OUTSOURCING TRAINING & CONSULTING
OTC Training Centre Sdn Bhd

HRD awards 2022 TRAINING PROVIDER

DATA PROTECTION OFFICER CERTIFICATE PROGRAMME

14 hours ZOOM & PHYSICAL Program

HYBRID TRAINING

5 & 6 Nov 2025 (Wed & Thu)

Remote Online Training (Zoom) &
Wyndham Grand Bangsar Kuala Lumpur Hotel (Physical)

** Choose either Zoom OR Physical Session

COURSE DESCRIPTION

This comprehensive DPO Certification Course is designed to equip professionals with the knowledge and skills necessary to fulfill the role of a Data Protection Officer under key data protection regulations, namely the Personal Data Protection (Amendment) Act 2024, Personal Data Protection Standards 2015 and other international privacy frameworks. The course provides a practical and legal foundation in data protection, privacy governance, risk management, and compliance.

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- Understand core principles of data protection under Personal Data Protection (Amendment) Act 2024 and Personal Data Protection Standards 2015
- Interpret and apply compliance requirements in real-world scenarios
- Manage data protection impact assessments (DPIAs) and data subject rights
- Monitor internal data processing activities and ensure lawful handling
- Serve as the contact point for supervisory authorities and data subjects
- Build and maintain a robust data protection compliance framework
- Spot red flags in the Personal Data Protection framework

WHO SHOULD ATTEND:

- Appointed or aspiring Data Protection Officers (DPOs)
- Compliance officers, legal professionals, IT/security managers
- Data privacy consultants or auditors
- HR, marketing, or operations professionals handling personal data

METHODOLOGY

- Virtual Online Training Session via Zoom
- Highly Interactive Session, with a bilateral approach to the subject participants to share incidences at respective work locations,
- Case Studies, ,
- Mind Mapping and Recap Sessions,

For Enquiries, Please Call: 010-789 9532 | Email: brenda@otc.com.my | Website: www.otc.com.my

OUTSOURCING TRAINING & CONSULTING
OTC Training Centre Sdn Bhd

COURSE CONTENT

1. **The Underlying reason for the enactment of Personal Data Protection Act 2010**
   - Increasing number of the following cases- Identity Theft, Data Loss, Unauthorized dissemination of data, Fraudulent Activities

2. **Overview of Personal Data Protection Act 2010**
   - Regulates processing of personal data
   - Only commercial transactions
   - Not data processed outside Malaysia
   - 7 Principles
   - Criminal
   - No civil remedies
   - Other supporting Regulations under PDPA 2010
   - Personal Data Protection Standards 2015
   - Personal Data Protection (Ammendment) Act 2024
     - Change of definition from Data User to Data Controller
     - Cross Border Transaction - Removal of whitelisted countries to introduction of minimum standards of countries who qualify to cross border transactions.
     - Increase of penalties for PDP principles breach to RM 1 Million
     - Introduction of biometrics data as sensitive personal data
     - Introduction of Data portability and the Data Subject's rights
     - Introduction to mandatory personal data breach notification.
     - Imposition of obligations on Data Processor directly to comply with Security Principle
     - Introduction of the mandatory appointment of a Data Protection Officer (DPO)

   The above proposed amendments will also be discussed in terms of compliance and to be read together with current related legal requirements, including the Evidence Act 1950

3. **Data Subject, Data Controller & Data Processor (New definition under the amendment 2024)**
   - Definition
   - Categories

4. **Personal data**
   - What is Personal Data and its express and implied definition
   - Forms of Personal Data: As long as it identifies a data subject
   - Email – Whether it can be classified as personal data depends on the circumstances of the case.
   - IP address - Whether it can be classified as personal data depends on the manner in which it is disclosed.
   - Employer and Employee relationship. Data collated as pre-employment checks; Data volunteered just prior to employment; Data obtained during the course of employment.

