TECHCIRCLE kyndryl

# The Cost of Trust

## Inside India's DPDP Act and the Future of Responsible Growth

TECHCIRCLE

kyndryl

# Table of Contents

## Chapter 1

# Executive Summary

India's BFSI sector is now the nervous system of a USD 4+ trillion economy. More than 1 billion Indians are online, and December 2025 alone recorded transactions valued at INR 27 lakh crore. *(December 2025, India Today)* This data has become both an accelerator and a massive vulnerability, From large PSBs and private banks to SFBs, RRBs, cooperative banks and NBFCs, every category now runs on **always-on digital rails**—core banking, mobile apps, digital lending, wallets, and instant payments.

### The Business Case for Privacy

- 72% of Indians believe financial institutions collect more data than required, and 86% of users express a desire for granular control over their data sharing, indicating that Indian consumers increasingly expect stronger privacy practices and explicit consent mechanisms in BFSI interactions. *(Business Standard. 2024)*
- Global surveys like PwC consistently show that **trust and privacy** rank among the top three factors influencing customers' choice of financial institution. (*Global Digital Trust Insights, 2023, PwC)*

Against this backdrop, the **Digital Personal Data Protection Act, 2023 (DPDP Act 2023)** is India's new baseline for responsible growth. For simplicity, this paper refers to it as the **DPDP Act** or **DPDP** hereafter.

### DPDP Act at its core

1. Recognises individuals as **Data Principals** and financial institutions as **Data Fiduciaries** with explicit obligations. *(DLA Piper Data Protection, 2025)*
2. Codifies seven core principles—**lawful purpose, consent, data minimization, accuracy, storage limitation, security safeguards, and accountability**. *(Advent of Privacy Era in India, EY, 2023)*
3. Allows data use without consent in **specified legitimate scenarios** (e.g., compliance with statutory obligations, court orders, or regulatory reporting under laws such as CICRA)—but only **to the extent and for the duration required by that mandate**. *(Advent of Privacy Era in India, EY, 2023)*

For BFSI leaders, DPDP is not just another compliance regime. It is:

A **trust and reputation strategy** (customer retention, digital adoption, ecosystem partnerships).

A **technology-architecture reset** (data lineage, consent-aware platforms, zero trust).

A **board-level governance agenda** that must sit alongside credit, liquidity, and cyber risk.

This playbook is written for CIOs, CISOs, CDOs, CROs, and board members of banks, insurers, NBFCs, and payments players. It aims to answer the question:

***How do we turn DPDP from a cost of regulation into an engine for trust, resilience, and growth?***

*The Digital Personal Data Protection Act, 2023 reshapes the future of banking by embedding trust, accountability, and customer empowerment into the financial system. By clearly defining data ownership and consent, it restores control to individuals while reinforcing privacy as a core financial right. Purpose-driven data usage aligns innovation with responsibility, allowing banks to leverage data for personalization, risk management, and financial inclusion without compromising trust. As institutions adopt privacy-by-design and compliant digital architectures, DPDP becomes an enabler of next-generation banking—secure, intelligent, and customer-first—where long-term value is created through confidence, transparency, and responsible use of data.*

**Rakesh Ranjan**
CDO, Kyndryl India

## Chapter 2

# India's Data Moment: Beyond UPI

The narrative of India's digital growth often fixates on UPI volumes, yet the reality is far broader. The digitization of India's BFSI sector now permeates every layer of the economy—from Scheduled Commercial Banks (SCBs) and Small Finance Banks (SFBs) to the extensive network of Rural Cooperative Banks (RCBs). With NABARD driving the computerization of thousands of Primary Agricultural Credit Societies (PACS), the "digital footprint" now extends to the remotest villages.

