WHITEPAPER

# The Complete DPDP Compliance Playbook

## for Indian Enterprises

A step-by-step framework for achieving Digital Personal Data Protection Act readiness in 2026, built from real-world compliance engagements

threatsafe

CERT-In Empanelled

ISO 27001 Certified

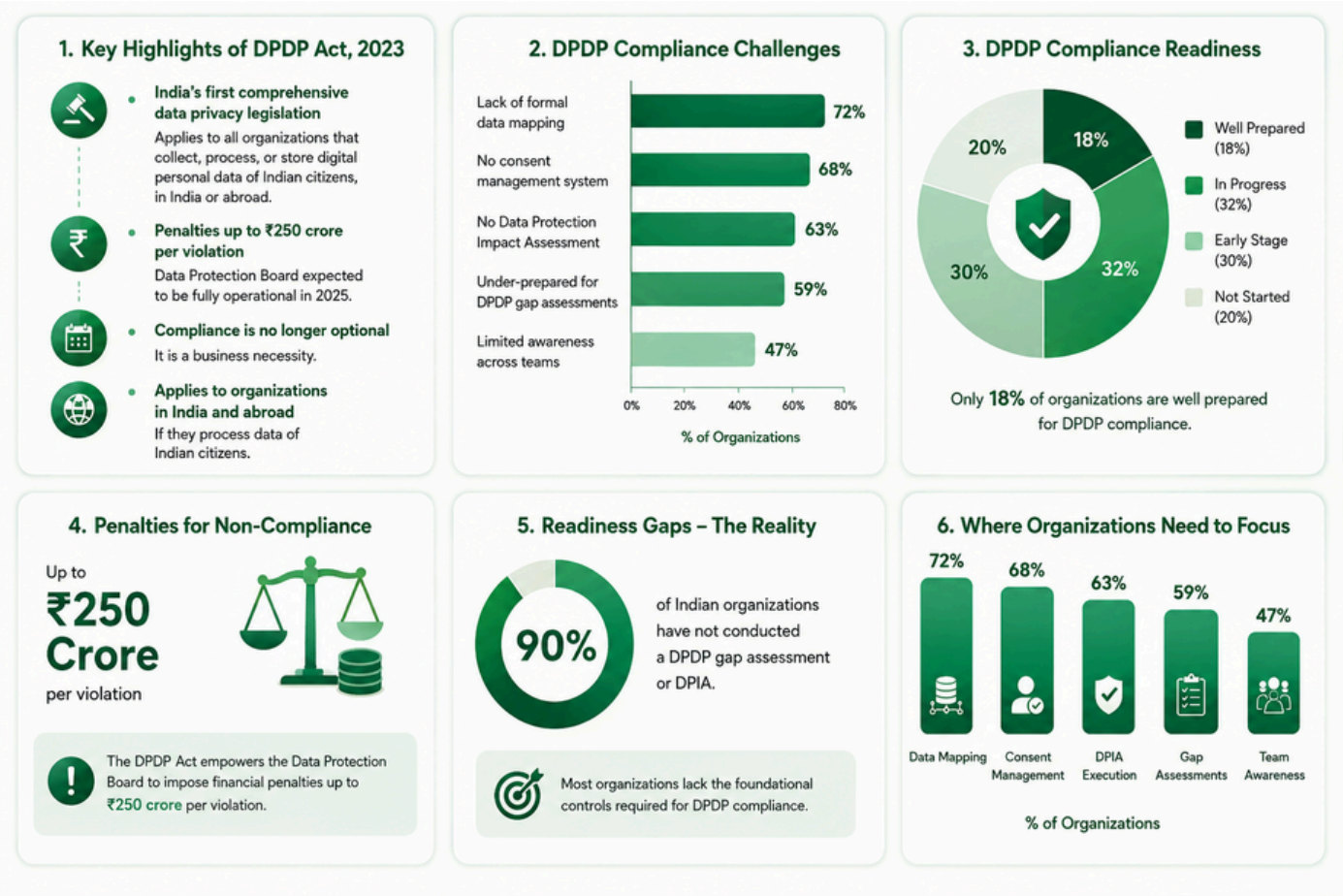
DPDP Advisory Partner

# Executive Summary

India's Digital Personal Data Protection Act, 2023 (DPDP Act) is the country's first comprehensive data privacy legislation, and it applies to virtually every organization that collects, processes, or stores digital personal data of Indian citizens, whether the organization is based in India or abroad.

With penalties reaching up to ₹250 crore per violation, and the Data Protection Board expected to become fully operational in 2025, compliance is no longer optional, it is a business necessity. Yet, in ThreatSafe's experience across hundreds of DPDP gap assessments, most Indian organizations are significantly under-prepared. The majority lack formal data mapping, have no consent management system, and have never conducted a Data Protection Impact Assessment.

