INFOSECTRAIN

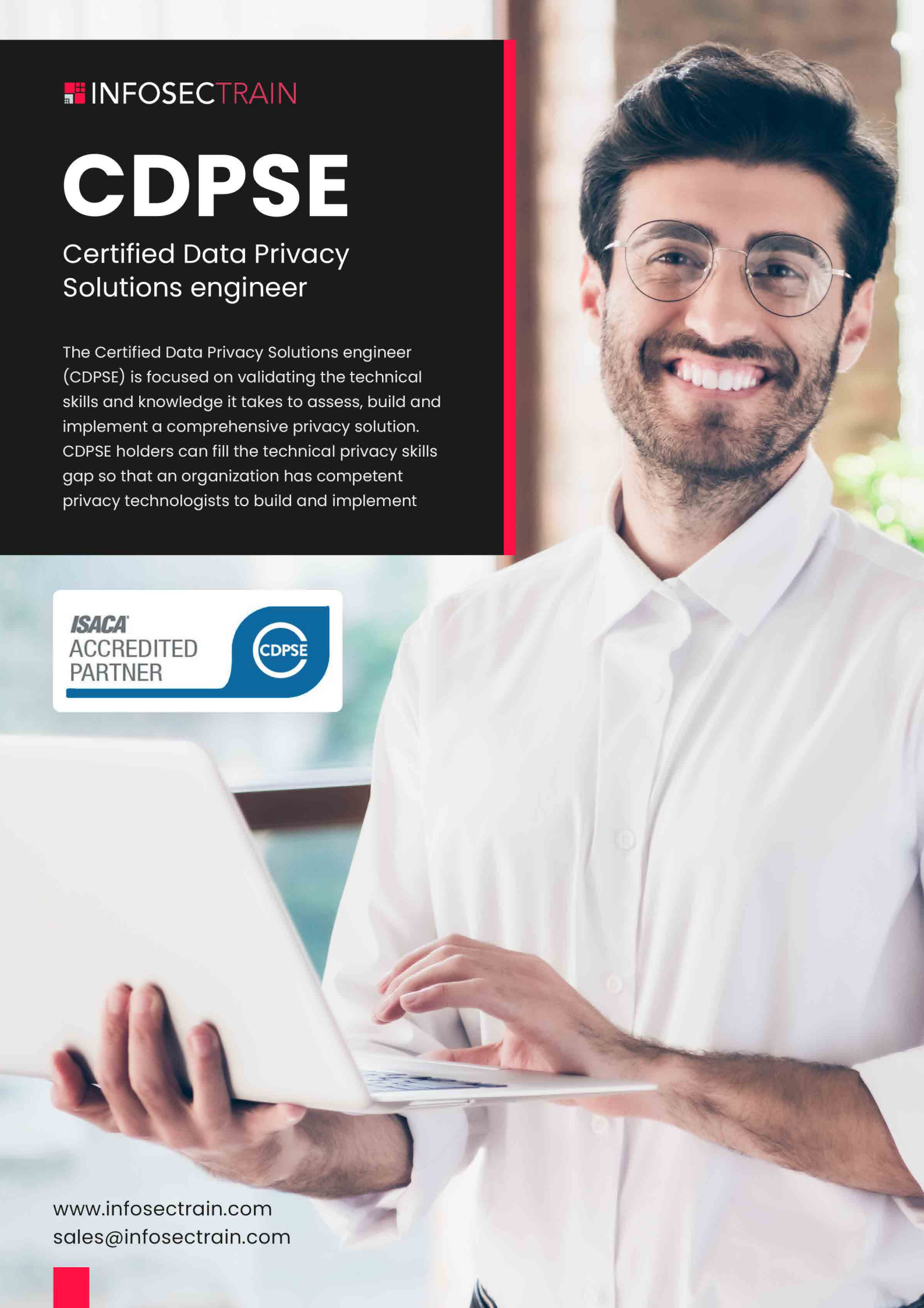
CDPSE

Certified Data Privacy Solutions engineer

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

ISACA ACCREDITED PARTNER

CDPSE



www.infosectrain.com
sales@infosectrain.com

INFOSECTRAIN

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.

INFOSECTRAIN

Why CDPSE with InfoSec Train?

The CDPSE certification training course from InfoSec Train 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/ Compliance/Privacy
- IT Project Manager
- Privacy Analyst/Engineer
- Software 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.

Exam Information

Duration	3.5 hours (210 minutes)
Number of Questions	120
Question format	Multiple Choice
Passing grade	You must score 450 or higher to record a pass in the exam
Languages available	English

Why Infosec Train?

- Certified & Experienced Instructor
- Flexible Schedule
- Access to the recorded sessions
- Post Training Support
- Tailor Made Training
- 4 hrs/day in Weekend/ Weekday

CDPSE Course Outline

Upon completing this course, you will be able to

- Identify the privacy program requirements
- Describe the privacy governance practices
- 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 the privacy program requirements
- Describe the privacy governance practices
- 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 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 problematic data actions during data processing leading to these privacy harms.
- Identify the common established PIA methodologies.
- Describe the NIST privacy risk assessment methodology and EU GDPR DPIA Identify various types of computing infrastructure.

- Recognize the responsibilities of the Cloud Service Provider and the cloud consumer in a shared responsibility model
- Identify the advantages and limitations of cloud computing
- Apply privacy controls for the privacy risks and issues associated with the remote access options.
- List the various considerations for endpoint security
- Identify the best practices for system hardening.
- Describe the elements and principles of privacy by design
- 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 relevant privacy controls to handle the identified privacy risks.
- Recognize the risks associated with the various communication protocols.
- Recognize the risks covering the various communication protocols.
- Describe WLAN security, TLS, and Secure Shell.
- 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 relevant privacy controls to handle the identified privacy risks.
- Recognize the risks associated with the various communication protocols.
- Recognize the risks covering the various communication protocols.
- Describe WLAN security, TLS, and Secure Shell.
- Explain the steps to create a data inventory.
- Describe the four process areas of data quality
- Illustrate the different data flow diagrams

- Explain data analytics and its privacy concerns.
- Explain the steps to create a data inventory.
- Describe the four process areas of data quality
- Illustrate the different data flow diagrams
- Explain data analytics and its privacy concerns

Course Topics include

Governance

- Personal Data and Information
- Privacy Laws and Standards across Jurisdictions
- Privacy Documentation
- Legal Purpose, Consent and Legitimate Interest
- Data Subject Rights

Management

- Roles and Responsibilities Related to Data
- Privacy Training and Awareness
- Vendor and Third-party Management
- Audit Process
- Privacy Incident Management
- Risk Management
- Risk Management Process

Infrastructure

- Cloud Computing
- Remote Access
- Endpoints
- System Hardening
- Secure Development Life Cycle

Applications and Software

- Application and Software Hardening
- APIs and Services
- Tracking Technologies

Technical Privacy Controls

- Communication and Transport Protocols
- Encryption, Hashing and De-identification
- Key Management
- Encryption, Hashing and De-identification
- Monitoring and Logging
- Identity and Access Management

Data Purpose

- Data Inventory and Classification
- Data Quality
- Data Flow and Usage Diagrams
- Data Use Limitation
- Data Analytics

Data Persistence

- Data Minimization
- Data Migration
- Data Storage
- Data Warehousing
- Data Retention and Archiving
- Data Destruction

www.infosectrain.com | sales@infosectrain.com