

Data Protection Governance & Accountability Officer

Introduction

The Data Protection Governance & Accountability Officer programme is designed for individuals who carry formal responsibility for overseeing personal data protection within an organisation. Under the amended PDPA, accountability is no longer a technical issue delegated to IT teams. It is a governance and leadership obligation that sits squarely with the organisation and its appointed officers.

This programme focuses on the role commonly performed by a Data Protection Officer, but positions it correctly as a governance and accountability function. Participants will develop the knowledge and judgement required to advise senior management, oversee compliance, coordinate incident response, and act as the organisation's focal point for data protection matters.

Through 8 targeted modules, the programme covers legal accountability, governance structures, policy oversight, data breach notification duties, audit readiness, and ongoing compliance monitoring. It is designed for senior managers, heads of function, compliance leaders, and professionals formally appointed to oversee PDPA compliance.

This programme is not about technical operations. It is about leadership, responsibility, and defensible decision-making. Graduates are equipped to perform their role with confidence, clarity, and credibility, ensuring the organisation can demonstrate accountability in line with the expectations of regulators, stakeholders, and the law.

The Data Protection Governance & Accountability Officer programme aims to prepare participants to oversee and coordinate personal data protection compliance at an organisational level. The programme focuses on governance, accountability, and oversight responsibilities rather than technical implementation.

It is designed to support individuals who are formally appointed or expected to act as the focal point for data protection matters, ensuring that reasonable and structured steps are taken to meet regulatory expectations.

Learning Outcomes

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

- Describe the accountability obligations of organisations under the PDPA and its amendments
- Oversee the implementation and maintenance of data protection policies and governance structures
- Coordinate internal roles and responsibilities related to personal data protection
- Assess and respond to personal data breaches in line with legal notification requirements

- Support management in demonstrating compliance during audits or regulatory reviews
- Monitor ongoing compliance and recommend practical improvements where necessary

Target Participants

All officers, senior officers, and appointed focal persons responsible for coordinating or overseeing data protection matters. Specially for officers formally appointed Data Protection Officers, senior managers, heads of HR, IT, Legal, Risk, and Compliance functions

DAY 1

Core Legal Framework

Module 1: PDPA Scope, Amendments, and Applicability

- Purpose and objectives of the Personal Data Protection Act 2010
- Scope of application to private sector organisations in Malaysia
- Key changes introduced by the Personal Data Protection (Amendment) Act 2024
- Applicability to employees, customers, vendors, and other data subjects
- Practical implications of non-compliance for organisations

Module 2: Key Definitions and Risk Exposure

- Meaning of personal data and sensitive personal data
- Inclusion of biometric data as sensitive personal data
- Roles and responsibilities of data controllers and data processors
- Definition and implications of personal data breaches
- Understanding organisational risk exposure arising from data handling

Module 3: Seven Principles of Personal Data Protection

- General Principle and lawful processing of personal data
- Notice and Choice Principle and transparency obligations
- Disclosure Principle and limits on data sharing
- Security Principle and protection of personal data
- Retention Principle and data storage limitations
- Data Integrity Principle and accuracy requirements
- Access Principle and data subject rights

Module 4: Offences, Penalties, and Management Liability

- Overview of offences under the PDPA
- Enhanced penalties under the 2024 amendments
- Fines, imprisonment, and personal liability
- Accountability of senior management and decision-makers
- Reputational, operational, and business consequences of breaches

DAY 2

Accountability and Oversight

Module 5: DPO Role and Statutory Accountability

- Legal requirement to appoint a Data Protection Officer
- Purpose and responsibilities of the DPO role
- Positioning the DPO within the organisational structure
- Relationship between the DPO, management, and operational teams
- Limitations of delegation and non-transferable accountability

Module 6: Policies, SOPs, and Compliance Documentation

- Importance of documented data protection governance
- Development and maintenance of data protection policies
- Standard operating procedures for data handling
- Record-keeping and documentation discipline
- Ensuring alignment between policies and actual practices

Module 7: Personal Data Breach Governance and Notification

- Identifying personal data breach incidents
- Initial containment and response measures
- Assessing whether a breach causes or is likely to cause significant harm
- Notification obligations to the Commissioner

- Notification obligations to affected data subjects
- Managing communications and maintaining defensible records

Module 8: Audit Readiness, Monitoring, and Continuous Improvement

- Purpose and scope of internal PDPA compliance audits
- Monitoring compliance across departments and vendors
- Identifying gaps and areas for improvement
- Ongoing staff awareness and training
- Preparing for regulatory enquiries and investigations