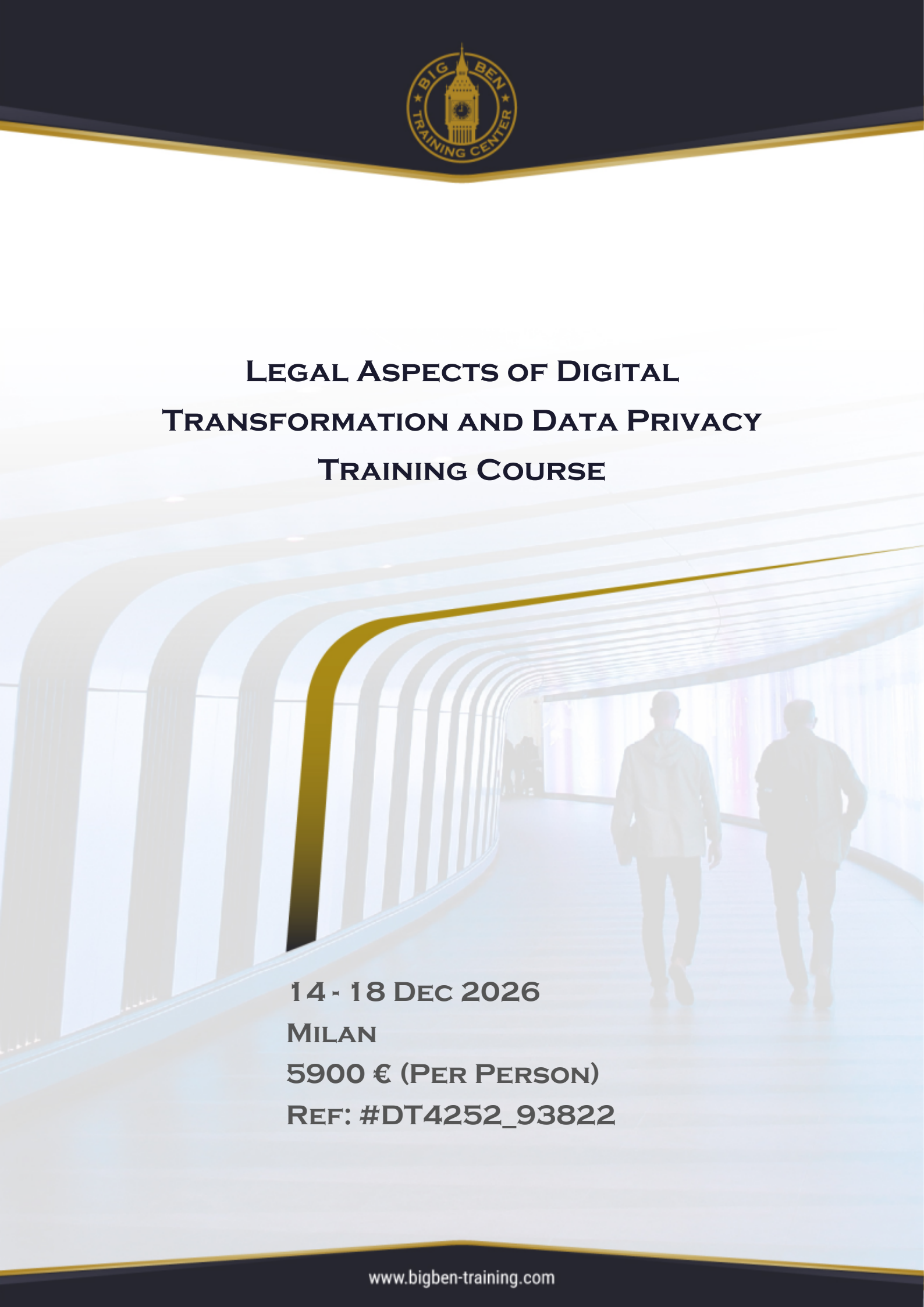
Legal Aspects of Digital Transformation and Data Privacy Training Course



14 - 18 Dec 2026

Milan

5900 € (Per Person)

Ref: #DT4252_93822

Course Introduction / Overview:

In an era defined by rapid technological advancement, understanding the legal landscape of digital transformation is no longer optional but a critical necessity for organizational survival and growth. This comprehensive course is meticulously designed to navigate the complex intersection of law, technology, and data privacy. It provides a deep dive into the regulatory frameworks, compliance requirements, and legal risks associated with digital innovation. Drawing upon foundational concepts from experts like Lawrence Lessig and his seminal work, "Code and Other Laws of Cyberspace," participants will explore how technology itself can regulate behavior and the legal implications this carries. This program offered by BIG BEN Training Center moves beyond theoretical knowledge, equipping professionals with the practical skills to manage data governance, mitigate cybersecurity threats, and ensure ethical AI implementation. We will dissect global data protection regulations, analyze the legalities of emerging technologies, and formulate robust compliance strategies, ensuring your organization can innovate confidently while upholding legal and ethical standards in the digital age.

Target Audience / This training course is suitable for:

- Legal Counsel and Corporate Lawyers.
- Data Protection Officers (DPOs) and Privacy Professionals.
- Compliance and Risk Management Officers.
- IT Managers and Cybersecurity Specialists.
- C-Suite Executives (CEOs, CIOs, CTOs).
- Policy Makers and Government Regulators.
- Human Resources Managers.
- Digital Marketing and E-commerce Managers.
- Entrepreneurs and Business Owners.