Across **scheduled commercial banks, small finance banks, regional rural banks, co-operative banks, and NBFCs**, digital is now embedded in:

- **Customer onboarding** (video KYC, digital documentation)
- **Everyday banking** (mobile/internet banking, UPI, wallets)
- **Lending** (digital journeys, embedded finance, co-lending)
- **Wealth & insurance** (robo-advisory, online policy issuance)

But this ubiquity has a dark twin:

**₹23,000 Crore**

**lost due to** cyber fraud cases in 2024, a jump of nearly 206 percent in comparison to 2023. *(The New Indian Express, 2025)*

**₹2.2 Crore**

Cost of **an average data breach in India** with financial services consistently among the most targeted and most expensive sectors to remediate. *(Cost of Data Breach Report, Aug 2025, IBM)*

The DPDP Act arrives to secure this sprawling ecosystem, ensuring that the momentum of financial inclusion does not come at the cost of citizen privacy.

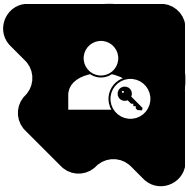
## Chapter 3

# What the DPDP Act Means for BFSI

The DPDP Act shifts control of personal data from institutions to individuals, redefining how trust is earned and sustained in BFSI. Banks and financial institutions now operate as custodians rather than owners of customer data. This change is highlighted in the distinct roles and responsibilities set out by the Act.

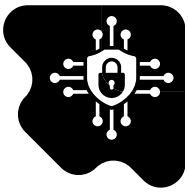
To navigate the Act, BFSI leaders must clearly distinguish between two pivotal roles. The Act shifts the power dynamic from the institution to the individual.

### Data Principal



The individual to whom the personal data relates (e.g., the customer, employee, or guarantor).

### Data Fiduciary



The entity that determines the purpose and means of processing the data (e.g., the Bank, Insurer, or NBFC).

### The Implication for BFSI

**The Owner:** They now hold the right to access, correct, and erase their data. They can withdraw consent at any time, forcing banks to stop processing immediately (unless a regulatory exemption applies).

**The Accountable:** The bank is fully liable for the data's safety, accuracy, and usage - even if the actual processing is outsourced to a third-party vendor (Data Processor).

### Key Takeaway

For most mid-to-large BFSI institutions, you should assume you will either be designated as an SDF or expected to operate at SDF-level maturity.

### Significant Data Fiduciary (SDF)

A Data Fiduciary is designated as “significant” by the government based on factors such as volume and sensitivity of data, risk to rights, and potential impact on sovereignty. SDFs face stricter obligations (e.g., Data Protection Impact Assessments, audits, DPO appointment).

### Boardroom Priority: Data Governance

The DPDP Act explicitly places the onus of compliance on the Data Fiduciary, effectively making data governance a Board-level responsibility. It is no longer an IT issue; it is a fiduciary duty.

## The Board's Mandate

**Oversight of Third Parties**: The Board must ensure that all outsourcing contracts (TSPs, Cloud Providers, DSAs) enforce DPDP standards. The bank cannot "outsource" liability.

**Grievance Redressal Mechanism**: The Board must verify the existence of an effective, accessible mechanism for Data Principals to register complaints.

**Periodic Audit**: Regular, independent data audits must be agenda items for the Risk Committee.

For BFSI CIOs, **three mandates** now dominate the boardroom agenda:

### Manage Consent as Core Capability

Consent must be explicit, granular, and easily revocable – centrally governed across internal systems and trusted third-party platforms, not buried in terms and conditions.

### Operationalize Privacy-by-Design

Privacy must move from documentation to design - embedded into applications, APIs, and analytics pipelines from day one.

### Govern Third-Party Ecosystems

Accountability extends to every Technology Service Provider (TSP). Banks remain liable for how partners collect, store, and share personal data.

## The cost of failure is real

Penalties of up to **₹250 crore** per violation, alongside reputational damage in an industry where trust has become the ultimate currency.

> *Data stewardship is no longer an IT mandate; it is a leadership obligation that defines enterprise credibility*

**Salil Walke**
Associate Director,
Kyndryl India

## Chapter 4

# The Need for a Unified Counsel

For BFSI leaders, the DPDP Act is not a standalone law but an overlay on existing sectoral regulations. It is critical to map RBI guidelines against DPDP mandates because banks require a unified counsel to understand how these overlapping rules impact their various business streams and processes.

