Hospitality Guest Data Protection and Privacy Controls Training Course

2 – 6 August 2027
Addis Ababa

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Hospitality Guest Data Protection and Privacy Controls Training Course

Ref: 818_224034 **Date:** 2 – 6 August 2027 **Location:** Addis Ababa **Fees:** 4500 Euro

Overview

Hospitality Guest Data Protection and Privacy Controls Training Course is a one-week intermediate course for hospitality managers, operations leaders, guest services teams, privacy coordinators, compliance staff, and IT governance professionals who leave with a Hospitality Privacy Controls Pack. Participants map guest and workforce data, assess processing risks, define controls for reservations, loyalty, payments, CCTV, marketing, vendors, retention, rights, and incidents, and test evidence through realistic hotel scenarios. Agile Leaders Training Center develops practical hospitality data protection capability.

Who Should Attend

- Hotel operations functions responsible for guest journeys, reservations, stays, and service records
- Guest services functions responsible for profiles, preferences, requests, complaints, and identity checks
- Privacy and compliance functions responsible for requirements, records, rights, and assurance
- Information technology governance functions responsible for access, systems, logs, integrations, and suppliers
- Marketing and loyalty functions responsible for permissions, preferences, segmentation, and communications
- Human resources and security functions responsible for workforce, CCTV, and access-control records

The course assumes participants already handle hospitality information or control processes at work, and leaves out legal representation, penetration testing, system administration, and payment-card certification.

Departments and Industries

The course supports departments and industries that process guest, visitor, workforce, payment, preference, and service information.

- Hotel operations, front office, reservations, guest relations, and revenue operations
- Privacy, compliance, risk, audit, legal operations, and information governance
- Marketing, loyalty, events, food and beverage, spa, and concierge services
- Information technology, cybersecurity coordination, procurement, and vendor management
- Hotels, resorts, serviced residences, restaurants, venues, and travel services

Learning Objectives

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

- Map hospitality data flows and assign accountable owners
- Assess privacy risks across guest and workforce journeys
- Design operational controls for collection, access, sharing, retention, and disposal
- Manage consent, preferences, rights requests, and privacy notices
- Coordinate vendor assurance and privacy incident response
- Build a Hospitality Privacy Controls Pack

Course Agenda

Day 1: Map Hospitality Data and Responsibilities

- Guest and Workforce Data Inventory
- Reservation, Stay, Loyalty, and Service Data Flow Map
- Processing Purpose and Responsibility Matrix
- Data Classification and Sensitivity Guide
- Hospitality Privacy Risk Register

Day 2: Control Guest Data Across Operations

- Reservation and Check-In Data Collection Checklist
- Guest Profile and Preference Handling Rules
- Payment Handoff and Restricted Data Boundary
- Room, Service, Complaint, and Special-Request Records
- Access Approval and Activity Review

Day 3: Manage Monitoring, Marketing, and Retention

- CCTV and Access-Record Privacy Assessment
- Marketing Consent and Preference Register
- Loyalty Data Use and Sharing Decision Table
- Retention Schedule and Disposal Evidence
- Privacy Notice and Frontline Communication Review

Day 4: Govern Vendors, Rights, and Incidents

- Hospitality Vendor Privacy Due Diligence
- Data-Sharing and Processor Control Checklist
- Data Subject Rights Request Workflow
- Privacy Incident Triage and Escalation Matrix
- Notification Decision and Response Record

Day 5: Test and Improve Hospitality Privacy Controls

- Control Evidence and Assurance Checklist
- Privacy Metrics and Exception Dashboard
- Exercise: Trace a Guest Data Journey
- Exercise: Coordinate a Hotel Privacy Incident
- Capstone: Hospitality Privacy Controls Pack

Practical Exercises

The course uses suggested activities based on hotel reservations, guest services, loyalty, marketing, monitoring, workforce, and supplier scenarios.

- Suggested activity: map a reservation-to-checkout data journey, identify owners, and record high-risk handoffs.
- Suggested activity: review guest profile fields, access permissions, preferences, and retention decisions.
- Suggested activity: assess a CCTV or access-record use case and define proportionate operational controls.
- Suggested activity: triage a vendor-related privacy incident, assign actions, and prepare assurance evidence.

FAQs

Who suits hospitality guest data protection training, and what does it assume?

Managers and functions responsible for hospitality information, operations, privacy, compliance, technology governance, marketing, loyalty, security, or suppliers suit the training; it assumes practical familiarity with routine hotel processes.

What information belongs in a hospitality data flow map?

A hospitality data flow map should record data categories, individuals, collection points, purposes, systems, users, transfers, service providers, storage locations, retention points, disposal actions, and accountable owners.

How should hotels control guest profiles and preferences?

Hotels should define necessary fields, valid purposes, access roles, update processes, sharing boundaries, retention periods, deletion rules, and evidence for sensitive requests and marketing preferences.

How does hospitality vendor privacy due diligence work?

Hospitality vendor privacy due diligence examines processing purposes, data access, security and privacy controls, locations, subcontractors, incident duties, retention, deletion, rights support, contractual terms, and assurance evidence.

What should a hotel privacy incident workflow include?

A hotel privacy incident workflow should include reporting, containment, evidence preservation, risk assessment, decision authority, legal and contractual escalation, communication, corrective action, closure, and lessons learned.

Conclusion

Participants take back a Hospitality Privacy Controls Pack containing a data inventory, flow map, responsibility matrix, risk register, collection and access checks, preference register, retention schedule, vendor review, rights workflow, incident records, and assurance dashboard. It connects guest trust with practical operating controls across hospitality services. The pack gives teams a repeatable basis for decisions, evidence, escalation, and improvement.