This whitepaper is written for CISOs, legal teams, data protection officers, IT heads, and compliance managers who need a clear, structured, and actionable path to DPDP readiness. It distills ThreatSafe's end-to-end compliance methodology, refined through real engagements across BFSI, healthcare, e-commerce, and SaaS, into a framework any organization can adopt.

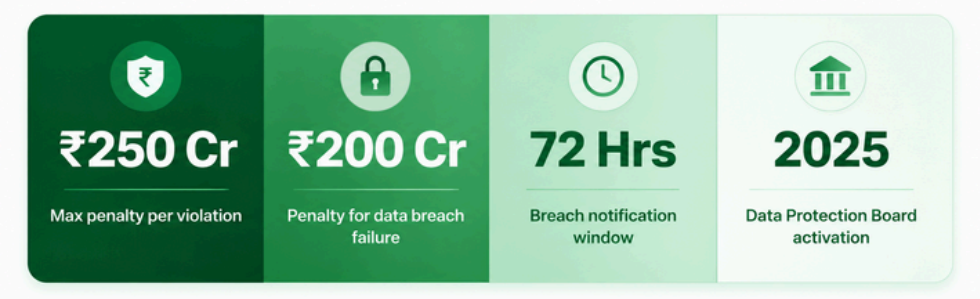


# 1.

# Why DPDP Demands Immediate Attention

India processes personal data at an unprecedented scale, driven by rapid digital adoption across banking, healthcare, retail, SaaS, telecom, and government services. With over 850 million internet users and one of the fastest-growing digital economies globally, organizations today handle enormous volumes of sensitive customer and employee information. The Digital Personal Data Protection (DPDP) Act introduces a major shift in how businesses must collect, process, store, and secure personal data, making compliance, transparency, and accountability business-critical priorities.

## The Stakes Are High




Unlike many global regulations where penalties are calculated on annual turnover, DPDP Act penalties are fixed, and can stack per violation. A single negligent data breach that also involves failure of consent management, breach notification delay, and inadequate security controls could attract multiple separate penalties simultaneously.

## What ThreatSafe Sees During Gap Assessments

Across DPDP readiness assessments conducted by ThreatSafe, several recurring compliance gaps consistently emerge. Many organizations still operate without structured consent management, formal data inventories, incident response workflows, or clear data retention policies. Businesses also struggle with third-party vendor governance, employee awareness, access control visibility, and breach reporting preparedness. These gaps not only increase regulatory exposure but also create significant operational and reputational risk.

| Compliance Area | % of Organizations With Gap |
| --- | --- |
| Formal data mapping and inventory | **89%** have no complete data map |
| Consent management system | **94%** lack a structured consent mechanism |
| Data Principal rights process | **91%** have no formal rights request workflow |
| Data Protection Impact Assessment | **97%** have never conducted a DPIA |
| Breach notification plan | **83%** have no DPDP-aligned IR plan |
| Vendor/processor agreements | **88%** lack data protection clauses with vendors |

## ThreatSafe Insight

The organizations most at risk are not those who are unaware of DPDP, they are the ones who believe their existing IT security controls, privacy policies, and ISO 27001 certification automatically satisfy DPDP requirements. They do not. DPDP introduces specific legal obligations around consent, rights, and governance that technology controls alone cannot fulfill.

# 2.

# What the DPDP Act Actually Says

The Digital Personal Data Protection Act, 2023 was passed by the Indian Parliament on August 11, 2023, and received Presidential assent shortly after. It is the culmination of nearly a decade of deliberation following the Supreme Court's landmark 2017 Puttaswamy judgment that recognized privacy as a fundamental right.

## Scope and Applicability

**The DPDP Act applies to the processing of digital personal data where:**

1. The processing takes place within the territory of India, OR
2. The processing takes place outside India but involves offering goods or services to Data Principals (individuals) in India

## Key Definitions You Must Know

| Term | Definition |
|---|---|
| **Personal Data** | Any data about an identifiable individual, name, email, phone, location, device ID, biometrics, financial data, health data |
| **Digital Personal Data** | Personal data collected or stored in digital form, including data that was originally non-digital but has been digitized |
| **Data Principal** | The individual to whom the personal data belongs, the person whose data is being processed |
| **Data Fiduciary** | Any person or entity that determines the purpose and means of processing personal data (equivalent to 'Data Controller' in GDPR) |
| **Data Processor** | Any entity that processes data on behalf of a Data Fiduciary (equivalent to 'Data Processor' in GDPR) |
| **Consent Manager** | A registered entity that manages consent on behalf of Data Principals through an interoperable platform |
| **Significant Data Fiduciary (SDF)** | A Data Fiduciary designated by the Central Government based on volume, sensitivity, national security risk, or impact on elections |

