CDPSE Course Content

Overview

The Certified Data Privacy Solutions engineer (CDPSE) is focused on validating the technical skills and knowledge it takes to assess, build and implement a comprehensive privacy solution. CDPSE holders can fill the technical privacy skills gap so that an organization has competent privacy technologists to build and implement solutions that mitigate risk and enhance efficiency.

Why CDPSE with Skillcertified?

The CDPSE certification training course from Skillcertified is taught by highly experienced and certified professionals in the privacy domain. They have achieved the certification through years of experience and superior knowledge. The course content is created with care and precision keeping the candidate in mind. Candidates who pursue our CDPSE Certification Online Training will be able to pursue the certification and achieve it quickly.

Target audience

The following job roles will highly benefit from obtaining the CDPSE certification

- Consultant
- Data Scientist
- IS Engineer (User Data Protection)
- Privacy Advisor / Manager
- Privacy Solutions Architect
- Data Analyst
- Domain Architect (Legal Care / Privacy / Compliance)
- IT Project Manager
- Privacy Analyst / Engineer

Pre-requisite

Three (3) or more years of experience in data privacy governance, privacy architecture, and/or data lifecycle work. No experience waivers or substitutions are given for this certification.

CDPSE Course Outline

Upon completing this course, you will be able to

- Identify the privacy program requirements
- Describe the types of privacy protection legal models
- Identify the common privacy laws and regulations
- Identify the various privacy standards
- Identify the different types of documentation necessary for data privacy management
- Explain the requirements to address the data subjects' right
- Identify roles & responsibilities of various stakeholders
- Define & execute a privacy awareness program
- Apply privacy controls for the privacy risks and issues
- Define privacy incident management program
- Identify the common privacy-related vulnerabilities caused by the problematic data actions
- Identify the methods of exploiting these vulnerabilities leading to privacy breaches and harms
- Identify the common established PIA methodologies
- Describe the NIST privacy risk assessment methodology and EU GDPR
- Describe Data Protection Impact Assessment (DPIA)
- Identify various types of computing infrastructure
- Identify the advantages and limitations of cloud computing
- Recognize the responsibilities of the Cloud Service Provider and the cloud consumer in a shared responsibility model
- Describe Secure Development Life Cycle
- List the various considerations for endpoint security
- Describe the elements and principles of privacy by design
- Identify the best practices for system hardening
- Explain the steps involved in application and system hardening to protect the enterprise's software/applications from privacy breach
- Describe the privacy considerations required for applications using APIs and web services
- Recognize the risks associated with the various communication protocols
- Explain the steps to create a data inventory & classification
- Describe the four process areas of data quality
- Illustrate the different data flow diagrams
- Explain data analytics and its privacy concerns

- Explain data minimalization
- Explain data migration & storage requirements
- Explain data warehousing
- Explain data retention, archiving & destruction