This training program equips participants with the essential knowledge and skills to implement effective privacy management programs within their organizations. Through a combination of classroom instruction, exercises, and case studies, participants will learn how to assess privacy risks, develop robust policies and procedures, manage data governance, and respond to privacy incidents. The program is designed to help organizations meet regulatory requirements, protect sensitive data, and build trust with stakeholders.

# At the end of this course, participants should be able to:

- Develop a practical roadmap for implementing a privacy management program within the organization.

# Course Outline

- 1: Introduction to Privacy Management – Provides a foundational understanding of privacy management, including its importance, legal and regulatory context, and key concepts.
    - Definition of privacy management
    - Importance of privacy in today's digital age
    - Legal and regulatory framework for privacy
    - Key concepts and principles of privacy management
- 2: Privacy Risk Assessment – teach participant how to identify and assess privacy risks within their organization's data processing activities, using various risk assessment methodologies
    - Identifying privacy risks
    - Assessing the likelihood and impact of risks
    - Risk assessment methodologies
    - Prioritizing risks for mitigation
- 3: Privacy Policies and Procedures – Guides participants in developing comprehensive privacy policies and procedures that align with legal requirements and organizational objectives.

    - Developing comprehensive privacy policies
    - Creating standard operating procedures (SOPs)
    - Ensuring alignment with legal requirements
    - Communicating policies and procedures to stakeholders
- 4: Data Governance and Management – Covers the principles of data governance and management, including data classification, retention, and disposal
    - Data classification and categorization
    - Data retention and disposal policies
    - Data access controls and authorization
    - Data quality and integrity management
- 5: Privacy Training and Awareness – Discuss the importance of privacy training and awareness programs for employees, contractors, and other stakeholders.
    - Developing privacy training programs
    - Tailoring training to different roles and levels
    - Creating awareness campaigns
    - Measuring training effectiveness
- 6: Incident Response and Breach Management – Prepares participants to handle privacy incidents and data breaches effectively, including steps to contain, investigate, and respond to such events.
    - Incident response planning
    - Breach notification requirements
    - Forensic investigation techniques
    - Remediation and recovery strategies
- 7: Monitoring and Compliance – Explains how to monitor compliance with privacy laws and regulations, including conducting regular audits and assessments.
    - Conducting regular audits and assessments
    - Monitoring compliance with laws and regulations
    - Identifying and addressing non-compliance issues
    - Implementing corrective actions
- 8: Emerging Trends and Best Practices – Discusses emerging trends in privacy management, such as artificial intelligence, Internet of Things, and cross-border data transfers, and provides best practices for addressing these challenges.
    - Privacy implications of new technologies (e.g., AI, IoT)
    - Cross-border data transfers

    - Data privacy regulations in different jurisdictions
    - Industry-specific privacy best practices
- 9: Privacy Impact Assessments (PIAs) – Explains the role of PIAs in privacy management, including how to conduct PIAs to assess the privacy implications of new projects or initiatives.
    - Purpose and scope of PIAs
    - Conducting PIAs for new projects or initiatives
    - Identifying privacy risks and mitigation measures
    - Documenting PIA findings and recommendations
- 10: Vendor and Third-Party Management -Discuss strategies for managing privacy risks associated with vendors and third-party service providers, including contract negotiation and oversight.
    - Assessing third-party privacy risks
    - Negotiating privacy clauses in contracts
    - Conducting due diligence on vendors
    - Overlaying third-party privacy practices
- 11: Privacy Metrics and Key Performance Indicators (KPIs) – Introduces privacy metrics and KPIs that can be used to measure the effectiveness of a privacy management program and identify areas for improvement.
    - Developing privacy metrics and KPIs
    - Measuring the effectiveness of privacy initiatives
    - Tracking compliance rates
    - Identifying areas for improvement
- 12: Continuous Improvement and Adaptation -Emphasizes the importance of continuous improvement in privacy management, including staying updated on legal and regulatory changes, conducting regular reviews, and adapting to evolving privacy challenges.
    - Staying updated on privacy laws and regulations
    - Conducting regular reviews of the privacy management program
    - Adapting to evolving privacy challenges
    - Implementing continuous improvement initiatives

# Course Duration

- 3 half days – online

# Delivery Methodologies

- Online Lecture and Discussion
- Individual Assignments
- Activity / Quizzes
- Case study

# This course is recommended for

- Data Protection practitioners
- Record and Database Administrators
- Legal, Regulatory and Compliance personnel
- People Who Deal with Customer Queries and Administer Personal Data
- IT and Other Staff, Including HR, Legal and Business Users
- Anyone who is involved in the processing of personal data

# Upcoming Events

Jun 23
June 23 @ 9:00 am – June 25 @ 12:00 pm
Compliance-Driven Implementation of Privacy Management Program
Oct 13
October 13 @ 9:00 am – October 15 @ 12:00 pm
Compliance-Driven Implementation of Privacy Management Program
View Calendar