## DPDP vs GDPR

Many organizations attempt to map **DPDP to GDPR** and assume compliance with one implies compliance with the other. This is incorrect. **The table below highlights the most important differences:**

| Aspect | GDPR (EU) | DPDP Act (India) |
|---|---|---|
| **Legal Bases** | 6 legal bases including legitimate interest | Primarily consent + certain legitimate uses |
| **Penalties** | Up to 4% of global annual turnover | Fixed up to ₹250 crore per violation |
| **Cross-Border Transfers** | Adequacy decisions + Standard Clauses | Blacklist approach, blocked countries notified |
| **Age of Minor** | Under 16 (varies by member state) | Under 18, verified parental consent required |
| **Right to Object** | Explicit right to object to processing | Not included in DPDP Act |
| **DPO Mandate** | Required for certain categories | Required only for Significant Data Fiduciaries |
| **Enforcement** | National DPAs in each member state | Centralized Data Protection Board of India |

**Note:**

DPDP is not the same as GDPR and introduces India-specific compliance obligations around consent, governance, and data rights. The Act applies to any organization processing digital personal data of individuals in India. Understanding core concepts like Data Fiduciary, Data Processor, and Consent Manager is essential for building an effective DPDP compliance program.

# 3.

# Data Fiduciary vs Data Processor

Understanding whether your organization is a Data Fiduciary, a Data Processor, or both, and in what capacity, is the first and most critical step in DPDP compliance. The obligations differ significantly.

## Data Fiduciary Obligations

If your organization decides WHY and HOW personal data is processed, you are a Data Fiduciary. This carries the heaviest obligations:

- Ensure processing only happens with valid consent or a permitted legal basis
- Provide a clear, plain-language privacy notice before collecting data
- Collect only the data necessary for the stated purpose (data minimisation)
- Retain data only as long as necessary and then delete it
- Implement appropriate technical and organizational security measures
- Honor Data Principal rights: access, correction, erasure, grievance
- Notify the Data Protection Board AND affected Data Principals in case of a breach
- Ensure Data Processors you engage also comply with DPDP obligations

## Data Processor Obligations

If your organization processes data on behalf of a Data Fiduciary (e.g., a cloud provider, SaaS vendor, BPO), you are a Data Processor. Your obligations are narrower but still significant:

- Process data only as instructed by the Data Fiduciary
- Implement security measures as required by the Data Fiduciary
- Assist the Data Fiduciary in responding to Data Principal rights requests
- Notify the Data Fiduciary immediately upon becoming aware of a personal data breach
- Not engage sub-processors without the knowledge of the Data Fiduciary

## Important: You Can Be Both

Many organizations are simultaneously a **Data Fiduciary** (for their customers' data) and a **Data Processor** (for their enterprise clients' data). For example, a payroll SaaS company processes employee data on behalf of its clients (Data Processor) while also collecting its own users' data for product improvement (Data Fiduciary). Each role demands separate compliance structures.

## Significant Data Fiduciary (SDF) - Additional Obligations

**The Central Government can designate certain Data Fiduciaries as 'Significant Data Fiduciaries' based on:**

- Volume and sensitivity of personal data processed
- Risk to rights of Data Principals
- Potential impact on sovereignty, integrity, or national security of India
- Risk to electoral democracy
- Security of the State

**SDFs face additional obligations including:**

- Mandatory appointment of a Data Protection Officer (DPO) based in India
- Appointment of an independent data auditor
- Periodic Data Protection Impact Assessments
- Algorithmic transparency requirements
- Regular data audits

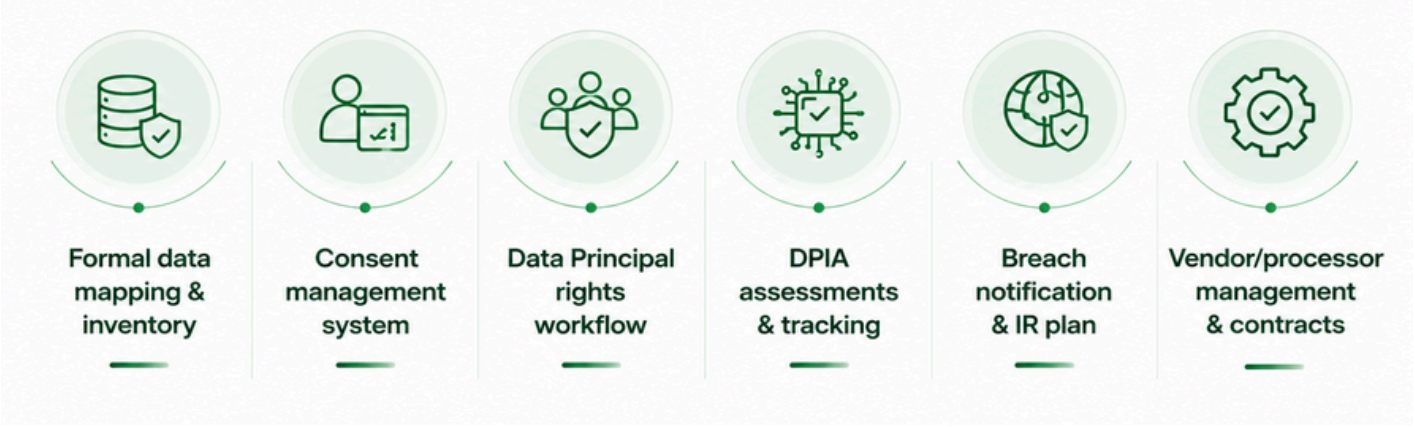
# 4.

