Legal Aspects of Cybersecurity and Data Protection Training Course

07 - 11 Dec 2026

Milan

5900 € (Per Person)

Ref: #LAW2046_43116

Course Introduction / Overview:

In our digital world, cybersecurity and data protection are no longer just technical issues; they are legal and strategic imperatives. This intensive training course from BIG BEN Training Center is designed to give participants a deep understanding of the legal frameworks that govern information security and privacy. We will explore key laws and regulations, such as GDPR and CCPA, and their impact on corporate operations. Drawing on insights from prominent legal scholars like Daniel J. Solove, a distinguished law professor and author of "Understanding Privacy," this course provides a comprehensive view of how privacy law and cybersecurity intersect. We'll examine the legal liabilities of data breaches, the importance of data governance, and the legal requirements for incident response. The program is designed to help professionals navigate a complex legal landscape and develop strategies to protect their organizations from legal and financial risks. We will cover everything from intellectual property protection to the legal challenges of cloud computing. Our goal is to equip you with the knowledge and skills needed to build a strong legal and compliance program for data protection and information security.

Target Audience / This training course is suitable for:

- Legal and compliance officers.
- IT and information security managers.
- Chief Information Officers (CIOs).
- Data privacy officers.
- Risk management professionals.
- Internal auditors.
- Corporate executives and board members.
- Human resources managers.
- Professionals responsible for data governance.

Target Sectors and Industries:

- Technology and telecommunications.
- Banking and financial services.
- Healthcare and insurance.
- Retail and e-commerce.
- Government agencies and public services.
- Legal and consulting services.
- Education and research institutions.
- Government agencies and equivalents.

Target Organizations Departments:

- Legal and compliance departments.
- Information technology and security.
- Risk management departments.
- Human resources.
- Internal audit.
- Corporate governance.
- Data privacy offices.
- Public relations.

Course Offerings:

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

- Master the legal requirements for data protection and privacy.
- Develop and implement a robust cybersecurity legal framework.
- Understand legal liabilities related to data breaches and cyber incidents.
- Apply key principles of data governance and information management.
- Navigate the complexities of international data transfer laws.
- Draft and negotiate contracts that address cybersecurity risks.
- Respond to regulatory investigations and compliance audits.
- Advise on legal issues related to intellectual property and trade secrets.
- Build a strong culture of compliance within the organization.

Course Methodology:

This training course uses a mix of interactive and practical methods to give participants a deep understanding of the material. Our approach includes detailed case studies based on real-world data breaches and legal disputes, allowing participants to apply their knowledge to challenging scenarios. We also use interactive group discussions and workshops to explore complex topics like data privacy and information security law. For instance, a session might simulate a regulatory audit, giving participants a chance to practice their response. We also include role-playing exercises that help you practice key skills, such as incident response and communication with legal counsel. The curriculum is designed to be highly engaging, with practical exercises that help participants apply legal frameworks to various scenarios. This hands-on approach, combined with expert-led discussions and continuous feedback, ensures a dynamic learning environment where participants can deepen their understanding and develop practical legal training skills for the digital age.

Course Agenda (Course Units):

Unit One: Foundations of Cybersecurity Law

- Overview of legal frameworks for cybersecurity.
- Legal principles of data protection and privacy.
- Understanding intellectual property in a digital context.
- Legal liabilities for data breaches.
- Introduction to international legal standards.

Unit Two: Data Privacy Regulations

- The General Data Protection Regulation (GDPR).
- The California Consumer Privacy Act (CCPA).
- Other regional and sectoral data privacy laws.
- Data governance and data minimization.
- Consent and consumer rights.

Unit Three: Information Security and Legal Compliance

- Developing a legal information security program.
- Incident response and breach notification laws.
- Cybersecurity contracts and vendor management.
- Legal requirements for cloud computing.
- Building a culture of security and legal compliance.

Unit Four: Regulatory Enforcement and Litigation

- Regulatory investigations and audits.
- Civil litigation and class action lawsuits.
- Criminal prosecution of cybercrimes.
- Legal strategies for mitigating risk.
- Working with legal counsel and law enforcement.

Unit Five: Emerging Legal Issues and Future Trends

- Legal challenges of AI and machine learning.
- The legal status of biometrics and facial recognition.
- Data localization and cross-border data transfers.
- The future of data protection law.
- Ethical considerations in cybersecurity.

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 technology continues to evolve, how can legal frameworks balance the need for innovation and data use with the fundamental right to privacy and security for individuals?

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

This training course is unique because it connects the technical aspects of cybersecurity with the crucial legal requirements of data protection. Many training programs focus on one or the other, but we believe professionals need to understand both to be effective. Our curriculum gives you a comprehensive view of the legal landscape, from major regulations like GDPR to emerging issues like AI. We use a case-based approach, which is far more engaging than a typical lecture, to help you understand how legal principles are applied in real-world scenarios, such as responding to a data breach or drafting a privacy policy. This program is also designed for a diverse audience, including both legal and technical professionals, fostering a collaborative learning environment. By focusing on both the legal framework and practical implementation, we ensure our graduates can not only advise on compliance but also help build a secure and resilient organization. This is a crucial skill set in a world where data is a primary asset.