Module Architecture Blueprint

Foundations of Data Privacy in Professional Settings

Target Audience

Early- to mid-career professionals working with client, employee, or consumer data in corporate environments.

Module Overview

Introduces core data privacy principles and a structured decision framework for responsible data handling.

Learning Outcomes

1. Define personal data and sensitive data within a professional context.
2. Distinguish between data privacy and data security.
3. Identify common risk points in routine data handling workflows.
4. Apply a four-step decision framework before collecting, storing, or sharing data.

Instructional Sequence

1. Context & Risk Landscape (5–7 minutes)

- Why failures occur
- Business and legal consequences
- Regulatory overview (GDPR, CCPA)

2. Core Concepts & Definitions (8–10 minutes)

- Personal vs. sensitive data
- Data minimization
- Lawful basis for processing
- Consent vs. legitimate interest
- Privacy vs. security distinctions

3. Operational Risk Points (8–10 minutes)

- Email and file-sharing risks
- Cloud storage and third-party tools
- Access permissions and role-based exposure
- Informal data capture (spreadsheets, notes, exports)

4. Decision Framework: Before You Act (8–10 minutes)o I need this data?

1. Do I need this data?
2. Do I have a lawful basis?
3. Is access limited appropriately?
4. Is retention defined?

5. Applied Scenario (5–7 minutes)

Marketing team requests expanded customer dataset for campaign analysis. Learners identify risks, apply the framework, and receive feedback tied directly to stated outcomes.

Reinforcement Strategy

- Knowledge checks embedded after core concepts and framework sections
- Scenario requires applied judgment, not recall
- Immediate feedback referencing regulatory principles
- Clear transition to next module: Data Retention & Incident Response

Assessment Structure

- 5 objective questions (concept clarity)
- 1 scenario-based application question
- Passing threshold: 80%
- Rationale provided for each answer