# Building A Consent Management System

Consent is the primary legal basis for processing personal data under DPDP. Unlike GDPR, which offers six lawful bases, DPDP's scope for processing without consent is narrow and limited to specific 'legitimate uses.' For most commercial organizations, consent will be the foundation of almost all data processing.

## What Valid Consent Looks Like Under DPDP

DPDP sets a high bar for consent validity. Consent must be:




## What DPDP Prohibits

Organizations cannot use dark patterns to obtain consent. Pre-checked boxes, bundled consent for unrelated purposes, consent buried in terms and conditions, and making consent a condition for services that don't require the data, all of these violate DPDP's consent requirements.

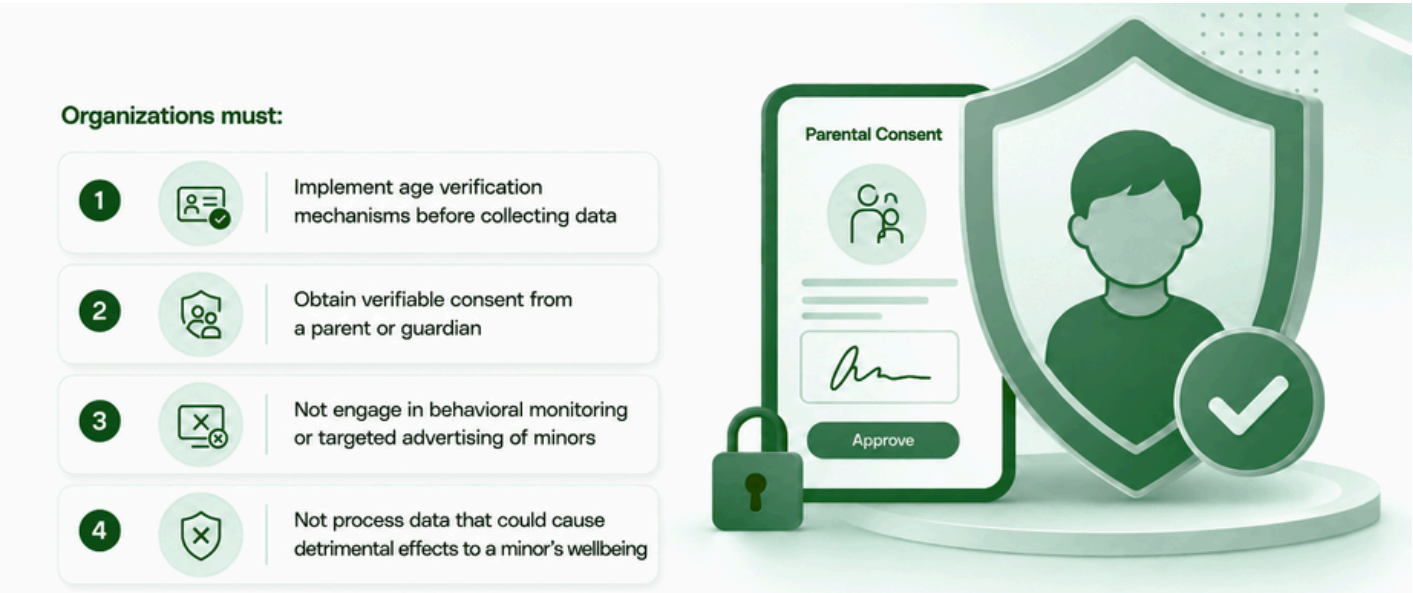
## Consent Management System, Technical Implementation

**ThreatSafe** recommends a four-layer consent management architecture:

| Layer | Component | What It Does |
|---|---|---|
| 1 | **Consent Collection Interface** | Purpose-specific consent notices at data collection points, website, app, offline forms digitized |
| 2 | **Consent Repository** | Immutable audit log of every consent: who, what purpose, when given, IP address, version of notice shown |
| 3 | **Preference Centre** | Data Principal portal to view, modify, and withdraw consents, accessible at all times |
| 4 | **Processing Controls** | Technical controls that enforce consent, no data flows unless consent record exists for that purpose |

## Consent for Children (Under 18)

DPDP treats all individuals under 18 as minors and requires verifiable parental consent before processing their data. This is stricter than GDPR in several member states. Organizations must



# 5.

# Honoring Data Principal Rights

The DPDP Act grants Data Principals five rights that organizations must operationalize, not just acknowledge in a privacy policy. Each right requires a concrete process, a response timeline, and an audit trail.

