

Data Protection and Privacy Policy

Malaysia PDPA awareness and practical information-handling controls

FA-0599 · Half day

Cybersecurity

Review Malaysia's amended PDPA, privacy notices and practical data-handling controls through a focused awareness workshop.

Introduction

This half-day course introduces personal-data protection and privacy-policy practice for staff involved in organisational data handling. It covers Malaysia's Personal Data Protection Act 2010 as amended, the seven principles, roles and practical controls, with introductory comparison to other privacy frameworks.

Participants review a sample notice and an illustrative incident scenario. The session builds awareness and identifies follow-up actions; it does not establish organisational compliance, confer DPO qualifications or replace case-specific legal advice. Applicable law, regulator guidance and sector requirements must be checked for the organisation and circumstances.

Learning outcomes

The course teaches participants to:

- Identify personal and sensitive data and common information-handling risks.
- Describe the seven PDPA principles and distinguish data-controller, processor and data-subject roles.
- Recognise important amended requirements and when specialist or regulator guidance is needed.
- Review a privacy notice for clarity, purpose, rights and relevant data flows.
- Identify practical access, retention, vendor and incident-response controls.
- Prepare a short follow-up checklist rather than claim compliance is assured.

Prerequisites

- Basic understanding of organizational data management processes.
- Familiarity with general legal and compliance terminology is helpful but not required.

Training outline

1. Module 1 – Privacy, Data and Risk

- Personal-data processing, sensitive data and common privacy/security threats.
- Data protection versus cybersecurity: overlapping controls and distinct obligations.
- High-level GDPR and California privacy-law comparison; applicability depends on circumstances, not the organisation's location alone.
- Map a simple illustrative data flow and identify the people affected.

2. Module 2 – Malaysia's PDPA as Amended

- Scope and applicability of Act 709; distinguish controller, processor and data-subject roles.
- General, Notice and Choice, Disclosure, Security, Retention, Data Integrity and Access principles.
- Amended controller terminology, biometric sensitive data and processor security responsibilities.
- Awareness of data-protection-officer criteria, breach-notification duties, data portability and cross-border-transfer considerations; refer to current regulator guidance for implementation.
- Enforcement and penalties in context; do not treat training attendance or a notice template as proof of compliance.

3. Module 3 – Privacy Notices and Secure Handling

- Purpose, categories of data, relevant disclosures, rights and contact information in a clear notice.
- Distinguish an external privacy notice from internal policies and operational controls.
- Review a synthetic sample notice for understandable and accurate descriptions.
- Data minimisation, secure storage/transmission, role-based access, retention and correction practices.
- Vendor responsibilities and sharing arrangements; identify matters requiring professional review.

4. Module 4 – Incident and Improvement Planning

- Recognise and escalate a suspected personal-data breach; retain facts and avoid premature assumptions.

- Identify the owner responsible for assessing and meeting current notification requirements.
- DPIA/risk-review concepts, training and awareness, and vendor oversight.
- Discuss an anonymised illustrative incident and prioritise corrective actions.
- Create a concise organisational follow-up checklist and identify specialist questions.