Certified Data Privacy Solutions Engineer (CDPSE)

Course Duration: 5 Days
Exam Reference: CDPSE

Course Overview

Certified Data Privacy Solutions Engineer (CDPSE) is focused on validating the technical skills and knowledge it takes to assess, build, and implement comprehensive data privacy measures. CDPSE holders help fill the technical privacy skills gap so that your organization has competent privacy technologists to build and implement solutions that mitigate risk and enhance efficiency.

Prerequisites

To apply for the CDPSE certification, you should have three years' experience in Privacy Governance (Governance, Management and Risk Management), Privacy Architecture (Infrastructure, Applications/Software and Technical Privacy Controls) and Data Lifecycle (Data Purpose and Data Persistence).

Course Objectives

Upon completion, you will be able to:

- Analyze and integrate security and privacy requirements to protect data across enterprise systems and applications.
- Articulate the relationship between technology implementation and legal/regulatory mandates, ensuring technical controls satisfy compliance obligations.
- Design and enforce data privacy controls across the entire data lifecycle (collection, processing, storage, use, and disposal).
- Establish, maintain, and manage a comprehensive privacy governance framework that defines policies, roles, and accountability within an organization.

APPLIED TECHNOLOGY ACADEMY

Contact Us

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

Certified Data Privacy Solutions Engineer (CDPSE)

- Design and implement privacy-enhanced solutions and privacy architectures that embed privacy controls by default (Privacy-by-Design).
- Evaluate and implement industry-leading privacy best practices and standards to mitigate risk and demonstrate compliance.
- Select, configure, and manage technical privacy solutions (e.g., anonymization, pseudonymization, encryption) to meet specific data protection goals.

Course Outline

Module 1: Privacy Governance

- Privacy Governance
  - Personal Information
  - Privacy Principles (e.g., Privacy by Design, Consent, Transparency)
  - Privacy Laws and Regulations
  - Privacy Documentation (e.g., Policies, Guidelines)

- Privacy Operations
  - Organizational Culture, Structure, and Responsibilities
  - Vendor and Supply Chain Management
  - Incident Management
  - Data Subject Rights, Requests, and Notification

Module 2: Privacy Risk Management and Compliance

- Risk Management
  - Risk Management Process and Policies
  - Privacy-Focused Assessment (e.g., Privacy Impact Assessment (PIA))
  - Privacy Training and Awareness
  - Threats and Vulnerabilities
  - Risk Response

- Compliance
  - Privacy Frameworks
  - Evidence and Artifacts
  - Program Monitoring and Metrics

Certified Data Privacy Solutions Engineer (CDPSE)

Module 3: Data Lifecycle (Implied Domain Title)

- Data Collection and Processing
  - Data Inventory, Dataflow Diagram, and Classification
  - Data Quality (e.g. Accuracy)
  - Data Use Limitation
  - Data Analytics (e.g., Aggregation, AI, Data Warehouse)

- Data Persistence and Destruction
  - Data Minimization
  - Data Disclosure and Transfer
  - Data Storage, Retention, and Archiving
  - Data Destruction

Module 4: Privacy Engineering

- Technology Stacks
  - Infrastructure and Platform Technology (e.g., legacy, cloud computing)
  - Devices and Endpoints
  - Connectivity
  - Secure Development Life Cycle
  - APIs and Cloud-Native Services

- Privacy Related Security Controls
  - Asset Management
  - Identity and Access Management
  - Patch Management and Hardening
  - Communication and Transport Protocols
  - Encryption and Hashing
  - Monitoring and Logging

- Privacy Controls
  - Consent Tagging
  - Tracking Technologies (e.g., cookie management)
  - Anonymization and Pseudonymization
  - Privacy Enhancing Technologies (PETs)
  - AI/Machine Learning (ML) Considerations