GDPR Operational Compliance and Accountability Training Course

16 – 20 August 2027
Addis Ababa

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

GDPR Operational Compliance and Accountability Training Course

Ref: 819_224035 **Date:** 16 – 20 August 2027 **Location:** Addis Ababa **Fees:** 4500 Euro

Overview

GDPR Operational Compliance and Accountability Training Course is a one-week intermediate course for privacy, compliance, governance, process, legal operations, and information security functions who leave with a GDPR Operations and Evidence Pack. Participants convert regulatory duties into processing records, lawful-basis decisions, notices, rights workflows, processor controls, transfer assessments, retention rules, DPIAs, incident coordination, and assurance evidence. The course separates legal interpretation from repeatable operational responsibilities. Agile Leaders Training Center develops practical GDPR accountability capability.

Who Should Attend

- Privacy functions responsible for governance, advice, records, rights, and assurance
- Compliance and risk functions responsible for control design, monitoring, and evidence
- Business process functions responsible for personal-data collection, use, sharing, and retention
- Legal operations functions responsible for requirements, contracts, and escalation coordination
- Information security functions responsible for safeguards, incidents, and breach evidence
- Procurement and vendor functions responsible for processors and international data flows

The course assumes participants already support processes involving personal data, and leaves out legal representation, regulator-specific case strategy, technical penetration testing, and certification examination preparation.

Departments and Industries

The course supports departments and industries that need structured evidence of personal-data governance and operational control.

- Privacy, compliance, risk, audit, legal operations, and corporate governance
- Information security, technology governance, data management, procurement, and vendor oversight
- Human resources, marketing, customer operations, finance, and product management
- Financial services, healthcare, technology, retail, telecommunications, and professional services
- Manufacturing, logistics, hospitality, education, and public-service organizations

Learning Objectives

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

- Apply GDPR principles to operational processing decisions
- Build records of processing and accountability evidence
- Evaluate lawful bases, transparency, and retention controls
- Manage data-subject rights and processor obligations
- Analyze DPIA, transfer, and breach-response requirements
- Build a GDPR Operations and Evidence Pack

Course Agenda

Day 1: Establish GDPR Governance and Processing Records

- GDPR Scope and Responsibility Map
- Controller, Joint Controller, and Processor Decision Guide
- Personal Data and Processing Inventory
- Record of Processing Activities Template
- Accountability Roles and Evidence Register

Day 2: Control Lawful Processing and Transparency

- Processing Principle Assessment
- Lawful Basis Decision Record
- Special-Category Data Condition Check
- Privacy Notice Content and Timing Review
- Purpose Change and Data Minimization Test

Day 3: Manage Rights, Retention, and Processors

- Data Subject Rights Intake and Verification Workflow
- Search, Review, Redaction, and Response Log
- Retention and Secure Disposal Schedule
- Processor Due Diligence and Contract Checklist
- Subprocessor and International Transfer Register

Day 4: Assess Design, Risk, and Incidents

- Data Protection by Design Control Review
- DPIA Screening and Assessment Template
- Necessity, Proportionality, and Risk Analysis
- Personal Data Breach Triage Matrix
- Notification Decision and Incident Evidence Record

Day 5: Test GDPR Compliance and Accountability

- Operational Control Testing Plan
- Compliance Exception and Remediation Register
- Exercise: Build a Processing Accountability File
- Exercise: Coordinate a Rights Request and Breach
- Capstone: GDPR Operations and Evidence Pack

Practical Exercises

The course uses suggested activities based on customer, workforce, supplier, digital-service, and cross-border processing scenarios.

- Suggested activity: classify processing roles, document purposes and data flows, and complete a record of processing.
- Suggested activity: assess lawful bases, special-category conditions, notices, minimization, and retention controls.
- Suggested activity: screen a proposed process for a DPIA and record necessity, proportionality, risks, and measures.
- Suggested activity: coordinate a rights request and breach scenario, document decisions, and assemble assurance evidence.

FAQs

Who suits GDPR operational compliance training, and what does it assume?

Privacy, compliance, governance, process, legal operations, security, procurement, and vendor functions suit the training; it assumes practical familiarity with organizational processes that collect or use personal data.

How does operational GDPR compliance differ from legal advice?

Operational compliance turns defined requirements into roles, records, workflows, checks, and evidence. Legal advice interprets obligations for specific facts, jurisdictions, disputes, or regulatory decisions and remains outside the course.

What belongs in a record of processing activities?

A processing record should identify purposes, data and individual categories, recipients, transfers, retention, safeguards, accountable functions, systems, processors, and supporting decisions, with enough context for review and maintenance.

When should an organization conduct a DPIA?

An organization should screen new or changed processing and conduct a DPIA where it is likely to create high risk to individuals, documenting context, necessity, proportionality, risks, measures, consultation, approval, and review.

What evidence supports GDPR accountability?

Useful evidence includes inventories, processing records, lawful-basis decisions, notices, consent records, rights logs, retention schedules, processor reviews, transfer assessments, DPIAs, security controls, incident decisions, training records, tests, exceptions, and remediation.

Conclusion

Participants take back a GDPR Operations and Evidence Pack containing governance maps, processing records, decision logs, transparency reviews, rights workflows, retention schedules, processor checks, transfer registers, DPIAs, incident records, and control tests. It connects regulatory requirements to accountable operational work. The pack gives teams a repeatable structure for decisions, escalation, evidence, monitoring, and improvement.