JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Data Governance and Privacy with GDPR Training Course

16 – 27 August 2027
Milan

Advanced Data Governance and Privacy with GDPR Training Course

Ref: 221_6822 **Date:** 16 – 27 August 2027 **Location:** Milan **Fees:** 12400 GBP

Advanced Data Governance and Privacy with GDPR is a 2-week training course for data protection officers, data governance leads and compliance managers who build a GDPR privacy control framework linking data ownership, records of processing, impact assessments and breach playbooks to the data protection principles. Customers, partners and supervisory authorities now expect organisations to prove, not merely claim, that personal information is handled lawfully. The course is delivered by Jupiter Prime Training.

Why Data Governance and Privacy with GDPR Matter Now

Three groups shape this field today. Data subjects exercise access, erasure and objection rights more often and through more channels; business units adopt cloud, marketing and analytics services that move personal information across borders and processors; and supervisory authorities expect documented accountability rather than policies on paper. An organisation that ties privacy duties to named data owners answers requests and incidents calmly, while one that does not faces complaints, enforcement and lost trust. The course rests on the General Data Protection Regulation GDPR and on the Data Management Body of Knowledge DAMA-DMBOK for stewardship roles.

Who Gains Most from Data Governance and Privacy with GDPR

- Privacy officers accountable for records of processing, impact assessments and supervisory authority contact
- Governance leads who assign data owners, stewards and custodians across business domains
- Assurance specialists who test privacy controls and report gaps to audit committees
- Information security leads who coordinate breach detection, containment and notification
- Procurement and legal partners who negotiate processor and data-sharing terms

A privacy office working alongside a data governance council gains most when several members attend together and agree one control set across legal, security and data teams.

Data Governance and Privacy with GDPR Capabilities

Participants move from interpreting articles in isolation to running a privacy control environment in which every processing activity has an owner, a purpose and evidence.

- Design a stewardship model that assigns privacy duties to data owners — the governance council approving accountability
- Build a record of processing activities linked to systems and retention — the privacy officer answering authority requests
- Assess lawful basis and legitimate interests for new processing — product and marketing sponsors launching initiatives
- Apply data protection impact assessments to high-risk processing — project boards deciding go or redesign
- Test breach detection, triage and notification procedures — incident managers and executives under time pressure
- Specify processor contracts and transfer safeguards — procurement and legal teams onboarding suppliers

Key Data Governance and Privacy with GDPR Terms

- Controller — the organisation that decides why and how personal data is processed and carries primary accountability for that processing.
- Processor — an organisation that handles personal data on behalf of a controller and only on its documented instructions.
- Lawful basis — one of the grounds GDPR recognises, such as contract or legitimate interests, that must exist before personal data is processed.
- Record of processing activities — the documented inventory of processing operations, their purposes, categories of data, recipients and retention periods.
- Data protection impact assessment — a structured evaluation of a high-risk processing activity that identifies privacy risks and the measures to reduce them.
- Data steward — a person responsible for the definition, quality and appropriate use of a data domain on behalf of its owner.

Data Governance and Privacy with GDPR Day by Day

Day 1: Privacy Accountability and Its Stakeholders

- GDPR Principles Map — Linking Lawfulness, Minimisation and Accountability to Daily Operations
- Supervisory Authority Expectations — Preparing Evidence Before an Inquiry Arrives
- Privacy Maturity Baseline — Scoring Current Controls Across Business Units
- Data Subject Journey Mapping — Seeing Processing Through Customer and Employee Eyes
- Board Reporting Template — Framing Privacy Exposure for Directors

Day 2: Stewardship Structures for Personal Data

- DAMA-DMBOK Stewardship Roles — Separating Owners, Stewards and Custodians
- Domain-Based Ownership Model — Assigning Customer, HR and Supplier Data
- Governance Council Charter — Setting Decision Rights and Escalation Paths
- RACI for Privacy Duties — Clarifying Who Approves New Processing
- Policy Hierarchy — Aligning Privacy Policy, Standards and Procedures

Day 3: Knowing What Personal Data Exists

- Data Discovery and Classification Scans — Locating Personal and Special Category Data
- Record of Processing Activities Build — Documenting Purposes, Recipients and Retention
- Data Flow Diagrams — Tracing Personal Data Through Systems and Suppliers
- Business Glossary and Lineage Links — Connecting Privacy Records to Data Catalogues
- Retention and Minimisation Rules — Removing Data No Longer Needed