### KYC & Onboarding

**RBI Mandate:**
Mandatory record retention, periodic KYC updates, and prescribed retention timelines for customer due-diligence records

**DPDP Intersection:**
Data may be retained only for legal or declared purposes.

**Operational Implication:**
Banks must separate regulatory retention data from analytics and marketing datasets, with independent consent and purpose controls

### Outsourcing

**RBI Mandate:**
Board oversight & audit rights to protect customer data from being mishandled by third parties

**DPDP Intersection:**
Data fiduciary liability - bank becomes fully liable for data mishandling by third-party providers

**Operational Implication:**
Contracts must enforce privacy-by-design, auditability and DPDP-aligned breach SLAs

### Digital Lending

**RBI Mandate:**
Restricted data collection of non-essential customer data

**DPDP Intersection:**
Credit data cannot be used without purpose-specific consent.

**Operational Implication:**
Product teams must prevent reuse of credit data for cross-sell or marketing without new consent

### Cross-Border

**RBI Mandate:**
Controlled cross-border processing of remitter and beneficiary data under FEMA and RBI directions

**DPDP Intersection:**
Remitter privacy must be maintained

**Operational Implication:**
Banks must maintain end-to-end, ready visibility of data flows across correspondent and UPI networks

## Chapter 5

# The P.R.I.V.A.C.Y. Framework: A Leadership Playbook for DPDP Readiness

To help BFSI leaders navigate the DPDP Act and turn compliance into capability, we have devised the "**P.R.I.V.A.C.Y. Framework**" - seven leadership imperatives that embed DPDP principles into day-to-day decision-making, turning data protection into a growth enabler rather than a constraint.

Adopting P.R.I.V.A.C.Y. turns compliance into culture - linking regulation, reputation, and revenue.

**Purpose**

*(Define, declare, and document why each dataset exists)*
Embed purpose-tagging within core systems; restrict reuse beyond declared intent.

**Risk**

*(Quantify privacy exposure across people, processes, and partners)*
Maintain enterprise-wide privacy risk registers; integrate privacy metrics with ERM dashboards.

**Integrity**

*(Ensure data accuracy and ethical processing)*
Implement data-quality controls, audit trails, and AI ethics frameworks.

**Value**

*(Convert privacy into brand equity and customer trust)*
Launch "data-trust scores" in apps; communicate transparency to users.

P
R
I
V
A
C
Y

**Accountability**

*(Establish clear ownership across the enterprise)*
Appoint Data Protection Officer; form a cross-functional privacy council, define clear SLAs for breach response, root-cause analysis and regulatory intimation within 6 hours.

**Consent**

*(Operationalize informed and dynamic consent management)*
Centralize consent hubs; enable multi-language opt-ins and real-time revocation.