Target Sectors and Industries:

- Technology and Software Development.
- Financial Services and FinTech.
- Healthcare and Life Sciences.
- Retail and E-commerce.
- Telecommunications and Media.
- Government Agencies and Public Sector Bodies.
- Consulting and Professional Services.
- Education and EdTech.
- Manufacturing and Industrial IoT.

Target Organizations Departments:

- Legal Department.
- Compliance and Regulatory Affairs.
- Information Technology (IT) and Information Security.
- Risk Management.
- Internal Audit.
- Executive Management.
- Human Resources.
- Marketing and Sales.
- Research and Development (R&D).

Course Offerings:

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

- Analyze the legal frameworks governing digital transformation and data privacy globally.
- Develop and implement comprehensive data protection programs compliant with GDPR, CCPA, and other regulations.
- Assess and mitigate legal risks associated with cybersecurity incidents and data breaches.
- Navigate the legal complexities of emerging technologies such as AI, blockchain, and the Internet of Things (IoT).
- Draft and review legally sound digital contracts, privacy policies, and terms of service.
- Manage intellectual property rights in a digital context, including software patents and digital copyright.
- Formulate strategies for lawful cross-border data transfers and cloud computing arrangements.
- Establish a corporate digital responsibility framework that aligns with legal and ethical standards.
- Lead an effective legal response to a cybersecurity incident or data privacy inquiry.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring participants can translate legal theory into actionable business strategy. We employ a blended learning approach that combines expert-led instruction with hands-on, collaborative exercises. The course is built around real-world case studies of landmark legal challenges in the digital space, allowing participants to analyze complex scenarios and debate potential outcomes. Interactive workshops will focus on practical skills such as drafting data processing agreements, conducting privacy impact assessments (PIAs), and developing incident response plans. Group discussions and peer-to-peer learning are encouraged to foster a dynamic environment where diverse professional experiences enrich the conversation. Participants will engage in simulation exercises that challenge them to make critical legal decisions under pressure. Continuous feedback from the instructor ensures a deep understanding of the material, empowering attendees to return to their organizations with the confidence and competence to lead digital legal and compliance initiatives effectively.

Course Agenda (Course Units):

Unit One: Foundations of Digital Law and Governance

- Introduction to Digital Transformation and its Legal Dimensions.
- Overview of Global Legal Frameworks for Technology.
- The Intersection of Law, Ethics, and Code.
- Key Principles of Data Governance and Information Management.
- Understanding Electronic Signatures and Digital Contracts.
- Jurisdictional Challenges in the Digital World.
- The Role of the Corporate Legal Department in Digital Strategy.

Unit Two: Mastering Data Privacy and Protection

- Deep Dive into the General Data Protection Regulation (GDPR).
- Exploring the California Consumer Privacy Act (CCPA) and other US Privacy Laws.
- Principles of Data Protection by Design and by Default.
- Managing Data Subject Rights and Consent Mechanisms.
- Conducting Data Protection Impact Assessments (DPIAs).
- Legal Requirements for Data Processing and Sharing Agreements.
- The Role and Responsibilities of the Data Protection Officer (DPO).

Unit Three: Cybersecurity Law and Incident Response

- The Legal Landscape of Cybersecurity and Cybercrime.
- Developing a Legally Compliant Cybersecurity Policy.
- Data Breach Notification Laws and Regulatory Obligations.
- Legal Best Practices for Incident Response Planning.
- Managing Digital Forensics and Evidence Preservation.
- Liability for Cybersecurity Failures and Vendor Risk Management.
- Cyber Insurance and its Role in Risk Mitigation.

Unit Four: Intellectual Property and Emerging Technologies

- Protecting Intellectual Property in the Digital Age.
- Copyright Issues in Software, Content, and Data.
- Trademark and Domain Name Disputes.
- Legal and Ethical Implications of Artificial Intelligence (AI).
- Navigating the Legal Framework for Blockchain and Cryptocurrencies.
- The Internet of Things (IoT) and Associated Legal Risks.
- Regulating Big Data and Algorithmic Decision-Making.

Unit Five: Strategic Compliance and Corporate Digital Responsibility

- Building an Integrated Digital Compliance Framework.
- Managing Lawful Cross-Border Data Transfers.
- Legal Considerations for Cloud Computing and SaaS Agreements.
- Corporate Digital Responsibility and Ethical Technology Use.
- Preparing for and Managing Regulatory Audits and Investigations.
- Future-Proofing Legal Strategy for Upcoming Technological Trends.
- Capstone Project: Developing a Digital Transformation Legal Roadmap.

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 autonomous, how should legal frameworks evolve to assign liability for its actions, moving beyond traditional models of corporate or individual responsibility?

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

This course distinguishes itself by moving beyond a mere recitation of existing laws and regulations. Its core strength lies in its forward-looking, strategic approach, preparing participants not just for today's compliance challenges but for the legal complexities of tomorrow's technologies. Unlike programs that focus narrowly on a single regulation, this curriculum provides a holistic, global perspective, integrating data privacy, cybersecurity, intellectual property, and the legalities of emerging technologies like AI and blockchain into a single, cohesive framework. The emphasis is on practical application and strategic decision-making. Through immersive case studies and simulations, participants learn to build robust compliance programs, manage incident responses, and draft effective digital policies. The course champions the concept of Corporate Digital Responsibility, embedding ethical considerations into legal strategy. This ensures that graduates are not only compliant legal or IT professionals but also strategic advisors who can guide their organizations to innovate responsibly and build sustainable trust in an increasingly digital world.