Vishwaas.ai

Industry Brief

BFSI

DPDP Act Compliance for Banking, Financial Services & Insurance

Why BFSI Has the Highest Compliance Exposure Under the DPDP Act

Banks, NBFCs, insurance companies, broking firms, and payment aggregators sit at the intersection of the highest-stakes personal data categories under the DPDP Act 2023:

- Financial data: account numbers, transaction history, credit scores, salary, loan repayment behaviour
- Identity data: PAN, Aadhaar, passport, voter ID — collected mandatorily under RBI KYC norms
- Health data (insurance): medical history, pre-existing conditions, diagnostic reports
- Biometric data: fingerprint and iris scans collected under Aadhaar-based eKYC

These are precisely the categories that draw the highest scrutiny from the Data Protection Board of India (DPBI) and carry penalties of up to ₹250 crore per instance under Schedule 1 of the DPDP Act.

At the same time, BFSI organisations operate under a multi-regulator environment — RBI, IRDAI, SEBI, PFRDA — where compliance obligations overlap, sometimes conflict, and must all be met simultaneously. Vishwaas AI is designed to navigate this complexity.

The Three BFSI-Specific Compliance Challenges

Challenge 1: Consent vs. Regulatory Mandate — What Needs Consent?

Not all data processing in BFSI requires consent. The DPDP Act recognises legitimate use (non-consent lawful bases) for processing mandated by law. But the line between "regulatory mandate" and "commercial use" is frequently crossed — and that crossing requires explicit consent.

Processing Activity	Lawful Basis	Consent Required?
YC data collection (RBI mandate)	Legitimate use — legal obligation	No
Credit bureau reporting (RBI mandate)	Legitimate use — legal obligation	No
Marketing emails / SMS	Commercial purpose	Yes — explicit
Cross-sell / upsell communications	Commercial purpose	Yes — explicit
Data sharing with group companies	Business purpose	Yes — explicit
Sharing with third-party fintechs / insurance partners	Data processor relationship	Yes — explicit + DPA required
Fraud detection and AML processing	Legitimate use — legal obligation	No
Loan underwriting using bureau data	Contractual necessity	Contextual

BFSI organisations routinely conflate regulatory mandates with commercial consent — bundling marketing permission into account opening forms alongside KYC acknowledgements. The DPDP Act requires these to be granular and unbundled: a customer cannot be required to consent to marketing communications as a condition of opening a bank account.

Vishwaas AI solution: Purpose-specific consent collection with the requires_explicit_opt_in flag per purpose, ensuring KYC acknowledgements and marketing consents are collected and stored separately, with distinct legal bases recorded on each consent record.

Challenge 2: The Multi-System Identity Problem at BFSI Scale

A leading Indian private bank's customer data is typically distributed across:

System	Data Held
Core Banking System (Finacle / Flexcube)	Account, KYC, transactions
Loan Origination System	Loan applications, bureau pulls, income data
CRM (Salesforce / proprietary)	Relationship data, interaction history
Mobile Banking App	Device IDs, behavioural data, UPI transactions
Credit Card System	Card transactions, spend categories
Insurance Subsidiary	Policy details, health declarations, nominees
Marketing Platform (CleverTap / MoEngage)	Campaign engagement, segment data

When a customer exercises their right to erasure under Section 12, "delete all my data" means deleting across all seven systems. Without a unified identity, the bank has no way to locate all records for that individual — let alone orchestrate their deletion.

Vishwaas AI solution: The Consumer Data Unification engine connects all seven source systems. Deterministic matching on PAN, Aadhaar hash, or mobile number auto-links records across systems into a single canonical profile. One DPR erasure request generates orchestrated erasure jobs across every linked system, tracked to completion.

Challenge 3: The 72-Hour Breach Clock Under DPDP + RBI

Under DPDP Act Section 8(6), a Data Fiduciary must notify the DPBI of a personal data breach within 72 hours of becoming aware of it. Under RBI's Cyber Security Framework, banks must also notify RBI's Computer Emergency Response Team (CERT-In) within a similar window.

BFSI breaches are disproportionately high-impact: a breach affecting account numbers, PAN, or loan data triggers both regulatory clocks simultaneously, plus notification obligations to every affected data principal.

Vishwaas AI solution: The Breach Management module starts a 72-hour countdown from the moment an incident is reported. It tracks all required notification steps (DPBI notification, principal notification, RBI/IRDAI notification where applicable), generates the required evidence package, and maintains an audit trail of every action taken within the breach response window.

BFSI Use Cases — Vishwaas AI in Action

Use Case 1: Retail Bank — Account Opening and Marketing Consent

Scenario: A retail bank onboards 50,000 new savings account holders per month via its mobile app.

Current risk: The account opening form presents a single consent checkbox: "I agree to the Terms & Conditions and consent to receiving product offers and marketing communications." This bundled consent violates DPDP Act Section 6(2), which requires consent to be specific to each purpose and not bundled with service terms.

