Cyber Law, Data Privacy, and Security Compliance Training Course



28 Dec 2026 - 01 Jan 2027

Milan

5900 € (Per Person)

Ref: #LAW8846_155382

Course Introduction / Overview:

In today's digitally-driven world, the intersection of law, technology, and data has created a complex regulatory landscape that is challenging for organizations to navigate. This course provides a comprehensive exploration of cyber law, data privacy principles, and digital security regulations. It is designed to equip professionals with the essential knowledge to ensure their organizations operate within legal boundaries while protecting critical digital assets. As the renowned legal scholar Lawrence Lessig argued in his seminal work, "Code and Other Laws of Cyberspace," the architecture of the digital world itself is a form of regulation. Understanding this "code" is no longer optional but a fundamental aspect of corporate governance and risk management. This program, offered by BIG BEN Training Center, moves beyond theoretical discussions to provide practical, actionable strategies for implementing robust compliance frameworks. Participants will delve into major international regulations, learn to manage data breaches effectively, and develop policies that align with both legal requirements and business objectives, ensuring a proactive stance on digital compliance.

Target Audience / This training course is suitable for:

- Legal Counsel and Corporate Lawyers.
- Compliance Officers and Managers.
- Information Security and Cybersecurity Professionals.
- IT Managers and Directors.
- Risk Management Professionals.
- Data Protection Officers (DPOs).
- Human Resources Managers.
- Internal and External Auditors.
- Executives and Senior Managers with oversight of data and technology.
- Policy Makers and Regulatory Affairs Specialists.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Technology and Telecommunications.
- E-commerce and Retail.
- Government and Public Sector Agencies.
- Consulting and Professional Services.
- Education and Research Institutions.
- Media and Entertainment.
- Energy and Utilities.

Target Organizations Departments:

- Legal Department.
- Compliance and Ethics Department.
- Information Technology (IT) and Information Security.
- Risk Management Department.
- Internal Audit.
- Human Resources (HR).
- Operations Management.
- Procurement and Vendor Management.
- Marketing and Sales.
- Research and Development (R&D).

Course Offerings:

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

- Analyze the core principles of international cyber law and its jurisdiction.
- Interpret the requirements of major data privacy regulations like GDPR and CCPA.
- Develop and implement effective data protection and information governance policies.
- Conduct a Privacy Impact Assessment (PIA) to identify and mitigate risks.
- Formulate a legally compliant data breach incident response plan.
- Evaluate the legal implications of cloud computing, IoT, and artificial intelligence.
- Manage cross-border data transfer challenges and solutions.
- Ensure third-party and vendor contracts are compliant with data security standards.
- Navigate the complexities of digital evidence and e-discovery processes.
- Foster a culture of data privacy and security awareness within the organization.

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 employ a blended learning approach that combines expert-led presentations with dynamic, hands-on activities. The course heavily features the analysis of recent, high-profile case studies to illustrate the consequences of non-compliance and the best practices for risk mitigation. Participants will engage in collaborative group workshops to draft sample data protection policies and simulate incident response scenarios, fostering teamwork and problem-solving skills. Interactive Q&A sessions, peer-to-peer discussions, and practical exercises are integrated throughout the five days to reinforce learning and address specific organizational challenges. Our experienced instructors provide continuous feedback and facilitate a learning environment where participants can confidently explore complex legal and technical concepts. This immersive approach ensures a deep and lasting understanding of cyber law and data privacy compliance.

Course Agenda (Course Units):

Unit One: Foundations of Cyber Law and Digital Governance

- Introduction to the legal framework of cyberspace.
- Sources of cyber law and key legal principles.
- Understanding jurisdiction in a borderless digital world.
- The intersection of technology, ethics, and law.
- Intellectual property rights in the digital age.
- Online contracts and the validity of electronic signatures.
- Introduction to information governance and its importance.

Unit Two: Global Data Privacy Regulations and Compliance

- Deep dive into the General Data Protection Regulation (GDPR).
- Understanding the California Consumer Privacy Act (CCPA) and its evolution.
- Comparative analysis of other global privacy laws (LGPD, PIPEDA).
- Core principles of data protection: lawfulness, fairness, and transparency.
- The roles and responsibilities of Data Controllers and Processors.
- Conducting Data Protection Impact Assessments (DPIAs).
- Mechanisms for lawful cross-border data transfers.

Unit Three: Digital Security, Cybercrime, and Incident Response

- The legal definition and classification of cybercrime.
- Key digital security regulations and standards (e.g., NIST, ISO 27001).
- Developing a comprehensive Information Security Policy.
- Legal requirements for data breach notification.
- Creating and testing an effective Incident Response Plan (IRP).
- The role of digital forensics in legal investigations.
- Understanding cyber insurance and liability.

Unit Four: Corporate Compliance and Information Governance

- Building a corporate data privacy compliance program.
- The function of the Data Protection Officer (DPO).
- Implementing Privacy by Design and by Default.
- Managing employee data privacy and workplace monitoring.
- Vendor and third-party risk management strategies.
- Conducting internal compliance audits and assessments.
- Developing effective data retention and destruction policies.

Unit Five: Advanced Topics and Future Trends in Cyber Law

- The legal implications of Artificial Intelligence (AI) and machine learning.
- Navigating the regulatory landscape for the Internet of Things (IoT).
- Legal challenges of cloud computing and data sovereignty.
- The future of digital identity and authentication.
- E-discovery and managing electronically stored information (ESI) in litigation.
- Ethical considerations in data collection and use.
- Preparing for upcoming changes in cyber law and data privacy.

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 corporate decision-making, how should legal frameworks evolve to assign liability for AI-driven data breaches or privacy violations?

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

This course distinguishes itself by adopting a holistic and integrative framework that bridges the critical gap between legal theory, technical implementation, and corporate strategy. While many programs focus narrowly on a single regulation or the legal aspects alone, this curriculum is meticulously designed to provide a 360-degree view of the digital compliance ecosystem. It moves beyond reciting legal articles to explore their operational impact, guiding participants on how to build practical, sustainable compliance programs from the ground up. The content is enriched with an in-depth analysis of contemporary case studies, focusing not just on the legal failings but on the organizational and technical precursors to major data breaches. Furthermore, the course places a strong emphasis on forward-looking topics such as the legal ramifications of AI and IoT, equipping professionals not only for today's challenges but also for the evolving digital landscape of tomorrow. The methodology prioritizes interactive problem-solving over passive listening, ensuring participants leave with tangible skills and strategic insights applicable within their own organizations.