| Right | What It Means | ThreatSafe Implementation Guidance |
|---|---|---|
| **Right to Access** | Data Principal can request a summary of what personal data is held about them and how it is being processed | Build a self-service data access portal; automate data retrieval across systems |
| **Right to Correction** | Data Principal can request correction of inaccurate or misleading data | Implement update workflows with verification and audit logging |
| **Right to Erasure** | Data Principal can withdraw consent and request deletion of their data, subject to legal retention obligations | Automated deletion workflows; maintain legal hold exceptions register |
| **Right to Grievance Redressal** | Data Principal can raise a complaint about data handling and must receive a response within a reasonable time | Dedicated grievance officer, tracked ticket system, escalation to Data Protection Board if unresolved |
| **Right of Nomination** | Data Principal can nominate another person to exercise rights on their behalf in case of death or incapacity | Nomination capture at consent stage; verification process for nominee claims |

## Response Timeline

DPDP does not specify exact timelines for rights requests in the Act itself, these will be defined in the Rules. However, ThreatSafe recommends adopting a 30-day response standard aligned with global best practices. For grievances escalated to the Data Protection Board, organizations must be prepared to respond within timeframes the Board specifies.

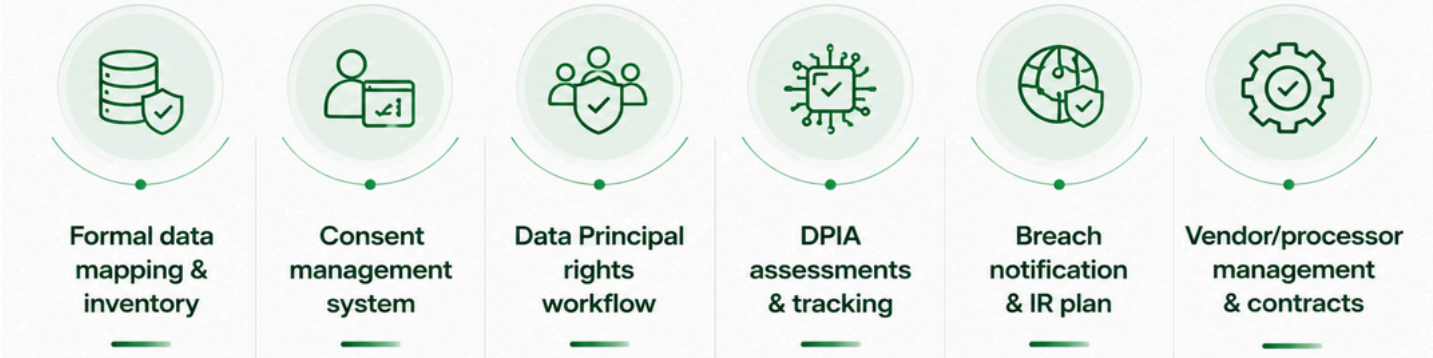
# 6.

# Data Protection Impact Assessment (DPIA)

A DPIA helps identify and reduce privacy risks before launching high-risk data processing activities. While mandatory for Significant Data Fiduciaries under DPDP, it is recommended for all organizations.

## When Should You Conduct a DPIA?

**ThreatSafe** recommends triggering a DPIA whenever any of the following apply:




## ThreatSafe's DPIA Methodology

| Step | Phase | Activities |
|---|---|---|
| 1 | Scoping | Define the processing activity, data flows, stakeholders, and systems involved |
| 2 | Necessity Assessment | Evaluate whether processing is necessary and proportionate to the stated purpose |
| 3 | Risk Identification | Identify potential privacy risks to Data Principals, unauthorized access, profiling, discrimination, financial harm |
| 4 | Risk Evaluation | Rate each risk by likelihood and severity; categorize as low, medium, or high |
| 5 | Mitigation Measures | Define controls to reduce identified risks, technical, organizational, and contractual |
| 6 | Sign-off and Review | Document outcomes, obtain sign-off from DPO/CISO, schedule periodic review |

# 7.

# Breach Notification And Incident Response

A personal data breach under DPDP is defined as any unauthorized processing, or accidental disclosure, acquisition, sharing, use, alteration, destruction, or loss of access to personal data in a manner that compromises the confidentiality, integrity, or availability of the data.

