Strategic Digital Ethics and Data Privacy Management Training Course



02 - 06 Nov 2026

Milan

5900 € (Per Person)

Ref: #IT3399_157270

Course Introduction / Overview:

In today's data-driven landscape, the ethical management of digital information and the protection of personal privacy are no longer optional but are fundamental pillars of corporate integrity and consumer trust. This course provides a comprehensive exploration of the critical intersection between digital ethics, data privacy, and corporate governance. We will delve into the principles that underpin responsible data handling, moving beyond mere legal compliance to foster a deep-seated culture of digital responsibility. As Luciano Floridi argues in his seminal work on the philosophy of information, we are living through "The Fourth Revolution," where the lines between our online and offline lives are blurred, making information ethics paramount. This program, offered by BIG BEN Training Center, is meticulously designed to equip professionals with the strategic foresight and practical skills needed to navigate the complex web of global privacy regulations, manage data risks effectively, and lead their organizations in the ethical adoption of emerging technologies like AI. Participants will gain the expertise to build and manage robust privacy programs that not only protect the organization from legal and reputational damage but also establish it as a trustworthy steward of digital information.

Target Audience / This training course is suitable for:

- Data Protection Officers (DPOs).
- Privacy Managers and Analysts.
- Compliance and Ethics Officers.
- IT Security and Information Governance Professionals.
- Legal Counsel and Corporate Lawyers.
- Risk Management Specialists.
- Human Resources Managers.
- Marketing and Data Analytics Leaders.
- Senior Executives and Business Leaders.
- Internal Auditors.

Target Sectors and Industries:

- Technology and Software Development.
- Financial Services, Banking, and Insurance.
- Healthcare and Pharmaceuticals.
- E-commerce and Retail.
- Telecommunications and Media.
- Government Agencies and Public Sector Bodies.
- Consulting and Professional Services.
- Education and Research Institutions.

Target Organizations Departments:

- Legal and Compliance Department.
- Information Technology (IT) and Cybersecurity.
- Risk Management and Internal Audit.
- Human Resources (HR).
- Marketing and Sales.
- Data Analytics and Business Intelligence.
- Corporate Governance and Strategy.
- Customer Service and Support.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop and implement a comprehensive privacy management framework aligned with organizational goals.
- Navigate the complexities of major global data privacy regulations, including GDPR and CCPA.
- Conduct thorough Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs).
- Establish and manage the roles and responsibilities of a Data Protection Officer (DPO).
- Formulate ethical guidelines for the use of artificial intelligence and machine learning.
- Create a robust data breach incident response plan and manage post-breach activities.
- Champion a culture of privacy and data ethics across all organizational departments.
- Implement the principles of Privacy by Design and by Default in new projects and systems.
- Advise senior leadership on strategic decisions related to data privacy and digital ethics.
- Manage cross-border data transfer mechanisms and associated legal requirements.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, practical, and engaging, ensuring that participants can translate theoretical knowledge into real-world application. We move beyond traditional lectures to create a dynamic learning environment centered on active participation. The course heavily utilizes case studies of prominent data breaches and ethical dilemmas, allowing participants to analyze complex scenarios and debate effective solutions in a controlled setting. Collaborative group workshops will challenge teams to design privacy policies, conduct mock Privacy Impact Assessments, and develop incident response strategies. Role-playing exercises will simulate interactions with regulators, data subjects, and senior management, honing communication and negotiation skills. Throughout the course, there will be ample opportunity for open discussion, Q&A sessions with the expert instructor, and peer-to-peer knowledge sharing. This hands-on approach, combining expert instruction with practical application and collaborative problem-solving, ensures that participants leave with the confidence and competence to lead digital ethics and privacy initiatives within their organizations.

Course Agenda (Course Units):

Unit One: Foundations of Digital Ethics and Data Privacy

- Introduction to Digital Ethics and Information Philosophy.
- The Historical Evolution of Privacy as a Concept.
- Core Principles of Data Protection and Fair Information Practices.
- Distinguishing Between Privacy, Security, and Confidentiality.
- The Business Case for Proactive Privacy Management.
- Ethical Frameworks for Decision-Making in Technology.
- Key Terminology and Concepts in the Privacy Profession.

Unit Two: Global Data Privacy Regulatory Landscape

- Deep Dive into the General Data Protection Regulation (GDPR).
- Understanding the California Consumer Privacy Act (CCPA) and CPRA.
- Exploring Other Key Global Regulations (LGPD, PIPEDA, etc.).
- Principles of Territorial Scope and Extraterritorial Application.
- Legal Bases for Processing Personal Data.
- Managing Data Subject Rights (DSRs) Requests.
- Requirements for Cross-Border Data Transfers.

Unit Three: Building and Managing a Privacy Program

- The Role and Responsibilities of the Data Protection Officer (DPO).
- Implementing Privacy by Design and by Default Methodologies.
- Conducting Privacy Impact Assessments (PIAs) and DPIAs.
- Techniques for Data Discovery and Information Flow Mapping.
- Developing and Maintaining Records of Processing Activities (ROPA).
- Vendor and Third-Party Risk Management Strategies.
- Creating Effective Privacy Policies, Notices, and Internal Training Programs.

Unit Four: The Ethics of Data and Emerging Technologies

- Ethical Challenges of Artificial Intelligence (AI) and Machine Learning.
- Addressing Algorithmic Bias and Promoting Fairness.
- The Ethics of Big Data Analytics and Profiling.
- Workplace Monitoring, Surveillance, and Employee Privacy.
- Ethical Considerations for the Internet of Things (IoT).
- Biometric Data and Facial Recognition Technology Governance.
- Corporate Digital Responsibility (CDR) as a Strategic Imperacy.

Unit Five: Incident Response and Fostering a Privacy Culture

- Developing a Comprehensive Data Breach Incident Response Plan.
- Phases of Incident Management: from Detection to Post-Mortem.
- Legal and Regulatory Notification Requirements.
- Managing Public Relations and Communications During a Crisis.
- Conducting Effective Internal Investigations.
- Strategies for Cultivating a Sustainable Culture of Privacy.
- Measuring and Reporting on the Privacy Program's Effectiveness.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As AI becomes more integrated into business operations, where should an organization draw the line between data-driven personalization and intrusive surveillance, and who is ultimately responsible for that decision?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by moving beyond a narrow focus on legal compliance to holistically integrate the three critical pillars of modern data management: legal regulation, operational implementation, and ethical responsibility. While many programs concentrate solely on the articles of regulations like GDPR, this training course emphasizes the strategic and ethical "why" behind the rules. We equip participants not just to follow the law, but to lead their organizations in building a robust culture of Corporate Digital Responsibility. The curriculum is uniquely structured to bridge the communication gap between legal, IT, and business departments, fostering a common language and collaborative approach to privacy. Through intensive case studies of both landmark failures and strategic successes, participants gain practical, actionable insights that are immediately applicable. Rather than simply listing requirements, we engage in deep-dive workshops on complex issues like algorithmic bias, the ethics of AI, and implementing Privacy by Design, ensuring professionals are prepared not only for today's challenges but also for the technological and ethical dilemmas of tomorrow.