CryptoBind®
By JISA Softech

CryptoBind's 5-Step Compliance Framework

A quick visual guide for organisations

1. Data Inventory & Classification

- Map all personal data you collect, store, process, and share
- Identify sensitive & high-risk data
- Define clear data retention timelines

2. Consent Governance

- Ensure consent is free, specific, informed, unambiguous & revocable
- Provide clear notices in simple language
- Enable easy opt-out & withdrawal

3. Rights of Data Principals

- Implement mechanisms for:
- Data access
- Data correction/updates
- Data erasure
- Grievance redressal within defined timelines

4. Security & Technical Controls

- Strong security controls required under DPDP for safeguarding personal data.

5. Governance, Record-Keeping & Accountability

- Appoint key roles (e.g., Data Protection Officer if applicable)
- Maintain processing logs & purpose documentation
- Ensure regular compliance reviews and DPIAs

DPDP Compliance Requirement	What the Law Expects	CryptoBind Solutions
Data Inventory & Classification	Maintain accurate records of personal data, sensitive data, Aadhaar data, and its purpose	• Data Discovery & Classification Engine
		• Aadhaar Data Vault
		• Data Masking
Purpose Limitation & Consent Management	Collect and process data only for clear, lawful purposes with revocable consent	• Data Privacy Vault
		• Application-Level Encryption
		• HSM Backed Policy-based access control
Data Minimisation & Access Controls	Ensure least privilege access; avoid unnecessary data collection	• Tokenisation (Vault & Vaultless)
		• Data Security Server
		• CryptoBinds Quantum-Ready HSM
Processing of Personal Data (Lawful Use)	Process only what is required and ensure data is protected throughout	• CryptoBinds Quantum-Ready HSM
		• Encryption (At Rest + In Transit)
		• Enterprise Key Management
Rights of Data Principals	Provide mechanisms for access, correction, erasure & grievance redressal	• Tokenisation for reversible updates
		• Quantum-Ready HSM and KMS
		• Data Security Server
Security Safeguards	Implement strong technical and organisational security controls	• Hardware Security Module (HSM)
		• Encryption Key Control & Protection
		• Database Encryption

DPDP Compliance Requirement	What the Law Expects	CryptoBind Solutions
Anonymisation & Pseudonymisation	Protect identity data for analytics while ensuring reversibility only when lawful	• SecureToken Vaultless tokenization
		• SecureVault
		• PII Data Vault
8. Data Storage Limitation	Retain data only as long as needed for legal/business purpose	• Enterprise Key Management
		• SecureVault and TDE
Data Breach Prevention & Monitoring	Real-time monitoring, detection & auditing of sensitive data access	• Data privacy Platform
Accountability & Governance	Appoint responsible roles, maintain records, ensure regular audits	• Security & Privacy Governance Dashboard
		• Audit Trail Engine
Secure Cross-Border Data Transfer	Ensure security, compliance, and contractual safeguards for international data flows	• Encryption + Tokenisation for outbound flows
		• HSM-backed Key Protection
		• Data Privacy Vault
Children's Data Obligations	Enhanced protection for minors' data and parental consent	• CryptoBinds Quantum-Ready HSM
		• Data discovery and classification
Data Fiduciary & Processor Obligations	Strong contracts, secure processing environment, risk assessments	• Data Protection & Privacy Platform
Incident Response & Breach Reporting	Notify authorities & users within mandated timelines	• Centralised Logging & Monitoring
		• Breach Detection Alerts