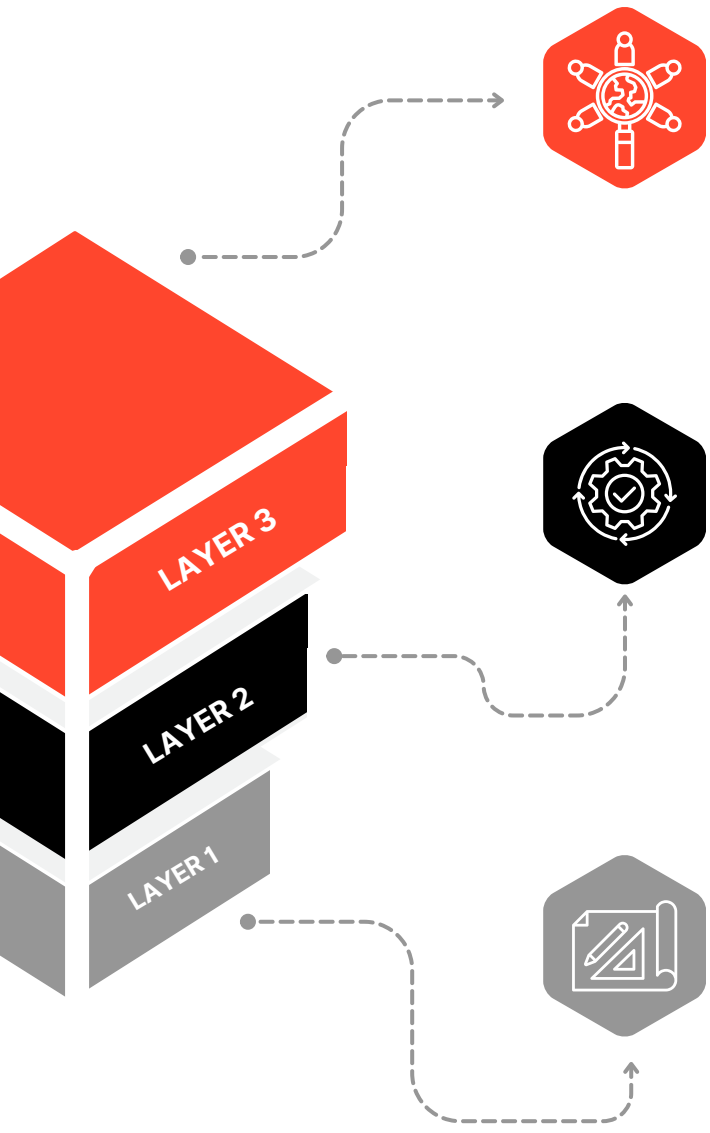
**Yield**

*(Measure returns on privacy investment)*
Track KPIs such as breach-reduction %, customer-trust index, and time-to-comply metrics.

## Chapter 6

# Operationalizing Privacy-by-Design

To move from policy to practice, CIOs must embed privacy into architecture, not appendices.




### Culture Layer

Make Privacy a Shared Responsibility

- Train employees on DPDP principles and customer rights.
- Tie privacy KPIs to managerial performance reviews.
- Publish annual data stewardship reports to reinforce transparency and trust.

### Process Layer

Integrate Governance into Daily Workflows

- Automate data-retention and deletion once business purpose expires.
- Embed privacy checkpoints into product development and marketing lifecycle approvals.
- Extend privacy and risk controls to TSPs through standardized contracts and continuous monitoring.

### Architecture Layer

Enable End-to-End Data Traceability

- Implement data lineage to track customer data from collection through deletion.
- Apply purpose and consent tagging across cloud platforms, APIs, and data warehouses.
- Adopt zero-trust architectures to control access by identity, context, and consent.

When privacy becomes a design input, compliance becomes a design outcome.

Chapter 7

# Top Five DPDP Risk Hotspots for BFSI

## The "Cumulative Penalty" Trap

- Large digital onboarding or Re-KYC programmes can involve tens of millions of records.
- Even a 0.2% error rate (incorrect notices, missing consents, unhonoured erasure requests) can translate into thousands of violations, each separately countable.

## Behavioral Cross-Selling

- Using transaction profiles to push third-party products (e.g., insurance, investments) without explicit opt-ins is high risk.
- Under DPDP, this is a new purpose, and it requires fresh consent.

## Fragmented incident response

- Many institutions still have separate IT, legal, and business incident playbooks, with no single command centre.
- Meeting tight reporting timelines under DPDP and sectoral regulations is difficult without an integrated cyber–privacy response framework.

## Third-party Data Processors

- Fintech partners, KYC vendors, collection agencies, and cloud providers often sit at the edge of the control perimeter.
- Under DPDP, the bank or insurer as Data Fiduciary remains fully liable, even if the breach originates at the vendor.

## Legacy data stores without consent meta-data

- Decades-old core banking and card systems rarely have usable consent trails.
- This makes it difficult to prove legal basis to regulators or honour Data Principal rights at scale.

- Deploying AI-driven data-discovery tools to locate and classify PII within minutes.
- Establishing “Consent Operations Centers” to monitor, manage, and revoke permissions in real time.
- Integrating DPDP controls into existing ISO 27001 and RBI cybersecurity frameworks for seamless compliance.

## Chapter 8

# Kyndryl's Governance Blueprint
# Operationalizing Trust

As BFSI organizations seek to balance innovation with regulatory rigor, technology partners play a critical role. Large-scale transformation requires **partners that understand both regulation and engineering**.

Kyndryl is collaborating with leading Indian banks and insurers to embed DPDP-ready data governance into their digital core through **Consult–Design–Manage** capabilities across data, cloud and cyber. Kyndryl addresses the dual challenge of **scale and compliance** through focused innovation across three layers.

