JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Data Protection Compliance Operations Training Course

31 January – 4 February 2027
Muscat

Data Protection Compliance Operations Training Course

Ref: 2965_112429 **Date:** 31 January – 4 February 2027 **Location:** Muscat **Fees:** 6500 GBP

Data Protection Compliance Operations is a 1-week training course for compliance officers, privacy leads and data owners who run daily personal information controls, ending with a data protection compliance plan. Organisations now collect personal details through more channels and suppliers than their controls were built for, so lawful handling has become an operating discipline. Jupiter Prime Training offers this course to strengthen Data Protection Compliance Operations.

Why Data Protection Compliance Operations Matters Now

Three pressures shape this work today. Individuals exercise their rights more often, testing how quickly an organisation can locate, correct or erase what it holds. Outsourcing to cloud hosts and payroll bureaux spreads personal information across contracts. Supervisory authorities expect evidence: a written lawful basis, a current inventory and a tested incident routine. Handled well, these earn trust; handled badly, they bring enforcement and reputational harm.

Who Gains Most from Data Protection Compliance Operations

- Those who keep the inventory of processing current
- Those who receive, verify and answer requests from individuals about their own information
- Those who own a business system or customer database and decide access
- Those who coordinate the response when personal information is lost or exposed

A privacy office that sends its compliance lead together with two or three system owners gains most, because lawful basis decisions and technical controls are then agreed by the people who apply them.

Data Protection Compliance Operations Capabilities

Participants turn legal principles into routines that a records owner or helpdesk agent can follow and evidence.

- Assess each processing activity against a documented lawful basis — the decision to continue, change or stop it
- Build an inventory of processing that links purposes, categories, recipients and retention — internal auditors and the supervisory authority
- Apply a structured impact assessment to new or changed processing — project sponsors approving launch
- Design a request-handling routine with identity checks and response timelines — individuals exercising their rights
- Test an incident playbook from detection to notification — senior leaders deciding whether to report
-

Specify contract clauses and assurance checks for outsourced processing — procurement and supplier owners

Key Data Protection Compliance Operations Terms

- Lawful basis — the recognised legal ground, such as consent or contract, that permits a specific use of personal information.
- Controller — the organisation that decides why and how personal information is used and carries primary accountability for it.
- Processor — a separate organisation that handles personal information only on the documented instructions of a controller.
- Inventory of processing — a maintained record of each activity, its purpose, data categories, recipients and retention period.
- Impact assessment — a structured review of a high-risk activity identifying harms to individuals and measures that reduce them.
- Personal data breach — a security incident leading to accidental or unlawful loss, alteration, disclosure of or access to personal information.

Data Protection Compliance Operations Day by Day

Day 1: Principles and Accountability

- Core Processing Principles — Setting the Tests Every Activity Must Pass
- Controller and Processor Roles — Allocating Accountability Across Partners
- Lawful Basis Selection Matrix — Choosing Consent, Contract or Legitimate Interest
- Legitimate Interest Balancing Test — Weighing Business Need Against Individual Expectations
- Accountability Evidence Map — Deciding What Proof the Organisation Must Hold

Day 2: Mapping Personal Information

- Data Flow Discovery Interviews — Revealing Hidden Collection Points and Recipients
- Inventory of Processing Template — Recording Purposes, Categories and Retention Periods
- Special Category Information Register — Applying Stricter Conditions to Sensitive Details
- Retention Schedule Design — Deciding When Records Are Deleted or Anonymised
- Cross-Border Transfer Checklist — Approving Safeguards Before Information Leaves

Day 3: Assessing Risk to Individuals

- Impact Assessment Screening Questions — Deciding Which Projects Need a Full Review
- Harm Likelihood and Severity Scale — Ranking Risks to Rights and Freedoms
- Privacy by Design Requirements — Building Minimisation Into New Systems
- Supplier Due Diligence Questionnaire — Approving Processors Before Contract Signature
- Processing Agreement Clause Review — Securing Instructions, Audit Rights and Deletion

Day 4: Rights Requests and Incidents

- Subject Access Request Workflow — Verifying Identity and Meeting Response Deadlines
- Erasure and Rectification Decisions — Handling Exemptions and Competing Obligations
- Objection and Marketing Opt-Out Handling — Stopping Processing Across Every Channel
- Breach Triage and Containment Steps — Limiting Exposure in the First Hours
- Notification Decision Record — Documenting Whether Authorities and Individuals Are Told

Day 5: Practising the Data Protection Compliance Plan

- Lawful Basis Review of a Sample Activity — Applying Day One Tests to Live Cases
- Inventory Gap Analysis — Comparing Mapped Flows With Recorded Entries
- Breach Tabletop Simulation — Rehearsing Triage, Containment and Notification Choices
- Compliance Metrics and Reporting Cadence — Showing Leaders Request and Incident Trends
- Data Protection Compliance Plan — Sequencing Remediation Actions, Owners and Review Points

Applying Data Protection Compliance Operations After the Course

- Run data flow discovery interviews with two business units and close the gaps they reveal in the inventory of processing.
- Hold a breach tabletop simulation with system owners and update the notification decision record from what it exposes.

Data Protection Compliance Operations Questions FAQ

What is Data Protection Compliance Operations and why does it matter now?

It is the daily work of applying data protection rules to real systems, suppliers and requests. It matters now because authorities expect written evidence that every use of personal information is lawful.

Which roles gain most from Data Protection Compliance Operations training?

Compliance officers, privacy leads and data owners gain most. Anyone who answers rights requests, approves suppliers or coordinates incident response uses the routines directly.

How does Data Protection Compliance Operations differ from a data governance course?

This course concentrates on the operational duties owed to individuals: lawful basis, impact assessments, rights requests and breaches. A data governance course looks more broadly at quality and stewardship of all information.

What do you bring back from Data Protection Compliance Operations training?

You bring back a drafted compliance plan, an inventory template, an impact assessment screening tool and a notification decision record, each adapted to an activity from your own organisation.

Data Protection Compliance Operations: The Way Forward

The data protection compliance plan gives the privacy office sequenced remediation actions with named owners. Its first use is deciding which activities need an impact assessment or a revised lawful basis. System owners and senior leaders use it to track progress, and it is worth revisiting after the first real breach it faces.