Advanced GDPR and Data Privacy for the Banking Sector Training Course



02 - 06 Nov 2026

Milan

5900 € (Per Person)

Ref: #BI2138_175414

Course Introduction / Overview:

The global banking sector operates on a foundation of trust, which is inextricably linked to the secure and ethical handling of customer data. In an era of increasing digitalization and sophisticated cyber threats, robust data privacy frameworks are not just a legal necessity but a core business imperative. This intensive training course is meticulously designed to navigate the complex landscape of data protection, with a specific focus on the General Data Protection Regulation (GDPR) and its profound implications for financial institutions. We will delve into the critical principles that govern data processing, security, and compliance, moving beyond theoretical knowledge to practical application. As highlighted by the renowned privacy scholar Daniel J. Solove in his works like "Understanding Privacy," the interpretation of privacy principles is nuanced and context-dependent. This program, offered by BIG BEN Training Center, provides that essential banking context, equipping professionals with the tools to build and manage effective data privacy programs, mitigate risks of costly data breaches, and uphold customer trust in a data-driven world. This course ensures your organization not only complies with regulations but also leverages data privacy as a competitive advantage.

Target Audience / This training course is suitable for:

- Data Protection Officers (DPOs).
- Compliance Managers and Officers.
- IT Security Professionals and Managers.
- Risk Management Professionals.
- Legal Counsel and In-house Lawyers.
- Internal and External Auditors.
- Senior Banking Executives and Managers.
- Operations Managers in Financial Institutions.
- Customer Relationship Managers.
- Product Development Teams in Fintech and Banking.

Target Sectors and Industries:

- Commercial and Retail Banking.
- Investment Banking and Asset Management.
- Credit Unions and Cooperative Banks.
- Financial Technology (Fintech) and Payment Processors.
- Insurance and Reinsurance Companies.
- Private Equity and Venture Capital Firms.
- Government Financial Regulatory Bodies.
- Central Banks and Monetary Authorities.
- Wealth Management and Private Banking.

Target Organizations Departments:

- Legal and Compliance Department.
- Information Technology (IT) and Cybersecurity.
- Risk Management Department.
- Internal Audit and Control.
- Operations and Back Office.
- Customer Service and Client Relations.
- Marketing and Sales Departments.
- Human Resources (for employee data).
- Product and Service Development.
- Executive Management.

Course Offerings:

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

- Interpret and apply the core principles of GDPR within a banking context.
- Develop and implement a comprehensive data privacy framework for a financial institution.
- Conduct a thorough Data Protection Impact Assessment (DPIA) for new banking products and services.
- Master the requirements for lawful data processing, including consent and legitimate interest.
- Design and manage a robust data breach incident response and notification plan.
- Navigate the complexities of international cross-border data transfers for financial data.
- Effectively manage data subject rights requests, including access, rectification, and erasure.
- Evaluate and mitigate data privacy risks associated with third-party vendors and partners.
- Implement Privacy by Design and by Default in banking systems and processes.
- Prepare for and confidently manage regulatory audits and investigations.

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 actionable skills. We move beyond traditional lectures to foster a dynamic learning environment where engagement is key. The course heavily relies on real-world case studies drawn from the banking and financial services industry, analyzing actual data breaches, regulatory enforcement actions, and compliance successes. Participants will engage in collaborative group workshops to tackle practical challenges, such as drafting a record of processing activities (ROPA) or developing a DPIA for a hypothetical fintech application. Interactive sessions, expert-led discussions, and Q&A segments encourage critical thinking and peer-to-peer learning. Role-playing exercises will simulate scenarios like responding to a data subject access request or managing a data breach crisis, providing hands-on experience in a controlled setting. Continuous feedback from the instructor ensures that participants grasp complex concepts and can confidently apply them within their own organizations upon completion of the course.

Course Agenda (Course Units):

Unit One: Foundations of Data Privacy in the Financial Sector

- The Evolution of Data Protection Law and the Rise of GDPR.
- Core GDPR Principles and Terminology (Personal Data, Processing, Controller, Processor).
- Special Categories of Data and Their Relevance in Banking.
- Legal Bases for Processing Customer Financial Data.
- The Role and Responsibilities of the Data Protection Officer (DPO) in a Bank.
- Understanding the Territorial Scope of GDPR for Global Financial Institutions.
- Key Differences Between Data Protection and Data Security.

Unit Two: Implementing GDPR Compliance in Banking Operations

- Managing Data Subject Rights (Access, Rectification, Erasure, Portability).
- Consent Management Frameworks for Banking and Marketing Activities.
- Conducting Data Protection Impact Assessments (DPIAs) for High-Risk Processing.
- Creating and Maintaining Records of Processing Activities (ROPA).
- Implementing Privacy by Design and by Default in System Development.
- Data Minimization and Retention Policies for Financial Records.
- Training and Awareness Programs for Bank Employees.

Unit Three: Data Security, Risk, and Breach Management

- Technical and Organizational Measures (TOMs) for Protecting Financial Data.
- Encryption, Pseudonymization, and Anonymization Techniques.
- Developing a Comprehensive Data Breach Incident Response Plan.
- Breach Notification Requirements to Supervisory Authorities and Data Subjects.
- Managing Cyber-Risks and Third-Party Vendor Security.
- Physical Security Measures for Data Protection.
- Conducting Regular Security Audits and Penetration Testing.

Unit Four: Advanced GDPR Topics and International Data Flows

- Navigating Cross-Border Data Transfers (SCCs, BCRs, Adequacy Decisions).
- Data Privacy Considerations for Cloud Computing in Banking.
- Compliance Challenges with FinTech, AI, and Big Data Analytics.
- GDPR Compliance in Digital Marketing and Customer Profiling.
- Liability and Responsibilities between Data Controllers and Processors.
- Data Protection for Employee and HR Data within a Bank.
- Understanding the ePrivacy Regulation and its Impact on Banking.

Unit Five: Enforcement, Auditing, and Future-Proofing Compliance

- The Role and Powers of Data Protection Authorities (DPAs).
- Understanding Administrative Fines, Penalties, and Sanctions.
- Preparing for and Managing a Regulatory GDPR Audit.
- Building a Culture of Data Privacy within the Organization.
- Monitoring and Reviewing the Data Protection Framework.
- Global Trends in Data Privacy Legislation Beyond GDPR.
- Strategic Planning for Future Data Protection Challenges in Finance.

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 and machine learning become more integrated into banking for services like credit scoring and fraud detection, how can financial institutions balance the drive for innovation with the fundamental GDPR principle of data minimization and purpose limitation?

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

This course distinguishes itself by moving beyond generic data protection training to offer a specialized, in-depth focus exclusively on the banking and financial services sector. While other programs provide a broad overview of GDPR, our curriculum is built around the specific and complex data processing activities inherent to finance, from customer onboarding and credit scoring to anti-money laundering (AML) checks and international fund transfers. We utilize case studies and practical scenarios that are directly relevant to banking professionals, such as managing data breaches involving financial information or conducting DPIAs for new mobile banking applications. The content is meticulously curated to address the unique intersection of data privacy laws with other financial regulations. Our approach emphasizes the practical application of principles, ensuring participants learn not just what the law says, but how to implement it within the intricate operational and technological frameworks of a modern financial institution. This targeted approach provides a level of depth and relevance that generalist courses cannot match, equipping attendees with immediately applicable, industry-specific expertise.