Day 4: Lawful Processing Decisions

- Lawful Basis Selection Matrix — Matching Contract, Obligation and Legitimate Interests
- Legitimate Interests Assessment — Balancing Organisational Benefit Against Individual Impact
- Consent Capture and Withdrawal Design — Making Choices Specific and Reversible
- Privacy Notice Layering — Explaining Processing in Plain Language
- Purpose Compatibility Test — Judging Reuse of Data for Analytics

Day 5: Rights of Individuals in Practice

- Access Request Workflow — Locating, Redacting and Releasing Personal Data on Time
- Erasure and Rectification Handling — Propagating Changes Across Linked Systems
- Objection and Restriction Procedures — Pausing Marketing and Profiling Activities
- Data Portability Formats — Providing Machine-Readable Copies
- Rights Request Metrics — Monitoring Volumes, Timeliness and Complaints

Day 6: Impact Assessment and Privacy by Design

- DPIA Screening Criteria — Deciding Which Projects Need a Full Assessment
- DPIA Risk Scoring Method — Rating Likelihood and Severity for Individuals
- Privacy by Design Patterns — Pseudonymisation, Aggregation and Access Minimisation
- Prior Consultation Triggers — Recognising When Residual Risk Stays High
- DPIA Sign-Off Workflow — Recording Owner Decisions and Review Dates

Day 7: Processors, Sharing and Transfers

- Processor Due Diligence Questionnaire — Vetting Cloud and Outsourcing Suppliers
- Data Processing Agreement Clauses — Securing Instructions, Audit and Sub-Processing Terms
- Joint Controller Arrangements — Allocating Duties Between Partner Organisations
- International Transfer Safeguards — Choosing Contractual and Supplementary Measures
- Data Sharing Agreements — Governing Exchanges With Public and Commercial Partners

Day 8: Breach Readiness and Response

- Personal Data Breach Classification — Separating Confidentiality, Integrity and Availability Events
- Breach Triage and Risk Assessment — Deciding Whether Authorities and Individuals Are Told
- Notification Content and Timelines — Preparing Statements Within the Required Window
- Breach Register and Lessons Log — Evidencing Every Incident and Remedy
- Tabletop Simulation — Rehearsing Ransomware and Misdirected Email Scenarios

Day 9: Assurance, Metrics and Continuous Control

- Privacy Control Library — Mapping Controls to Each GDPR Principle
- Control Testing Procedures — Sampling Evidence for Internal Audit
- Privacy Key Risk Indicators — Tracking Requests, Breaches and Overdue Assessments
- Awareness and Role-Based Training Plans — Targeting High-Risk Functions
- Accountability Evidence Pack — Organising Documents for Authority Review

Day 10: Practising the GDPR Privacy Control Framework

- Retail Loyalty Case — Applying Lawful Basis and Rights Workflows to Customer Data
- Hospital Records Case — Applying DPIA and Special Category Safeguards
- Supplier Onboarding Case — Applying Processor Clauses and Transfer Safeguards
- Peer Challenge Panel — Testing Ownership, Metrics and Escalation Choices
- GDPR Privacy Control Framework — Completing Owners, Controls and Evidence Map

Applying Data Governance and Privacy with GDPR After the Course

- Refresh the record of processing activities for one business domain with its data owner and close any gaps in purpose, retention or recipients.
- Run a breach tabletop simulation with security, legal and communications leads and update the notification procedure from its findings.

Data Governance and Privacy with GDPR Questions FAQ

What is advanced data governance and privacy with GDPR, and why does it matter now?

It is the practice of assigning ownership of personal data and running documented controls that meet the General Data Protection Regulation. It matters now because individuals use their rights more often and authorities expect evidence of accountability, not just written policies.

Which roles gain most from data governance and privacy with GDPR training?

Privacy officers, data governance leads and compliance managers gain most. You benefit if you maintain processing records, run impact assessments, negotiate processor terms or coordinate breach response in sectors such as retail, healthcare, financial services or public administration.

How does a data governance and privacy with GDPR course differ from an AI data governance course?

It covers every processing activity across the organisation rather than datasets used to train models. An AI-focused course centres on training data provenance and bias, while this subject centres on stewardship, individual rights, processors, transfers and breach handling.

What do you bring back from data governance and privacy with GDPR training?

You bring back a control map that links each GDPR principle to owners, procedures, metrics and evidence, together with worked retail, hospital and supplier cases your colleagues can reuse.

Data Governance and Privacy with GDPR: The Way Forward

The GDPR privacy control framework first informs which business domains need refreshed processing records and impact assessments before the next audit or product launch. Privacy officers, data owners and internal auditors use it to agree responsibilities and evidence. After its first cycle, revisit the key risk indicators, because real request and breach patterns show which controls deserve more attention.