Data Security and Information Privacy Essentials Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid convergence of Artificial Intelligence (AI), evolving global regulations like the EU?ÇÖs DSA/AI Act, and the increasing sophistication of cyber threats has made data protection an essential core competency for all professionals. This course is a vital and SEO-friendly program designed to equip participants with the foundational knowledge and practical skills in Data Security and Information Privacy required for the modern digital economy. We delve deep into the core principles of Confidentiality, Integrity, and Availability, mandatory regulatory compliance, and proactive risk management through Privacy-by-Design principles. Data Security and Information Privacy Essentials Training Course directly addresses the critical need for a privacy-first culture in a world of ever-growing data volumes, helping organizations mitigate the risk of costly data breaches and regulatory fines.

Data Security and Information Privacy Essentials Training Course essentializes complex concepts into actionable strategies for securing sensitive information and ensuring regulatory compliance. Professionals will master key trending skills, including data minimization, zero-trust architecture fundamentals, threat modeling, and incident response planning. The curriculum emphasizes real-world application, featuring a strong focus on emerging challenges like AI governance, cross-border data transfers, and managing third-party vendor risks. By integrating best practices in cybersecurity hygiene and modern privacy frameworks, participants will gain the confidence to implement robust data protection controls, uphold data subject rights, and contribute to their organization's overall cyber resilience and long-term brand trust.

Programme Curriculum

Data Security and Information Privacy Essentials Training Course

Introduction

The rapid convergence of Artificial Intelligence (AI), evolving global regulations like the EU?ÇÖs DSA/AI Act, and the increasing sophistication of cyber threats has made data protection an essential core competency for all professionals. This course is a vital and SEO-friendly program designed to equip participants with the foundational knowledge and practical skills in Data Security and Information Privacy required for the modern digital economy. We delve deep into the core principles of Confidentiality, Integrity, and Availability, mandatory regulatory compliance, and proactive risk management through Privacy-by-Design principles. Data Security and Information Privacy Essentials Training Course directly addresses the critical need for a privacy-first culture in a world of ever-growing data volumes, helping organizations mitigate the risk of costly data breaches and regulatory fines.

Data Security and Information Privacy Essentials Training Course essentializes complex concepts into actionable strategies for securing sensitive information and ensuring regulatory compliance. Professionals will master key trending skills, including data minimization, zero-trust architecture fundamentals, threat modeling, and incident response planning. The curriculum emphasizes real-world application, featuring a strong focus on emerging challenges like AI governance, cross-border data transfers, and managing third-party vendor risks. By integrating best practices in cybersecurity hygiene and modern privacy frameworks, participants will gain the confidence to implement robust data protection controls, uphold data subject rights, and contribute to their organization's overall cyber resilience and long-term brand trust.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Define the principles of the CIA Triad in a modern context.
2. Differentiate between Data Security and Information Privacy and explain their symbiotic relationship.
3. Identify and classify various types of sensitive data, including Personally Identifiable Information (PII).
4. Analyze the core requirements of major global data protection regulations.
5. Apply the Privacy-by-Design and Privacy-by-Default principles to new systems and processes.
6. Implement essential cybersecurity hygiene practices to protect endpoints and networks.
7. Understand the role of Data Protection Impact Assessments (DPIAs) and risk assessment frameworks.
8. Evaluate the security implications of cloud storage and international data transfers.
9. Employ key data minimization and data retention strategies to reduce legal exposure.
10. Recognize and respond effectively to common cyber threats, including phishing and ransomware.
11. Formulate a basic data breach incident response plan aligned with legal notification timelines.
12. Master best practices for managing and securing data related to third-party vendors and the supply chain.
13. Explain the emerging privacy challenges and AI governance considerations in data processing.

Target Audience

1. All Employees
2. Data Handlers and Processors
3. IT Support and System Administrators.
4. Compliance, Legal, and Risk Management Professionals.
5. Project Managers and Product Developers
6. Human Resources Staff
7. Marketing and Sales Teams

8. Business Owners and Departmental Managers

Course Modules

Module 1: Foundational Principles of Data Protection

- The CIA Triad as the bedrock of security.
- Defining and differentiating Personally Identifiable Information and sensitive data.
- The difference between Data Security and Information Privacy
- Understanding the data lifecycle.
- Establishing a Data Protection Culture and employee responsibilities.
- Case Study: Target Corporation Data Breach.

Module 2: Global Privacy Regulatory Compliance

- Overview of the General Data Protection Regulation principles and obligations.
- Key requirements of the California Consumer Privacy Act and other US State laws.
- Understanding sector-specific regulations, such as HIPAA and PCI DSS
- Navigating cross-border data transfer challenges and mechanisms.
- Defining Data Subject Rights and organizational response duties.
- Case Study: Google's CNIL GDPR Fine (2019).

Module 3: Essential Data Security Controls and Techniques

- Implementing strong Authentication and Access Controls.
- The role and types of Encryption for safeguarding PII.
- Fundamentals of Network Security.
- Secure handling of physical documents and electronic media disposal
- Basics of Endpoint Protection and the importance of timely patching and updates.
- Case Study: Capital One Cloud Breach (2019).

Module 4: Risk Management and Privacy-by-Design

- Introduction to Data Protection Impact Assessments.
- Integrating Privacy-by-Design and Privacy-by-Default into the system development lifecycle.
- Techniques for Data Minimization, pseudonymization, and anonymization.
- Performing simple Threat Modeling to identify potential vulnerabilities in a new system.
- Establishing and enforcing clear Data Retention and secure destruction policies.
- Case Study: Apple's Privacy-Focused App Tracking Transparency.

Module 5: Cybersecurity Hygiene and Threat Awareness

- Recognizing and preventing Phishing, spear-phishing, and social engineering attacks.
- Understanding the danger of Malware and best practices for prevention.
- Secure browsing and email practices
- The risks of using public Wi-Fi and securing remote work environments.
- Understanding the importance of security awareness training as the human firewall.
- Case Study: Colonial Pipeline Ransomware Attack (2021).

Module 6: Data Incident Response and Breach Management

- Defining a Security Incident versus a Data Breach and when to escalate.

- Key steps in the Incident Response Plan
- Understanding legal and regulatory breach notification obligations
- The role of Digital Forensics and maintaining a chain of custody during an investigation.
- Post-incident activities.
- Case Study: Marriott International Data Breach Notification (2018/2020)

Module 7: Third-Party and Vendor Risk Management

- Identifying risks associated with the supply chain and outsourcing data processing.
- Conducting vendor risk assessments and due diligence before sharing data.
- Key Contractual Obligations for data protection
- Monitoring and auditing third-party adherence to security and privacy standards.
- Managing the risks of shadow IT and unauthorized cloud services.
- Case Study: Equifax Data Breach (2017).

Module 8: Emerging Trends and Future Challenges

- The intersection of AI and Data Privacy.
- Managing the security and privacy risks introduced by IoT devices.
- Introduction to advanced Privacy-Enhancing Technologies
- The growing significance of Data Ethics and corporate social responsibility.
- The shift towards and implications of decentralized identity and tokenized consent.
- Case Study: Clearview AI and Biometric Data Collection.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com