Malaysia's Personal Data Protection Act (PDPA)
A Comprehensive Guide

Incorporating the 2024 Amendments with the 2025 Data Breach Notification and Cross-Border Transfer Guidelines

Ensuring Compliance, Accountability, and Data Resilience in Malaysia

"Trust is the ultimate digital currency.

How you handle Personal Data is a direct reflection of how much you value your customers' trust."

-IR

COURSE OVERVIEW

- This course offers a comprehensive introduction to Malaysia's Personal Data Protection Act 2010 (PDPA), Incorporating the 2024 Statutory Amendments and the latest Regulatory Guidelines issued in 2025

- It provides clarity on the expanded scope of the PDPA, including the mandatory appointment of data protection officers, the introduction of data portability rights, and the exclusion of deceased individuals' data from the PDPA

- The course integrates two key guidelines: the data breach notification guideline, which introduces mandatory reporting within 72 hours to the PDP Commissioner and within 7 days to affected individuals; and the cross-border personal data transfer guideline, which outlines conditions for lawful international data transfers, including Transfer Impact Assessments (TIA), consent, contractual necessity, and safeguards such as Binding Corporate Rules, Standard Contractual Clauses and Recognised Certifications

- Through practical scenarios and compliance-focused content, participants will gain a clear understanding of the seven personal data protection principles, breach governance obligations, cross-border transfer requirements, and their roles in ensuring organizational compliance under the PDPA framework

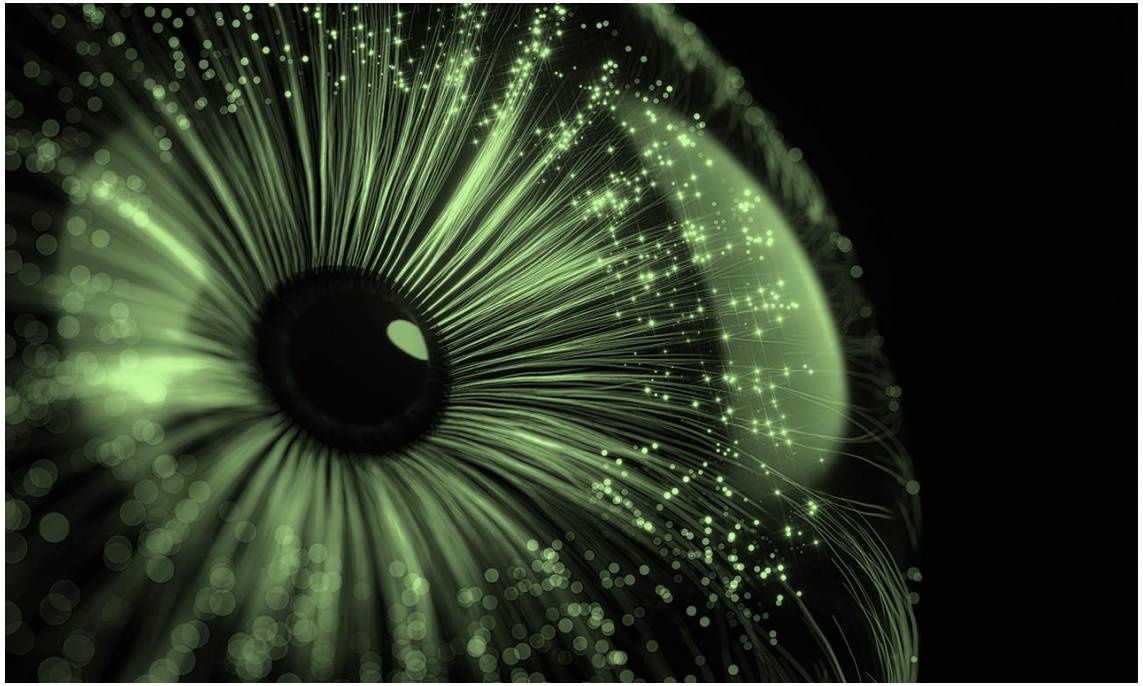
MODULE 1

AN INTRODUCTION TO THE PERSONAL DATA PROTECTION ACT (PDPA)

- Understand the scope, purpose, and enforcement framework of the Personal Data Protection Act 2010 (PDPA)
- Describe the key amendments introduced in 2024, including:
  Mandatory appointment of Data Protection Officers (DPOs)
  Introduction of the right to data portability
  Explicit classification of biometric data as Sensitive Personal Data
- Distinguish between the roles and responsibilities of Data Controllers and Data Processors under the amended PDPA
- Explore the key provisions of the 2025 Data Breach Notification Guideline
- Outline the requirements of the 2025 Cross-Border Personal Data Transfer Guideline

MODULE 2

KEY TERMS AND DEFINITIONS



- Clarify essential PDPA terminology, including Personal Data, Sensitive Personal Data, Data Subject, Data Controller, and Data Processor
- Differentiate between Personal Data and Sensitive Personal Data, including biometric information as defined in the amended PDPA
- Outline the responsibilities and obligations of Data Controllers and Data Processors
- Define what constitutes a data breach and discuss the extent of data portability rights
- Comprehend the principles surrounding data retention and the criteria for appointing Data Protection Officers (DPOs)
- Recognize the function of the Personal Data Protection Commissioner and the relevance of the PDPA to commercial transactions