## Partner Risk Management

**Embedded Vendor Controls:**
Privacy-focused SLAs and real-time monitoring are integrated into vendor delivery models, extending DPDP governance across fintech, cloud, and service-provider ecosystems.

## Process Workflow

**Agentic AI with Human Oversight:**
Autonomous AI agents monitor consent patterns and detect anomalies at scale, while operating under Human-in-the-Loop controls aligned with RBI's FREE-AI principles, ensuring explainability, ethical oversight, and clear accountability.

**Unified Data Governance:**
Automated discovery and classification span hybrid environments, delivering end-to-end visibility into PII lineage and usage.

## Architecture Design

**Regulation-Aware AI Models:**
Kyndryl enables the deployment of financial-sector AI models trained on Indian banking regulations and DPDP provisions to automate compliance queries and support continuous Privacy Impact Assessments (PIAs), ensuring architectures remain aligned with evolving legal interpretations.

**Zero-Trust Design:**
Data flows are segmented by identity and context, preventing lateral movement of sensitive PII and restricting access strictly to approved purposes.

*In an era where data fuels innovation, the DPDP Act compels BFSI leaders to redefine trust as a growth multiplier, not mere compliance. Kyndryl pioneers privacy-by-design through predictive governance platforms, transforming regulatory mandates into scalable trust architectures that propel sustainable leadership in India's digital economy.*

**Hussain Zaidi**
VP, Kyndryl India

## CASE STUDY

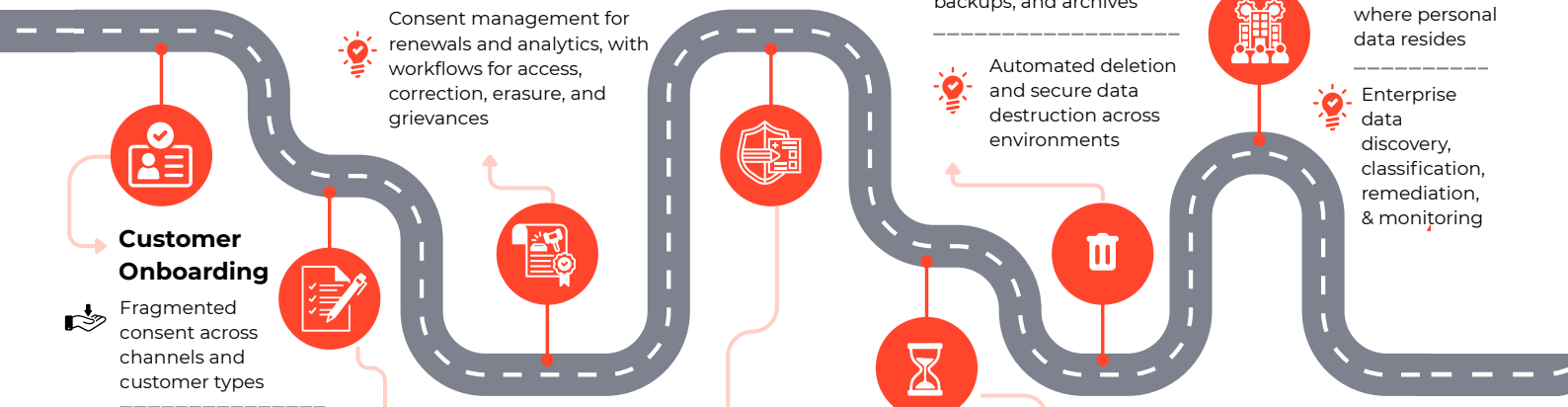
### Strengthening Data Trust Across the Insurance Business Lifecycle: Kyndryl's Proposal

A large, multi-channel insurance provider is seeking greater visibility, control, and consistency in how customer and policy data is managed across a complex ecosystem of systems and partners - in an attempt to navigate the DPDP journey.

**Business Requirement**
The organization needs a unified, scalable approach to manage personal data across the end-to-end insurance lifecycle - enabling consistent consent, secure third-party data sharing, and clear retention and deletion controls.