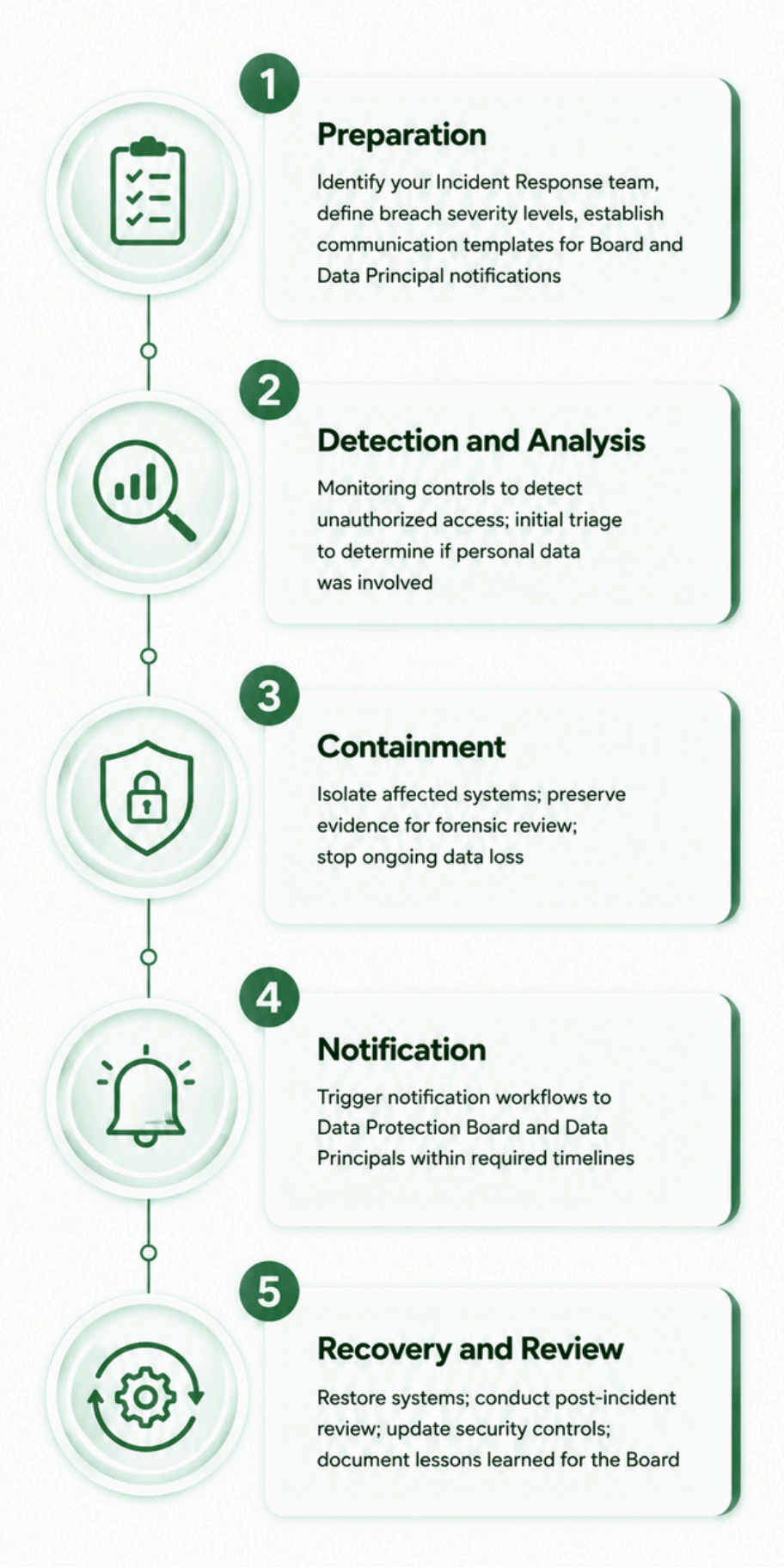
The DPDP Act imposes mandatory notification obligations on Data Fiduciaries in the event of a breach, both to the Data Protection Board and to each affected Data Principal.

## Breach Notification Timeline

| Timeframe | Required Action |
|---|---|
| **Immediately on detection** | Internal containment and evidence preservation, do not delete logs |
| **As soon as reasonably practicable** (Rules will specify exact window ThreatSafe recommends 72 hours) | Notify the Data Protection Board with: nature of breach, categories of data affected, estimated number of Data Principals, contact details of DPO/Grievance Officer, measures taken |
| **Simultaneously with Board notification** | Notify each affected Data Principal in clear, plain language about: what happened, what data was affected, what they should do to protect themselves |

## ThreatSafe's DPDP-Aligned Incident Response Plan Structure

Every organization should have a documented incident response plan that specifically addresses DPDP notification obligations. **ThreatSafe structures this plan across five phases:**



# 8.

# Cross-Border Data Transfer Rule

Unlike GDPR's adequacy decision model that pre-approves certain countries for data transfers, DPDP adopts a blacklist approach: personal data can be transferred to any country EXCEPT those specifically restricted by the Central Government through a notification.

This blacklist has not yet been published as of the date of this whitepaper. However, organizations should prepare for its publication and build transfer assessment processes now.

