Regulatory Requirements Summary (Example)

Purpose: Provide a concise, PM-friendly summary of commonly referenced obligations for a customer onboarding process that handles personal data and identity documents. This is not legal advice; it is a structured interpretation aid for requirement traceability.

Scope

Process: Customer onboarding (form submission, document upload, KYC check, approval, account creation). Data types: PII, ID document images, audit logs, risk scores.

Key GDPR Articles used in this use case

Reference	Theme	Obligation (PM wording)	Typical Evidence
GDPR Art. 5	Principles	Process data lawfully, minimize data, keep accurate, limit storage, ensure integrity and confidentiality.	Retention policy, minimization rationale, security controls.
GDPR Art. 25	Privacy by design	Build controls into the system by default (least privilege, secure defaults).	Architecture decision record, default settings, access model.
GDPR Art. 30	Records of processing	Maintain records of processing activities for onboarding workflows.	RoPA entry, system inventory, data flow map.
GDPR Art. 32	Security	Ensure appropriate security of processing (confidentiality, integrity, availability; testing).	Access logs, encryption evidence, pen test report, backup/restore test.

Operational Interpretation Notes (example)

- Identity documents are high sensitivity personal data. Limit access to trained roles; log access.
- Risk scoring must be explainable to internal reviewers; keep a minimal audit trail of inputs and decisions.
- Retention should be defined per regulatory and business need; delete/anonymize after retention expires.
- Third-party KYC provider requires vendor security and data processing terms (controller/processor roles).

RAG Indexing Hints (metadata fields)

Suggested metadata: document_type=regulation_summary; jurisdiction=EU; domain=privacy; articles=[5,25,30,32]; process=Customer Onboarding; data_types=[PII, ID_DOCS, LOGS].