**Data Privacy and Encryption**

**1. Data Privacy Implementation**

Ensuring **data privacy** means applying technical controls that limit exposure of personal and sensitive information while enabling business operations and analytics.

**Anonymization Techniques**

| **Technique** | **Description** | **Use Case** |
| --- | --- | --- |
| **Tokenization** | Replaces sensitive identifiers (e.g., credit card numbers, SSNs) with randomly generated tokens that have no exploitable meaning. | Used in payment processing, identity protection. |
| **Pseudonymization** | Replaces personal identifiers (names, emails) with fake but consistent values to allow analysis without identifying individuals. | For internal analytics with reduced compliance burden. |
| **Differential Privacy** | Introduces statistical noise into datasets, preserving aggregate insights while protecting individual records. | For large-scale analytics and AI model training. |
| **Dynamic Data Masking** | Masks data in real-time based on user role or context (e.g., showing only last 4 digits of SSN). | Used in dashboards, customer service interfaces. |

**2. Encryption Strategies**

Encryption ensures data confidentiality by transforming readable information into an unreadable format, only accessible with the correct decryption keys.

**Data at Rest**

* **AES-256 Encryption**
  + Industry-standard symmetric encryption used for securing databases, file systems, and backups.
  + Managed through enterprise Key Management Services (KMS).
* **Column-Level Encryption**
  + Sensitive fields like passwords, account numbers, or medical data are encrypted individually in the database.
  + Allows selective access control at the field level.
* **Full Disk Encryption (FDE)**
  + Encrypts entire physical storage devices (servers, laptops, drives) to protect data even if hardware is stolen.
  + Common tools: BitLocker, LUKS.

**Data in Transit**

* **TLS 1.3 Encryption**
  + Secures all communications over HTTPS, APIs, and internal services.
  + Reduces handshake time and enhances performance.
* **Secure VPN Access**
  + Remote employees and partners access systems through encrypted tunnels, shielding data from interception.
* **End-to-End Encryption (E2EE)**
  + Applied to digital banking platforms, mobile apps, and messaging systems.
  + Ensures that only sender and receiver can decrypt the message, not even the service provider.