# PERSONAL DATA PROTECTION ACT (PDPA)

All companies and organizations operating in Malaysia must abide by the terms and conditions of the Personal Data Protection Act 2010. It is essential to understand the obligations all parties have towards maintaining the integrity of data security in accordance with the relevant laws.

This Personal Data Protection Act training course will be one day course and it enable delegates to understand the legal requirements of compliance that apply to key areas of their daily working lives.

The training is tailor-made with a practical focus on answering the daily questions that may arise in relation to the participant's organisation handling of personal data. Participants able to know about the implementation of Personal Data Protection Act compliance at the workplace.

## Course Objectives:

- Understand the application of the Personal Data Protection Act 2010 and its related offences as a result of non-compliance.
- To reorganize the practices and process at the respective work areas to support data protection in line with Personal Data Protection Act 2010.
- To develop and execute a Risk Based Compliance Inspection Plan to protect personal data.
- To obtain ideas to implement PDPA requirements successfully at the workplace.

## Methodology:

This course utilizes an interactive lecture approach with an emphasis on discussions between participants sharing details of their workplace experiences and how PDPA compliance could be better achieved. Q&A sessions encouraged on all modules.

## Course Outline:

| | |
|---|---|
| **Personal Data Protection Challenges At the Workplace** | • Introducing PDPA 2010<br>• The main Ingredients of PDPA 2010<br>• Understanding Section 6 and Consent<br>• Forms of Consent -Implicit/Validity/Explicit and how to be compliant<br>• Managing Consent -How to obtain/Who consents/The process and compliance<br>• Sensitive Personal data and consent<br>• Personal Data and Cloud computing<br>• Guidelines on understanding Purpose under Section 6 PDPA 2010 |
| **Transparency of Data Handling and the Right To Be Forgotten** | • Primary duties of Data User under Section 7 PDPA 2010<br>• Data User subject to Audit and Inspection<br>• Due Diligence and role of Data User<br>• Statutory duties of Data User under PDPA 2010<br>• Channels of communication – Best practice |
| **Issues and Implications of the Principles** | • Disclosure Principle and guidelines on when you can refuse to disclose or partially disclose<br>• Guidelines and understanding the Retention Principle and how it relates to Employees and former employees |

# PERSONAL DATA PROTECTION ACT (1 DAY)

| | |
|---|---|
| | • Guidelines on Disposal of Records as per Retention Principle - Reasons for destruction/Destruction Methods/documentation for disposal/Checklist<br>• Guidelines and understanding the Data Integrity Principle<br>• Access Principle and guidelines on how and when to grant excess to access requests |
| **Security Guidance and Privacy Impact Assessment** | • Analysis of the Security Principle under Section 9 PDPA<br>• How security principle used in relation to Nature of Data / Location / Third Party Outsourcing / Measures<br>• Do's and Don'ts of Data Security and Common Breaches as highlighted by PDP office.<br>• Data Security Standard -Implementation and Compliance<br>• Assessing Risks and Impact – not yet<br>• Compliance with Inspection Requirements- not yet |
| **Compliance for The Personal Data Protection Standards** | • The Data Security Standard distinguishes between conventional and electronic data management and prescribes various security measures in relation to each.<br>1. Data Retention Standard<br>2. Data Storage Standards<br>3. Data Integrity Standard<br>4. Data Security Standard |