## What Organizations Must Do Today

- **Map all international data flows:** identify every country where personal data of Indian citizens is being sent, cloud providers, SaaS tools, analytics platforms, BPOs, subsidiaries
- **Maintain a data transfer register:** document the purpose, legal basis, recipient, country, and safeguards for each international transfer
- **Review vendor data processing agreements:** ensure contracts with overseas processors restrict their processing to agreed purposes and require them to comply with DPDP obligations
- **Monitor the blacklist:** once published, immediately assess whether any current transfers are restricted and have a contingency plan
- **Data localisation readiness:** certain categories of sensitive data may face localisation requirements, build architecture flexibility now

## ThreatSafe Recommendation

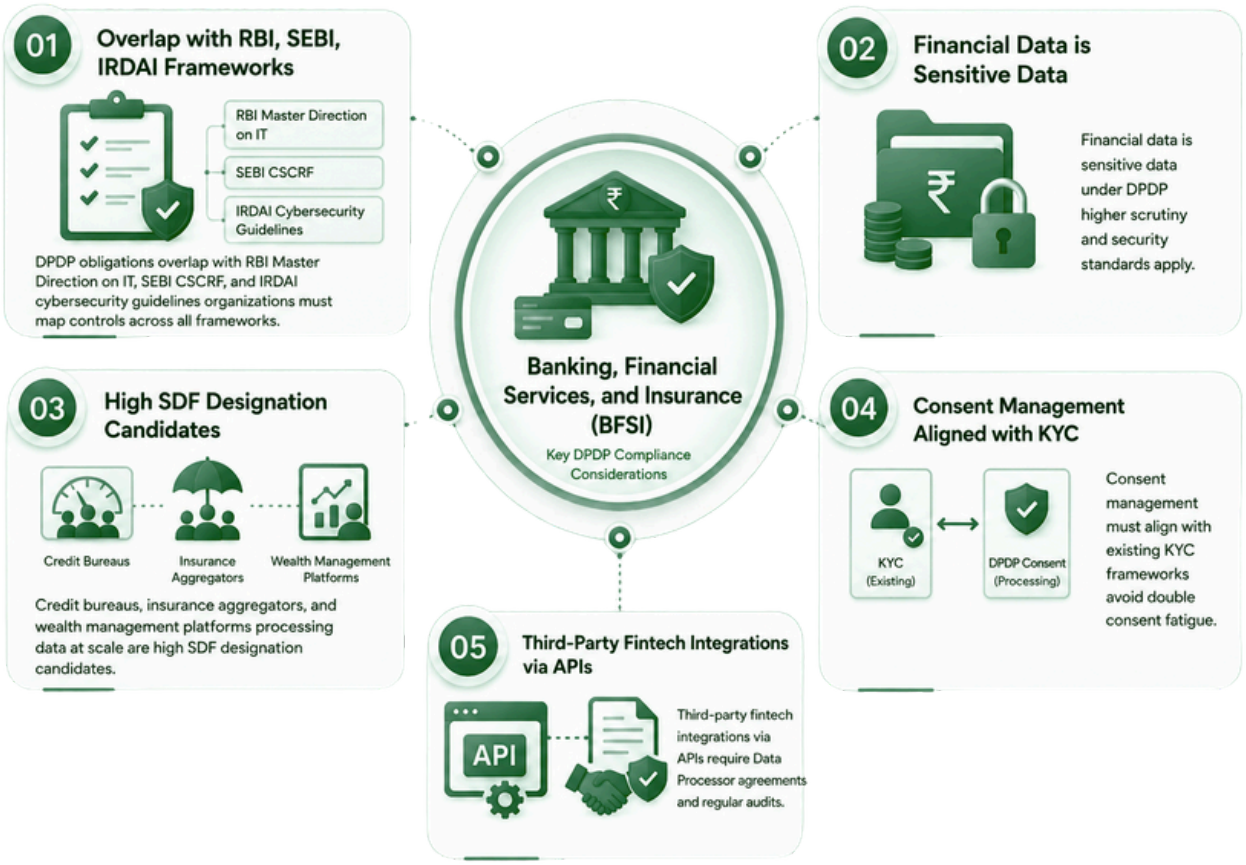
Do not wait for the blacklist to be published. Start your international data flow mapping today. The organizations that struggle most when new restrictions are published are those who have not mapped their data flows and discover at the last moment that critical business systems rely on restricted transfers.

