ADEPT
LEARN

Certified Data Privacy Solutions Engineer-CDPSE
Duration: 32 Hours (4 Days)

Overview

The Certified Data Privacy Solutions Engineer (CDPSE) course is a comprehensive program designed to equip learners with the necessary skills to implement privacy solutions and manage data protection within their organizations effectively. The course focuses on three critical areas: Module 1: Privacy Governance, which delves into the fundamentals of personal data and information management, exploring various privacy laws, documentation, consent processes, and responsibilities in data governance. It also emphasizes privacy training, vendor management, risk assessment, and incident management. Module 2: Privacy Architecture, which teaches learners about the technical aspects of data protection, including Secure technology stacks, Cloud services, System hardening, and Privacy-focused development practices. It covers Encryption, Identity management, and the critical role of Monitoring in maintaining privacy. Module 3: Data Cycle, which addresses the entire lifecycle of data, from inventory and classification to quality management and Data destruction, ensuring that data is protected throughout its journey within the organization. By mastering these areas, learners will be well-equipped to support and improve their organization's data privacy frameworks, aligning them with global standards and regulations.

Audience Profile

The Certified Data Privacy Solutions Engineer (CDPSE) course equips professionals with essential skills for privacy governance, architecture, and data lifecycle management.

- Data Privacy Officers
- Compliance Officers and Lawyers specializing in data privacy
- Information Security Analysts
- IT Managers and Consultants
- Risk Assessment Professionals
- Data Protection Managers
- Cybersecurity Professionals
- Systems and Network Administrators
- Software Developers with a focus on privacy
- Cloud Security Specialists
- Data Governance and Quality Managers
- Privacy and Security Architects
- IT Auditors involved in privacy audits
- Corporate Training Professionals specializing in privacy and compliance
- Government Officials dealing with data protection regulations
- HR Professionals overseeing employee data privacy
- Marketing Managers who handle customer data
- Product Managers incorporating privacy into product design
- Business Analysts involved in data-sensitive projects

Course Syllabus

Domain 1: Privacy Governance (34%)

A. Governance
- Personal Data and Information
- Privacy Laws and Standards across Jurisdictions
- Privacy Documentation (e.g., Policies, Guidelines)
- Legal Purpose, Consent, and Legitimate Interest
- Data Subject Rights

B. Management
- Roles and Responsibilities related to Data
- Privacy Training and Awareness
- Vendor and Third-Party Management
- Audit Process
- Privacy Incident Management

C. Risk Management
- Risk Management Process
- Privacy Impact Assessment (PIA)
- Threats, Attacks, and Vulnerabilities related to Privacy

Domain 2: Privacy Architecture (36%)

A. Infrastructure
- Technology Stacks
- Cloud-based Services
- Endpoints
- Remote Access
- System Hardening

B. Applications and Software
- Secure Development Lifecycle (e.g., Privacy by Design)
- Applications and Software Hardening
- APIs and Services
- Tracking Technologies

C. Technical Privacy Controls
- Communication and Transport Protocols
- Encryption, Hashing, and De-identification
- Key Management
- Monitoring and Logging
- Identity and Access Management

Domain 3: Data Cycle (30%)

A. Data Purpose

- Data Use Limitation
- Data Inventory and Classification (e.g., Tagging, Tracking, SOR)
- Data Quality and Accuracy
- Dataflow and Usage Diagrams
- Data Analytics (e.g., Aggregation, AI, Machine Learning, Big Data)

B. Data Persistence

- Data Minimization (e.g., De-identification, Anonymization)
- Data Migration
- Data Storage
- Data Warehousing (e.g., Data Lake)
- Data Retention and Archiving
- Data Destruction