

ADVANCED DATA PROTECTION :

Risk Management for DPOs

MALAYSIA HR FORUM ACADEMY,
MENARA PKNS PETALING JAYA

RM2,800



100% HRDC Claimable

MODULE OVERVIEW

2-day intensive programme designed to elevate Data Protection Officers (DPOs) from a compliance-focused role to a strategic risk advisor within the organisation.

This masterclass focuses on applying the DPO Core Competency Framework in complex and high-risk environments, strengthening risk-based governance aligned with the PDPA 2010, and equipping participants with the capability to independently conduct, defend, and advise on DPIAs, TIAs, and regulatory engagements.

Participants will gain practical frameworks, advanced methodologies, and strategic perspectives to confidently advise senior management and manage regulator and data subject interactions with credibility and consistency.

LEARNING OBJECTIVES

Participants will be able to:

- Apply the DPO Core Competency Framework strategically in complex organisational contexts
- Lead risk-based personal data protection governance aligned with PDPA 2010
- Conduct and defend Data Protection Impact Assessments (DPIA) and Transfer Impact Assessments (TIA) for high-risk processing activities
- Integrate data protection risk management into organisational decision-making
- Manage regulator and data subject engagement confidently and professionally
- Advise senior management using risk-informed and business-aligned recommendations

DURATION

2 Days



TARGETED PARTICIPANTS

This programme is designed for:

- Appointed Data Protection Officers (DPOs)
- Senior compliance, risk, and governance professionals
- Legal, IT security, and privacy professionals involved in data protection oversight
- Senior managers responsible for personal data governance and cross-border data transfers
- Practitioners seeking to move into advanced or strategic DPO roles

METHOD OF TRAINING

- Interactive lecture
- Practical hands-on exercises
- Demonstrations
- Group tasks and discussions

LEARNING OUTCOME

By the end of the training, participant able to:

- Apply the DPO Core Competency Framework strategically in complex organisational contexts
- Lead risk-based personal data protection governance aligned with PDPA 2010
- Independently conduct and defend DPIAs and TIAs for high-risk processing
- Manage regulator and data subject engagement with confidence and consistency
- Advise senior management using risk-informed and business-aligned recommendations



CONTENTS

Day 1

Module 1: Meeting the DPO Core Competencies Definition

1. The evolving role of DPO – from compliance officer to strategic risk advisor
2. Identifying core competencies to become a competent DPO
 - a. Advisory & support
 - b. Risk management & assessment
 - c. Compliance oversight & monitoring
 - d. Audit & reporting
 - e. Communication & stakeholder engagement
 - f. Regulatory & data subject management
3. KSA (Knowledge, Skill, Ability) Model – meeting the advanced tier DPO

Learning outcomes

Participants will be able to:

- Clearly articulate the six DPO core competency areas and their practical implications
- Distinguish between Fundamental and Advanced Tier responsibilities
- Assess their own competency gaps using a risk-based lens
- Position the DPO role credibly at senior management and board level

Module 2: Strategic Risk Management in Data Protection

1. Understanding risk-based approach framework under PDPA 2010
2. What is strategic management
3. Integrating strategic management and risk management
4. Risk assessment approaches via DPIA and TIA

Learning Outcomes

Participants will be able to:

- Identify and prioritise high-risk processing activities using structured risk criteria
- Advise on risk acceptance, mitigation, or avoidance decisions
- Integrate DPIA, TIA, and breach preparedness into a cohesive risk framework
- Provide defensible, documented recommendations to senior stakeholders

CONTENTS

Day 2

Recap and Review of Day 1

Module 3 : Strategic Data Protection Impact Assessments (DPIA)

1. When and Why DPIAs Matter – Regulatory expectations vs organisational value
2. Enhanced DPIA methodology from industrial perspective
3. Advising on DPIA outcomes to stakeholders
4. Embedding privacy-by-design into organisation culture

Learning Outcomes

Participants will be able to:

- Determine when a DPIA is required or strategically advisable
- Conduct and review DPIAs for complex processing scenarios
- Translate DPIA findings into practical mitigation measures
- Defend DPIA decisions during audits or regulatory inquiries

Module 4 : Ensuring Adequate Cross-border Protection

1. Cross-border transfer obligations – legal and regulatory expectations under PDPA
2. Transfer Impact Assessment (TIA) – assessing adequacy for compliance

Learning Outcomes

Participants will be able to:

- Identify scenarios requiring a Transfer Impact Assessment
- Assess legal and operational risks of cross-border transfers
- Recommend appropriate safeguards or restrictions
- Maintain defensible documentation for regulatory review



CONTENTS

Day 2

Module 5 : Strengthening Data Subject Rights & Transparency

- 1.Revising data subject rights under PDPA
- 2.New data portability right – business to business collaboration
- 3.Data breach notification to data subjects through strategic communication

Learning Outcomes

Participants will be able to:

- Manage data subject requests lawfully, consistently, and professionally
- Handle complaints and regulator engagement with confidence
- Balance transparency with organisational risk
- Strengthen organisational trust through effective communication

