



*Training Course:  
Cybersecurity Law: Legal Frameworks &  
Compliance*

*22 - 26 September 2025  
Madrid (Spain)  
Pestana CR7 Gran Vía*

## Training Course: Cybersecurity Law: Legal Frameworks & Compliance

Training Course code: IT235751 From: 22 - 26 September 2025 Venue: Madrid (Spain) - Pestana CR7 Gran Vía Training Course Fees: 6000 € Euro

### Introduction

As organizations become increasingly reliant on digital infrastructure, cybersecurity law has emerged as a critical area of focus. Governments and regulatory bodies worldwide are implementing legal frameworks to protect sensitive data, prevent cyber threats, and enforce compliance with cybersecurity regulations.

This 5-day training program provides professionals with comprehensive knowledge of cybersecurity law, covering legal obligations, regulatory compliance, incident response, and ethical considerations. Participants will gain an in-depth understanding of global cybersecurity laws, risk management practices, and legal responsibilities to ensure their organizations remain compliant while mitigating cybersecurity risks.

### Course Objectives

By the end of this training, participants will be able to:

- Understand the fundamentals of cybersecurity law and regulatory requirements.
- Analyze key cybersecurity laws and compliance frameworks across different jurisdictions.
- Identify legal responsibilities for data protection, privacy, and incident reporting.
- Navigate cybercrime regulations and enforcement mechanisms.
- Develop strategies for legal risk management in cybersecurity.
- Understand contractual obligations related to cybersecurity in business operations.
- Ensure organizational compliance with cybersecurity and data protection laws.

### Target Audience

This program is designed for professionals involved in cybersecurity, legal compliance, and IT governance, including:

- Legal Advisors & Compliance Officers overseeing cybersecurity regulations.
- IT & Cybersecurity Professionals responsible for data security and legal compliance.
- Risk Managers & Data Protection Officers DPOs handling cybersecurity governance.
- Corporate Executives & Decision-Makers ensuring regulatory adherence.
- Law Enforcement & Government Officials working in cybersecurity law enforcement.

### Training Program Outline

Day 1: Introduction to Cybersecurity Law & Global Legal Frameworks

- Understanding Cybersecurity Law and its Importance.
- Key principles of cyber law and regulatory compliance.
- Overview of international cybersecurity regulations and legal frameworks:
  - GDPR General Data Protection Regulation
  - CCPA California Consumer Privacy Act
  - NIST National Institute of Standards and Technology Cybersecurity Framework
  - ISO 27001 & Other Compliance Standards
- Case Study: Legal Implications of Cybersecurity Breaches.

#### Day 2: Data Protection & Privacy Laws

- The legal importance of data protection and privacy rights.
- Regulatory requirements for handling personal and sensitive data.
- Consent, data collection, and processing under privacy laws.
- Cross-border data transfers and legal challenges.
- Corporate liability in data breaches and legal penalties.
- Interactive Session: Analyzing Real-World Data Protection Cases.

#### Day 3: Cybercrime Laws & Legal Responsibilities

- Understanding cybercrime and legal enforcement mechanisms.
- Categories of cyber offenses: hacking, identity theft, phishing, malware attacks.
- International conventions and cybercrime laws:
  - Budapest Convention on Cybercrime
  - Computer Fraud and Abuse Act CFAA
  - Electronic Communications Privacy Act ECPA
- The role of law enforcement and corporate cybersecurity teams in combating cybercrime.
- Group Discussion: Cybercrime Cases and Legal Consequences.

#### Day 4: Incident Response & Legal Obligations in Cybersecurity

- Legal obligations in cybersecurity incident response.
- Incident reporting requirements under various legal frameworks.
- Understanding cybersecurity liability and corporate governance.
- Legal considerations for forensic investigations and digital evidence.
- Workshop: Developing a Legally Compliant Incident Response Plan.

#### Day 5: Cybersecurity Contracts, Compliance, & Risk Management

- Cybersecurity clauses in business contracts and vendor agreements.
- Third-party risk management and legal accountability.
- Best practices for ensuring cybersecurity compliance.
- Ethical considerations in cybersecurity law and policy.
- Final Case Study: Building a Cybersecurity Legal Compliance Strategy.

## Registration form on the Training Course: Cybersecurity Law: Legal Frameworks & Compliance

Training Course code: IT235751 From: 22 - 26 September 2025 Venue: Madrid (Spain) - Pestana CR7 Gran Vía Training Course Fees: 6000 € Euro

Complete & Mail or fax to Global Horizon Training Center (GHTC) at the address given below

### Delegate Information

Full Name (Mr / Ms / Dr / Eng): .....  
 Position: .....  
 Telephone / Mobile: .....  
 Personal E-Mail: .....  
 Official E-Mail: .....

### Company Information

Company Name: .....  
 Address: .....  
 City / Country: .....

### Person Responsible for Training and Development

Full Name (Mr / Ms / Dr / Eng): .....  
 Position: .....  
 Telephone / Mobile: .....  
 Personal E-Mail: .....  
 Official E-Mail: .....

### Payment Method

- Please find enclosed a cheque made payable to Global Horizon
- Please invoice me
- Please invoice my company

### Easy Ways To Register

Telephone:  
+201095004484 to  
provisionally reserve your  
place.

Fax your completed  
registration  
form to: +20233379764

E-mail to us :  
info@gh4t.com  
or training@gh4t.com

Complete & return the  
booking form with cheque  
to: Global Horizon  
3 Oudai street, Aldouki,  
Giza, Giza Governorate,  
Egypt.