Issues about privacy could determine the success or failure of implementation and compliance with the requirements of the Law. Any project that has personal information could have risks. If you ignore privacy, you could lose clients' trust, damage your reputation, fail to meet community expectations, and breach the Data Privacy Act of 2012 privacy principles, the rights of the data subjects, and the preservation of confidentiality, integrity, and availability of your data subjects' personal information.

This course will help establish a systematic assessment that identifies any impact that your project/data processing systems might have on the privacy of data subjects and you to provide recommendations for managing, minimizing, or eliminating that impact.

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

- Demonstrate a functional understanding of privacy impact assessments
- Identify and assess privacy risks
- Develop mitigation strategies to address identified privacy risks
- Know how to document and communicate PIA findings
- Explain the importance of monitoring

Course Outline

- Introduction to Privacy Impact Assessments – Provides a foundational understanding of PIAs, including their purpose, legal context, and benefits.
    - What is a PIA?
    - Definition and purpose
    - Legal and regulatory context
    - Why conduct a PIA?
    - Risk management
    - Compliance
    - Stakeholder trust
    - PIA process overview

- Identifying and Assessing Privacy Risks – Teaches participants how to identify potential privacy risks within their organization's data processing activities and assess the likelihood and impact of these risks.
    - Privacy risk identification
    - Data collection and processing activities
    - Sensitive data handling
    - Third-party involvement
    - Potential data breaches
    - Risk assessment methodologies
    - Qualitative and quantitative methods
    - Risk scoring and prioritization
- Developing Mitigation Strategies- Guides participants in developing effective mitigation strategies to address identified privacy risks, ensuring compliance with legal requirements and protecting sensitive data.
    - Mitigation strategies
    - Technical measures (e.g., encryption, access controls)
    - Organizational measures (e.g., policies, procedures)
    - Legal measures (e.g., contracts, data retention)
    - Feasibility and effectiveness
    - Cost-benefit analysis
    - Implementation challenges
- Documenting and Communicating the PIA – Covers the process of documenting the PIA findings and recommendations in a clear and comprehensive report, as well as communicating the results to relevant stakeholders.
    - PIA report structure
        - Executive summary
        - Risk identification and assessment
        - Mitigation strategies
        - Conclusion and recommendations
    - Stakeholder communication
        - Internal and external stakeholders
        - Effective communication channels
- Monitoring and Review – Explains the importance of ongoing monitoring and periodic review of the PIA to ensure that mitigation strategies remain effective and that new

risks are identified and addressed.
    - Ongoing monitoring
        - Changes in data practices
        - Regulatory updates
    - Periodic review
        - Assessment of mitigation effectiveness
        - Identification of new risks

Course Duration

- 2 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

Notice

There are no upcoming events.