Advanced Regulatory Compliance for the Digital Age Training Course

14 - 18 Dec 2026

Milan

5900 € (Per Person)

Ref: #DT1213_93930

Course Introduction / Overview:

The rapid expansion of the digital economy presents unprecedented opportunities alongside complex regulatory challenges. This course provides a comprehensive framework for understanding and navigating the intricate web of laws governing digital transactions, data privacy, and emerging technologies. As organizations increasingly operate in a borderless digital marketplace, maintaining compliance is not just a legal necessity but a critical component of corporate strategy and public trust. We will explore the foundational principles discussed by legal scholars like Lawrence Lessig in his seminal work "Code and Other Laws of Cyberspace," examining how technology itself can regulate behavior. This program, offered by BIG BEN Training Center, is meticulously designed to equip professionals with the knowledge to manage risks associated with data protection, financial technology (Fintech), artificial intelligence (AI), and e-commerce. Participants will gain practical insights into implementing robust compliance programs, ensuring their organizations can innovate responsibly while adhering to global standards like GDPR and navigating the complexities of digital taxation and cybersecurity mandates. This training moves beyond theory, focusing on actionable strategies to build a resilient and ethical digital compliance culture within your organization.

Target Audience / This training course is suitable for:

- Compliance Officers and Managers.
- Legal Counsel and Corporate Lawyers.
- Risk Management Professionals.
- IT and Cybersecurity Managers.
- Internal and External Auditors.
- Data Protection Officers (DPOs).
- Business Development and Strategy Managers.
- Product Development Leaders.
- Public Policy and Government Affairs Specialists.
- Executives and Senior Management.

Target Sectors and Industries:

- Financial Services and Banking (Fintech).
- Technology and Software Development.
- E-commerce and Retail.
- Telecommunications and Media.
- Healthcare and Health Tech.
- Insurance and Insurtech.
- Consulting and Professional Services.
- Governmental and Public Sector Agencies.

Target Organizations Departments:

- Legal and Compliance Department.
- Risk Management Department.
- Information Technology and Cybersecurity.
- Internal Audit and Control.
- Finance and Accounting.
- Product and Service Development.
- Marketing and Digital Advertising.
- Corporate Governance and Strategy.
- Human Resources (related to employee data).

Course Offerings:

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

- Analyze the core legal frameworks governing the global digital economy.
- Implement compliance programs for major data protection regulations like GDPR and CCPA.
- Navigate the regulatory landscape for Fintech, including AML and KYC requirements for digital payments.
- Assess and mitigate legal risks associated with artificial intelligence and algorithmic decision-making.
- Develop strategies for protecting intellectual property in a digital environment.
- Manage cybersecurity compliance according to international standards.
- Understand the principles of digital taxation and cross-border e-commerce laws.
- Conduct effective internal compliance audits for digital operations.
- Formulate a corporate digital responsibility and ethics policy.
- Anticipate and prepare for future trends in technology regulation.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring that participants can translate theoretical knowledge into real-world application. We move beyond traditional lectures to foster a dynamic learning environment where engagement is key. The course heavily utilizes case study analysis of prominent international compliance successes and failures, allowing participants to dissect complex scenarios and understand their practical implications. Interactive group discussions and workshops will challenge attendees to solve real-world problems, such as designing a data breach response plan or evaluating the ethical implications of an AI-driven service. Role-playing exercises will simulate compliance audits and regulatory negotiations, building confidence and practical skills. Our expert instructors facilitate a collaborative atmosphere, encouraging peer-to-peer learning and knowledge sharing. Continuous feedback is provided throughout the sessions to ensure a deep understanding of the material. This hands-on, problem-solving approach ensures that participants leave not just with knowledge, but with the competence to implement effective digital compliance strategies immediately within their organizations.

Course Agenda (Course Units):

Unit One: Foundations of Digital Economy Regulation

- Introduction to the Digital Economy and Its Legal Architecture.
- Key Global Regulatory Bodies and Enforcement Agencies.
- Core Principles of Digital Governance and Rule of Law Online.
- The Intersection of Technology, Ethics, and Law.
- Understanding Jurisdiction in a Borderless Digital World.
- An Overview of Major International Digital Trade Agreements.
- The Role of Corporate Digital Responsibility (CDR).

Unit Two: Data Privacy and Protection Compliance

- Deep Dive into the General Data Protection Regulation (GDPR).
- Navigating the California Consumer Privacy Act (CCPA) and other US State Laws.
- Principles of Data Minimization, Consent Management, and Lawful Processing.
- Managing Data Subject Access Requests (DSARs).
- Legal Frameworks for Cross-Border Data Transfers.
- Developing a Comprehensive Data Breach Incident Response Plan.
- The Role and Responsibilities of the Data Protection Officer (DPO).

Unit Three: Regulating Fintech, E-Commerce, and Digital Markets

- Anti-Money Laundering (AML) and Know Your Customer (KYC) in Digital Finance.
- Regulatory Approaches to Cryptocurrencies and Digital Assets.
- Consumer Protection Laws for E-commerce and Online Marketplaces.
- Rules Governing Digital Advertising and Online Marketing.
- Understanding Digital Services Taxes and Online Sales Tax Compliance.
- Competition Law and Antitrust Issues in Big Tech.
- Compliance for Digital Payment Systems and Gateways.

Unit Four: Cybersecurity, AI, and Intellectual Property Law

- Key Cybersecurity Compliance Frameworks (e.g., NIST, ISO 27001).
- Legal Requirements for Cybersecurity Risk Management and Reporting.
- Emerging Legal Frameworks for Artificial Intelligence (AI) Governance.
- Addressing Algorithmic Bias, Transparency, and Accountability.
- Protecting Copyright and Trademarks in the Digital Sphere.
- Patent Law Considerations for Software and Technology Innovations.
- Trade Secrets and Confidential Information in a Digital Workplace.

Unit Five: Advanced Compliance Strategy and Future Horizons

- Leveraging Regulatory Technology (RegTech) for Automated Compliance.
- Designing and Implementing an Integrated Digital Compliance Program.
- Conducting Effective Digital Compliance Audits and Risk Assessments.
- Managing Third-Party and Supply Chain Digital Risks.
- Crisis Management for Major Compliance Failures.
- Horizon Scanning. Preparing for Future Regulations in Quantum Computing and IoT.
- Developing a Culture of Proactive and Ethical Digital Compliance.

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 artificial intelligence becomes more autonomous, at what point should legal liability for its actions shift from the human creators and operators to the AI entity itself, and what regulatory framework could support such a concept?

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

This course distinguishes itself by adopting a forward-looking, integrated perspective on digital regulation, recognizing that compliance is no longer a siloed function. Unlike programs that focus on a single area like data privacy or fintech, we connect the dots between data protection, AI ethics, cybersecurity law, and digital market regulation, providing a holistic understanding of the modern compliance landscape. Our curriculum is built on a foundation of practical application rather than abstract legal theory. We emphasize strategic thinking through extensive use of contemporary case studies from leading global technology and financial firms, enabling participants to learn from real-world successes and failures. The content is continuously updated to reflect the latest regulatory developments and technological trends, ensuring participants receive the most current and relevant knowledge. Furthermore, the course structure encourages critical thinking about future challenges, moving beyond current laws to prepare professionals for the next wave of regulatory change in areas like quantum computing and the Internet of Things (IoT), making it an investment in long-term strategic competence.