**Data Privacy and Encryption Implementation Plan**

**1. Data Privacy Measures**

**Anonymization Techniques**

To protect personally identifiable information (PII) and sensitive data, the following anonymization methods will be applied:

* **Tokenization**
  + Replace sensitive identifiers (e.g., credit card numbers, SSNs) with non-reversible tokens.
  + Used in payment processing and database storage.
* **Pseudonymization**
  + Replace direct identifiers (e.g., names, emails) with aliases to prevent direct identification.
  + Reversible only with a secure key management system.
* **Differential Privacy**
  + Add controlled noise to datasets used for analytics to prevent re-identification.
  + Applied in statistical reporting and machine learning models.
* **Dynamic Data Masking**
  + Real-time masking of sensitive data (e.g., showing only the last 4 digits of a credit card).
  + Role-based access ensures only authorized users see full data.

**2. Encryption Strategies**

**A. Data at Rest Encryption**

Protecting stored data from unauthorized access:

* **AES-256 Encryption**
  + Industry-standard symmetric encryption for databases, files, and backups.
  + Used for full-disk encryption (FDE) on servers and endpoints.
* **Column-Level Encryption**
  + Sensitive fields (e.g., passwords, financial data) encrypted individually.
  + Decrypted only when accessed by authorized applications/users.
* **Full Disk Encryption (FDE)**
  + BitLocker (Windows), FileVault (macOS), or LUKS (Linux) for all company devices.

**B. Data in Transit Encryption**

Securing data during transmission:

* **TLS 1.3 Encryption**
  + Mandatory for all web traffic (HTTPS), APIs, and internal communications.
  + Perfect Forward Secrecy (PFS) ensures session keys are not reused.
* **Secure VPN for Remote Access**
  + IPsec or WireGuard VPNs for employees accessing internal systems.
  + Multi-factor authentication (MFA) required for VPN login.

**C. End-to-End Encryption (E2EE)**

* **Digital Banking & Messaging**
  + Messages, transactions, and files encrypted on the sender’s device and decrypted only by the recipient.
  + Uses **AES-256 + RSA-4096** for key exchange (e.g., Signal Protocol).

**3. Key Management & Access Control**

* **Hardware Security Modules (HSMs)** for secure encryption key storage.
* **Role-Based Access Control (RBAC)** to limit decryption privileges.
* **Automated Key Rotation** every 90 days for compliance (GDPR, HIPAA, PCI-DSS).

# 4. Compliance & Auditing

* Regular **penetration testing** and **vulnerability scans**.
* **Audit logs** for all encryption/decryption activities.
* Compliance with **GDPR, CCPA, HIPAA, and PCI-DSS** regulation