Legal Memo (Sample) - Data Processing in Customer Onboarding

Document type: Internal legal/compliance interpretation memo (template). **Not legal advice.**

1. Background

The Company plans to modernize the legacy onboarding process. The process collects personal data and identity documents, runs KYC checks via a third-party provider, and creates accounts in the core platform.

2. Legal basis and scope (example structure)

2.1 Legal basis for processing

- Identify the lawful basis (e.g., contract necessity, legal obligation, legitimate interests).

- For identity verification, legal obligation may apply depending on sector rules.

2.2 Data categories

- PII: name, address, date of birth, contact details.

- Identity documents: document number, photo, issuing authority (high sensitivity).

- Operational data: risk scores, decision reasons, audit logs.

3. Mandatory controls (requirements implications)

The following controls should be treated as mandatory for the onboarding modernization scope:

- Role-based access control for ID documents and risk review screens.
- Audit logging for access to identity documents and risk decisions (who/when/what).
- Retention rules for identity documents and logs, including deletion/anonymization after expiry.
- Third-party KYC: data processing terms, security requirements, and transfer assessment if applicable.

4. Open questions for Product and Engineering

These questions must be resolved before finalizing requirements:

- Which user roles will access ID documents (support, compliance, onboarding ops)?
- What is the target retention period for ID documents and logs, and why?
- Do any steps require manual review for high-risk cases, and what triggers it?
- How will we evidence control effectiveness for audit (reports, logs, screenshots)?

5. References

EU GDPR: Articles 5, 25, 30, 32 (security and accountability themes).

Internal policies: Access Control Policy, Data Retention Policy, Vendor Risk Policy (if applicable).