assessing “significant harm”
- Notification obligations to the Commissioner
- Notification obligations to data subjects
- Crisis management and defensible documentation

Module 8: Audit, Monitoring, and Improvement

- Internal PDPA compliance audits
- Ongoing staff awareness and training
- Reporting to management
- Preparing for regulatory enquiries and investigations

DAY 3

Module 9: Legal Responsibilities of Data Controllers

- Statutory obligations of data controllers under the PDPA
- Accountability despite outsourcing or delegation of processing activities
- Oversight responsibilities over data processors
- Management and organisational liability for non-compliance

Module 10: Data-Related Decision-Making and Risk Exposure

- Lawful collection and use of personal data
- Disclosure of personal data to third parties
- Cross-border transfer of personal data
- Data portability requests and operational implications

Module 11: Policies, Contracts, and Board-Level Oversight

- Incorporating PDPA obligations into vendor and service contracts
- Internal approval and control mechanisms for data-related activities
- Role of senior management and the board in data protection governance

- Alignment of PDPA compliance with organisational risk management

DAY 4

Module 12: Obligations of Data Processors

- Legal position of data processors following the 2024 amendments
- Direct obligation to comply with the Security Principle
- Scope and limits of authority when processing data on behalf of controllers
- Accountability within outsourced and shared service arrangements

Module 13: Operational Security and Daily Controls

- Access control and handling of personal data in daily operations
- Common operational weaknesses and human error risks
- Safeguards for systems, processes, and data storage
- Managing security risks involving third-party systems and vendors

Module 14: Incident Response and Reporting

- Early detection of potential data incidents
- Internal escalation and reporting procedures
- Reporting obligations to data controllers and designated officers
- Cooperation during investigations and corrective follow-up actions