



Product Privacy and Consumer Data Protection Training Course

24 – 28 May 2027
Kuala Lumpur

Product Privacy and Consumer Data Protection Training Course

Ref: 801_160837 **Date:** 24 – 28 May 2027 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Overview

Product Privacy and Consumer Data Protection Training Course is a five-day professional course for product managers, product owners, digital service leaders, designers, privacy, legal, and compliance functions who leave with a Product Privacy Decision and Evidence Pack. Participants connect product discovery, purposes, data inventories, transparency, consent, rights, minimization, vendors, analytics, retention, security, release gates, and incident readiness. The course addresses privacy decisions made too late or without evidence. Agile Leaders Training Center develops product privacy and consumer data protection.

Who Should Attend

- Product management functions responsible for strategy, requirements, prioritization, launch, and lifecycle decisions
- Product ownership functions responsible for backlog choices, acceptance criteria, and delivery evidence
- Design and research functions responsible for user journeys, notices, choices, testing, and accessibility
- Privacy and legal functions responsible for advising on processing purposes, rights, contracts, and risk
- Compliance functions responsible for controls, reviews, records, monitoring, and assurance
- Engineering and security functions responsible for technical safeguards, access, logging, and incident coordination

The course assumes participants can describe a digital product, its users, data flows, vendors, and release process, and leaves out introductory product management, legal representation, advanced security engineering, and external certification preparation.

Departments and Industries

The course supports departments and industries that design or operate consumer-facing products and services using personal data.

- Product, design, research, engineering, security, privacy, and legal teams
- Retail commerce, loyalty, delivery, and customer-service products
- Banking payment, account, credit, and digital-service journeys
- Healthcare appointment, patient portal, remote care, and wellness products
- Telecommunications account, device, location, and service applications
- Public-service identity, application, eligibility, and case-management services

Learning Objectives

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

- Analyze product data flows, purposes, user expectations, and privacy risks
- Apply data minimization, transparency, consent, and rights requirements
- Build privacy acceptance criteria and product review gates
- Evaluate analytics, vendor, sharing, retention, and security decisions
- Design rights-handling and incident-coordination workflows
- Build traceable product privacy decisions and release evidence

Course Agenda

Day 1: Frame Product Privacy Decisions

- Product Lifecycle and Privacy Decision Map
- User, Data Subject, Controller, and Processor Role Map
- Product Data Inventory and Flow Diagram
- Purpose, Necessity, and Legal-Basis Decision Record
- Privacy Risk, Harm, Owner, and Escalation Register

Day 2: Design Transparent Data Journeys

- Notice Layer, Timing, Context, and Language Checklist
- Consent Request, Choice, Withdrawal, and Evidence Flow
- Data Minimization and Default Setting Review
- Access, Copy, Correction, and Destruction Request Journey
- Research Participant and Test Data Protection Plan

Day 3: Govern Product Data Use

- Analytics Purpose, Event, Attribute, and Access Matrix
- Vendor Due Diligence and Processing Instruction Checklist
- Data Sharing, Interface, and Transfer Decision Log
- Retention Trigger, Period, Archive, and Destruction Rule Set
- Security Safeguard, Access, Logging, and Test Requirement Map

Day 4: Control Release and Post-Launch Privacy

- Product Requirement and Privacy Acceptance Criteria
- Design Review, Development Review, and Release Privacy Gate
- Change Assessment and Feature Reappraisal Method
- Monitoring, Complaint, Rights, and Fix Triage Dashboard
- Privacy Incident Coordination and Evidence Checklist



Day 5: Practice Product Privacy Delivery

- Exercise: Map a Feature's Data Flow and Purpose
- Exercise: Repair Notice, Consent, and Default Choices
- Exercise: Assess an Analytics Vendor and Retention Rule
- Exercise: Run a Release Gate and Incident Coordination Review
- Capstone: Product Privacy Decision and Evidence Pack

Practical Exercises

The course uses suggested activities based on retail, banking, healthcare, telecommunications, and public-service product scenarios.

- Suggested activity: map feature data, record purposes and roles, identify risks, and assign decision owners.
- Suggested activity: redesign a notice and consent journey, reduce unnecessary collection, and specify rights-handling paths.
- Suggested activity: assess analytics events, vendor instructions, sharing, retention, access, logging, and safeguards.
- Suggested activity: conduct a release privacy gate, document unresolved issues, and rehearse product-security-privacy incident coordination.

FAQs

Who suits product privacy training, and what does it assume?

Product managers, owners, digital service leaders, designers, privacy, legal, compliance, engineering, and security functions suit the course; it assumes they can describe a product, its users, data flows, vendors, and release process.

How does product privacy training differ from a general data protection law course?

Product privacy training translates requirements into discovery, design, backlog, acceptance, vendor, analytics, release, monitoring, and evidence decisions, while a general law course concentrates on legal concepts, organizational duties, rights, and interpretation across business activities.

When should product teams review consumer data protection?

Product teams should review data protection at discovery, research, design, development, testing, procurement, analytics configuration, release, feature change, vendor change, complaint or rights trends, security events, and decommissioning, with the depth proportionate to processing and risk.



What evidence supports a product privacy decision?

Product privacy evidence includes inventories, flow maps, purpose records, requirement decisions, notices, consent logs, minimization reviews, rights workflows, vendor assessments, retention rules, safeguard tests, approvals, release checks, monitoring results, issue decisions, and incident records.

How can product teams avoid dark patterns in privacy choices?

Product teams avoid dark patterns by presenting balanced options, plain language, relevant timing, equal effort for acceptance and refusal, specific purposes, uncluttered controls, reversible choices, accessible design, no misleading emphasis, and tests showing that users can identify and exercise their choices.

Conclusion

Participants take back a Product Privacy Decision and Evidence Pack containing data maps, purpose records, notice and consent journeys, minimization reviews, rights workflows, vendor and analytics assessments, retention rules, safeguard requirements, release gates, monitoring, and incident evidence. It changes late privacy review into lifecycle product decisions. The pack keeps users, data, purposes, controls, owners, and evidence connected.