MODULE 3

THE *7* PERSONAL DATA PROTECTION PRINCIPLES

- Identify and explain the seven Personal Data Protection Principles under the PDPA
- Understand the legal significance and compliance obligations associated with each principle under the PDPA 2010 (as amended)
- Apply the principles to organizational processes, policies, and technologies

MODULE 4

DATA BREACH NOTIFICATION GUIDELINE

- Clarify the essential data breach notification obligations
- Define what constitutes a Personal Data breach and evaluate instances that may lead to “significant harm”
- Detail the timeline and method for notifying the PDP Commissioner and affected Data Subjects
- Explain appropriate approaches for informing individuals about breaches, including alternative public notification methods
- Differentiate the responsibilities and duties of Data Controllers and Data Processors in the context of breach response
- Comprehend governance requirements, such as breach response strategies, staff training initiatives, and evaluations following incidents
- Identify the immediate actions for containment and recovery after a breach.
- Summarise the obligations for record-keeping related to breaches (including those not requiring notification), specifying a 2-year retention period
- Identify situations in which notification under additional laws (e.g., PDRM, BNM, MCMC, NACSA) may also be necessary

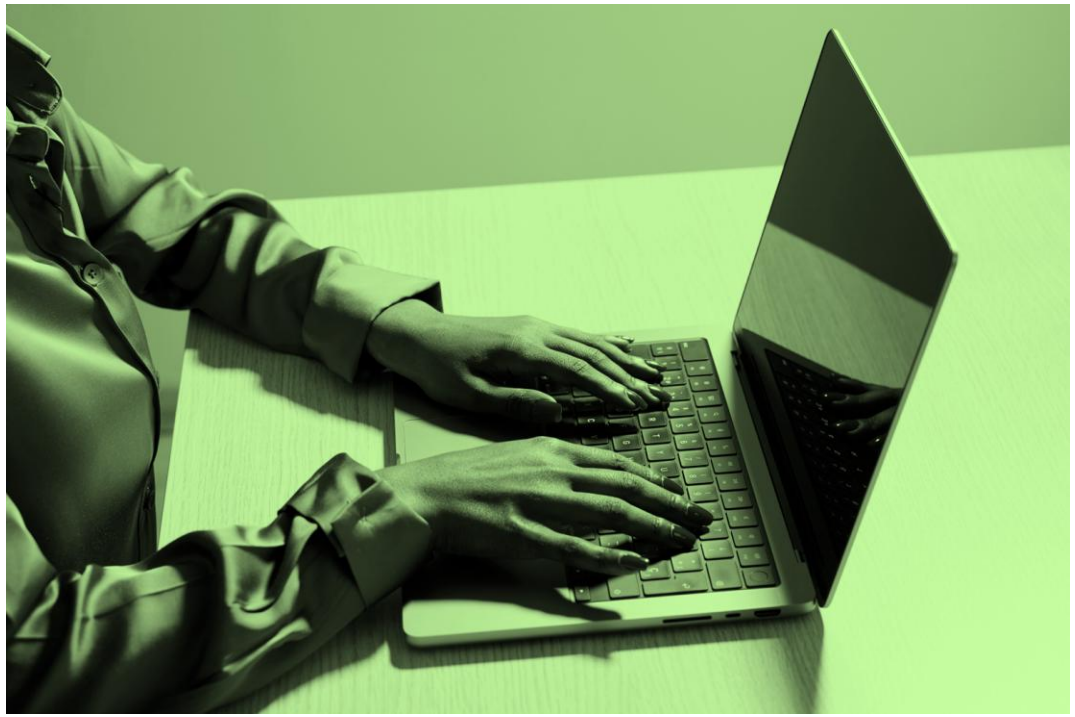
MODULE 5

CROSS BORDER PERSONAL DATA TRANSFER (CBPDT)

- Identify the lawful grounds for transferring data, which encompass consent, contractual necessity, legal obligations, public interest, and vital interests
- Understand how to evaluate the legal systems of recipient countries for "substantially similar law" or "adequate level of protection"
- Explain the purpose, necessary steps, and review criteria involved in a Transfer Impact Assessment (TIA)
- Differentiate between the various safeguards applicable to international data transfers, including:
  - *Binding Corporate Rules (BCR)*
  - *Standard Contractual Clauses (SCC)*
  - *Recognised certification mechanisms*
- Assess the validity of consent for cross-border transfers
- Recognize the obligations of Data Controllers and Data Processors when working with third parties abroad
- Identify the necessary documentation and record-keeping procedures for various transfer conditions and safeguards

NUR INSPIRASI

Malaysia's Personal Data Protection Act (PDPA)
A Comprehensive Guide



Cost

HRDC claimable

Course Duration

3 hours - on demand 24 x 7

Methodology

Self-paced interactive online course

Our Contact Details

Nur Inspirasi Sdn Bhd (1184263-V)

E: jasim@nurinspirasi.com

T: +6012 288 8918