**Kyndryl's Proposed Approach**
Kyndryl proposed a **business lifecycle-aligned data trust framework**, designed to integrate with the insurer's existing IT infrastructure and operating model.

**Business Lifecycle –Aligned Data Trust Framework**



**Customer Onboarding**
Fragmented consent across channels and customer types

Unified, purpose-based consent across all channels, covering new/existing customers, third-party and child data

**Policy Administration and Servicing**
Consent refresh, analytics usage, customer data rights

Consent management for renewals and analytics, with workflows for access, correction, erasure, and grievances

**Policy Underwriting & Issuance**
Sensitive data use and automated decisions

Risk-based controls, explicit consent for sensitive data, data minimization, and AI governance

**Claims Processing**
Sensitive data shared with multiple partners

Consent-driven third-party data sharing with audit trails and breach readiness

**Deletion**
Residual data in systems, backups, and archives

Automated deletion and secure data destruction across environments

**Policy Maturity**
Data retained beyond business purpose

Clear retention-versus-erasure controls aligned to purpose fulfillment

**Enterprise-Wide (Across Lifecycle)**
Limited visibility into where personal data resides

Enterprise data discovery, classification, remediation, & monitoring

## Chapter 9

# The Road Ahead:
## Trust as the New ROI

DPDP reframes trust from a regulatory obligation into a strategic asset for BFSI, with the next 12–18 months determining who can translate governance into sustained advantage.

In a TechCircle survey, 60% of CIOs responded that they are in either of the two stages: initiating internal boardroom discussions or analysing gaps and preparing formal assessments. But only 2% have a structured plan aligned to the 2027 mandate.

### Leadership Priorities for 2026-27

- Treat **data governance** as a board-level priority alongside credit and liquidity risk.
- Establish end-to-end visibility into **data lifecycle** and **consent flows**.
- View **cyber and privacy investments** as strategic capital expenditure.
- Adopt the **P.R.I.V.A.C.Y. framework** as an enterprise-wide north star.
- Partner with **trusted technology leaders** to operationalize **privacy-by-design** at scale.

By embedding trust into their digital core, financial institutions won't just comply with DPDP - they will capitalize on it. In the coming data decade, trust is no longer a soft metric; it is the hardest currency of growth.

*DPDPA 2023 and DPDP Rules 2025, transform privacy into BFSI's trust currency, requiring consent-aware architectures to drive compliance, customer retention, and inclusive innovation. Those institutions, that demonstrate absolute transparency of personal data privacy & protection along with unambiguous demonstration of consent management, would emerge as the hyper growth businesses in their respective domains.*

**Jayakrishnan Rajagopalan**
Industry Consulting Partner, Kyndryl

## The Final Word:
## From Compliance to Competitive Advantage

In the coming decade, data-rich, trust-poor institutions will lose—regardless of how sophisticated their technology stack looks on slides.

- The banks and financial institutions that win will be those that:
- Treat every customer as a Data Principal with rights, not just an account number.
- Embrace their role as Data Fiduciaries who design for privacy and security from day one.
- Turn DPDP into the foundation of scalable AI, analytics, and ecosystem partnerships.

DPDP, in that sense, is not just a constraint; it is the price of admission to India's next wave of BFSI innovation. The institutions that understand this fastest will convert trust into the hardest ROI metric of all - sustained, profitable growth.

TECHCIRCLE

## About TechCircle

TechCircle is a trusted Go-to-Market consulting and intelligence platform for technology providers. We enable global and Indian tech suppliers to accelerate growth by combining account-level research, market insights, and exclusive executive engagement platforms.

Through in-depth industry intelligence, account profiling, and tailored engagement formats, we connect technology providers with the right decision-makers across BFSI, manufacturing, healthcare, and other industries.

By bridging enterprise intent with supplier opportunity, TechCircle acts as a growth partner, helping tech providers build meaningful client relationships and convert them into measurable business outcomes.


Author

**Anoop Kubba**
Customer Advisory Head,
TechCircle

TECHCIRCLE kyndryl

# The Cost of Trust

## Inside India's DPDP Act and the Future of Responsible Growth

Access the full library of whitepapers, playbooks and more.

Scan to explore more