With Vishwaas AI:

- Account opening integrates the Vishwaas AI Consent SDK (embeddable banner/form)
- Separate consent prompts are displayed for: (a) account servicing communications, (b) cross-sell product offers, (c) data sharing with group insurance subsidiary, (d) third-party partner offers
- Each consent is collected in the language the customer has selected (22 Indian languages supported)
- Each consent is stored as a separate, hash-chained record with RFC 3161 TSA timestamp — legally defensible proof of exactly what was agreed, in exactly what language, at exactly what time
- Marketing consent is propagated in real time to the marketing platform; customers who decline are never added to campaign segments

Use Case 2: Insurance Company — Health Data and Renewal Consent

Scenario: A life and health insurer holds policyholder health declarations, diagnostic reports, and nominee details for 2 million customers across three product lines (term life, health, motor).

Current risk: Health data is among the most sensitive categories under the DPDP Act. Sharing policyholder health data with reinsurers or third-party administrators requires documented consent. Renewal communications must be distinct from marketing. The insurer has no systematic record of what each policyholder consented to and when.

With Vishwaas AI:

- Source system connectors link the Policy Administration System, Claims Management System, and Marketing CRM
- Consent is collected at policy issuance — separately for: (a) core policy servicing, (b) data sharing with reinsurer, (c) third-party administrator access, (d) renewal reminders vs. new product offers
- Consent records are hash-chained and signed — when a policyholder or IRDAI challenges a data sharing decision, the signed consent record and TSA token provide court-admissible evidence of authorisation
- A DPO dashboard tracks consent expiry dates across the policyholder base; renewal reminders are dispatched via the Consent Campaign module before expiry, maintaining a compliant consent chain without interrupting coverage

Use Case 3: NBFC / Fintech Lender — Bureau Data and Purpose Limitation

Scenario: A digital lending platform pulls credit bureau data for every loan applicant. It also sells anonymised portfolio data to analytics companies.

Current risk: Credit bureau pulls require consent under the Credit Information Companies (Regulation) Act and implicitly under the DPDP Act. Portfolio data "anonymisation" that retains PAN or mobile number hash is not anonymised under DPDP Act standards. The company has no documented consent for these secondary uses.

With Vishwaas AI:

- The Consent module captures explicit, purpose-specific consent at loan application: (a) credit bureau pull for underwriting, (b) marketing communications, (c) data sharing with analytics partners
- The Notice module delivers a DPDP-compliant privacy notice in the applicant's language at the point of consent — satisfying Section 5 notice requirements
- The Data Map module documents which data categories are shared with which processors, supporting a vendor DPA for each analytics partner
- If the applicant later exercises erasure rights, the DPR module orchestrates deletion from the NBFC's systems while flagging bureau data (which has its own retention obligations under CICA) for regulatory review before deletion

Regulatory Alignment

Regulation	Relevant Obligation	Vishwaas AI Module
DPDP Act §5	Itemised, language-accessible notice before consent	Notice Module — 22 languages, standalone notice format
DPDP Act §6	Specific, granular, unbundled consent per purpose	Consent Module — purpose catalogue with requires_explicit_opt_in
DPDP Act §8(6)	Breach notification to DPBI within 72 hours	Breach Module — 72-hour countdown, DPBI notification workflow
DPDP Act §§11–12	Right to access, correct, erase	DPR Module — rights request queue, erasure orchestration
DPDP Act §13	30-day grievance resolution SLA	DPR Module — SLA tracking, DPBI escalation
RBI KYC Master Directions	Data minimisation; purpose limitation for KYC data	Consent Module — lawful basis tagging; purpose-specific records
RBI Cybersecurity Framework	Breach notification to RBI/CERT-In	Breach Module — multi-authority notification workflow
IRDAI Data Protection Guidelines	Policyholder data confidentiality; reinsurer sharing consent	Vendor Module — DPA tracking; Consent Module — sharing consent
SEBI Cybersecurity Circular	Client data protection; incident reporting	Breach Module — incident intake and reporting workflow
CICA (Credit Bureau)	Credit information handling; purpose limitation	Data Map — retention policies; DPR — erasure flag for bureau data

Why BFSI CISOs and DPOs Choose Vishwaas AI

Non-repudiation that satisfies regulators: BFSI organisations face regulatory audits from RBI, IRDAI, SEBI, and now the DPBI. When a regulator asks "prove this customer consented to that data sharing", Vishwaas AI produces a signed consent record with an RFC 3161 TSA timestamp — independently verifiable by any party, including the regulator, without depending on Vishwaas AI infrastructure.

Scale built for BFSI volumes: Consent ledger designed for millions of records. Batch consent status API handles 1,000 consent checks in < 200ms — suitable for pre-send filtering across large customer bases.

PII encryption matching BFSI security standards: All PII fields (Aadhaar, PAN, account-linked identifiers) stored as AES-256-GCM ciphertext + SHA-256 hash for indexed lookup. Aadhaar never stored in plaintext — not even in staging records. Key management via AWS KMS with per-tenant key pairs.

India data residency: All data stored exclusively in AWS Mumbai (ap-south-1). No cross-region replication of personal data. Satisfies RBI's directive on storage of payment system data and DPDP Act data localisation expectations.

Deployment in days, not months: BFSI organisations already operating OneTrust or similar platforms pay ₹25–50L+ per year for a GDPR-first product that requires extensive configuration for Indian regulatory requirements. Vishwaas AI is DPDP-native, deployable in

+1 888 208 5076
+91 901 926 6824
sales@crossidentity.com
www.crossidentity.com