5. **Commercial Transaction**
   - Any transaction of a commercial nature, whether contractual or not.
   - What are the areas of commercial activity that falls under the purview of Commercial > Transaction.
   - Contracts (Data Processor Agreements)
   - Transfer of personal data overseas

6. **Sensitive personal data**
   - Definition and categories
   - Circumstances and conditions under which it can be processed or disseminated within the ambits of Personal Data Protection (Amendment) Act 2024

COURSE CONTENT

7. Processing – What constitutes Processing

- Collecting
- Recording
- Holding
- Storing
- Organizing
- Publishing on the Internet
- Making available

8. Principles of Data Protection

For data to be processed lawfully in Malaysia, a data user shall comply with the following principles, namely

- General Principle
  - Consent Management (Express / Implied Consent)
- Notice and Choice Principle
- Disclosure Principle
- Security Principle
- Retention Principle
- Data Integrity Principle
- Access Principle

A detailed explanation coupled with examples and case studies of each principle will be shared with participants. The exception to the General Principle will also be discussed. These principles will be read together with the Personal Data Protection Standards 2015.

9. Data Breach Management

- Types of Data Breaches
- Breach Notification Requirements
- Internal Breach Response Procedures
- Communicating with Affected Parties and The Personal Data Protection Commissioner

10. Rights of data subject

- Right to access personal data
- Right to correct personal data
- Right to withdrawn consent
- Right to prevent processing likely to cause damage or distress
- Right to prevent processing for purpose of direct marketing

11. Transfer of Data Overseas

- Who can authorise transfer
- Circumstances under which Data User can effect transfer within the ambits of Personal Data Protection (Amendment) Act 2024

12. What Constitutes an Offence under the Personal Data Protection (Amendment) Act 2024

- Summary of Offences

13. Appointment of a Data Protection Officer

- Competency (Qualifications, experience, skill sets)
- Skill sets
- Scope of Work
- Job Description

14. The job tasks of a Data Protection Officer

- **Ensuring PDPA Compliance:**
  To ensure the organization's data processing activities align with the law's requirements.
- **Advising on Data Protection Matters:**
  Provision of expert advice to the organization on all aspects of personal data protection, including data protection impact assessments (DPIAs) and the development of data protection policies.
- **Fostering a Data Protection Culture:**
  Playing a crucial role in promoting a culture of data protection within the organization. This involves educating employees about their responsibilities and ensuring data protection is integrated into the organization's operations.
- **Managing Data Breaches:**
  Responsible for managing the incident, including reporting to the Commissioner and affected data subjects, and implementing measures to prevent future breaches.
- **Acting as a Liaison:**
  Is a point of contact between the organization and the Commissioner, as well as between the organization and data subjects. This includes handling inquiries, requests, and complaints related to personal data.
- **Monitoring Compliance:**
  Monitors the organization's compliance with the PDP(A) A, including conducting regular audits and reviews of data processing activities.
- **Managing Data Subject Requests:**
  Facilitates the exercise of data subject rights, such as the right to access, correct, or withdraw consent for the processing of their personal data.
- **Updating Policies and Procedures:**
  Responsible for reviewing and updating the organization's data protection policies, practices, and procedures to ensure they remain aligned with the PDPA and best practices.
- **Conducting Gap Analysis:**
  Conducts gap analysis to identify areas where the organization's data protection practices fall short of compliance requirements and provides recommendations for improvement..
- **Developing Data Breach Response Plans:**
  Responsible for developing and maintaining a comprehensive data breach response plan, outlining the steps to be taken in the event of a data breach

15. Data Protection Impact Assessment (DPIA)

- Critical process(s) that poses a major data protection risk(s)
- Identifying Gaps (Vulnerabilities) in the critical process(s)
- Risk Description based on the vulnerabilities
- Severity Rating
  - Impact Analysis and rating
  - Likelihood Analysis and rating
- Corrective Action / Data Protection Risk Mitigation Plan
- Data Protection Risk Maturity Tracker.

16. Final Assessment & Certification

- Multiple-choice test or project
- Certification of completion (if accredited course)
- Feedback and next steps for professional development

End of Session - Q & A