# 9.

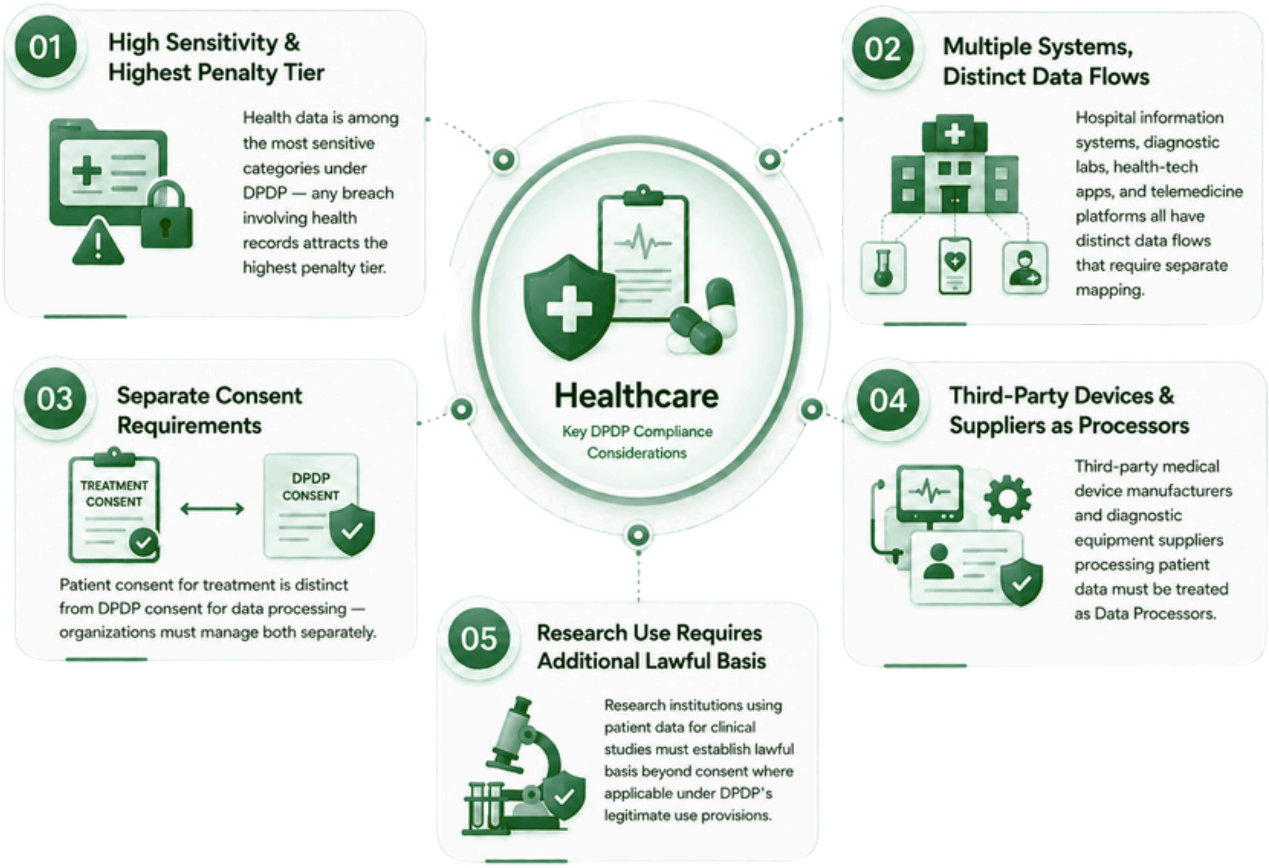
# Industry-Specific Compliance Considerations

While DPDP applies uniformly, the practical compliance burden varies significantly by industry. Based on ThreatSafe's sector experience, here are the key additional considerations for the three highest-risk verticals

## Banking, Financial Services, and Insurance (BFSI)



## Healthcare




## E-Commerce and Consumer Tech

# 10.

# Common Mistakes ThreatSafe Finds During Gap Assessment

In **ThreatSafe's** experience conducting DPDP gap assessments across Indian enterprises, the same mistakes appear repeatedly. Awareness of these patterns helps organizations prioritize correctly.

| Common Mistake | Why It Matters and What to Do Instead |
|---|---|
| Assuming ISO 27001 = DPDP compliance | ISO 27001 addresses information security. DPDP adds legal obligations around consent, rights, and governance that ISO 27001 does not cover. Both are needed. |
| Incomplete data mapping | Organizations map only obvious data (CRM, databases) but miss shadow IT, analytics tools, email systems, and offline-to-digital data. Start with a comprehensive data flow discovery exercise. |
| Blanket consent in T&Cs | Embedding consent in terms and conditions does not constitute valid DPDP consent. Consent must be separate, purpose-specific, and unambiguous. |
| Ignoring Data Processors | Organizations focus on their own obligations but fail to ensure their vendors, cloud providers, and SaaS tools comply. Under DPDP, you remain responsible for your processors' compliance. |
| No Data Principal rights workflow | Most organizations have a privacy policy that mentions rights but no actual process to receive, verify, and respond to rights requests within required timelines. |
| Treating DPDP as a one-time project | DPDP compliance is a continuous obligation. Consent must be refreshed when purposes change. DPIAs must be reviewed periodically. Policies must evolve with the business. |

# 11. ThreatSafe's 90-Day DPDP Implementation Roadmap

Based on ThreatSafe's compliance engagements, we have developed a phased 90-day roadmap that takes an organization from no compliance program to a defensible, documented DPDP-ready posture. The roadmap is designed to be practical, prioritizing the highest-risk gaps first.

### Phase 1: Days 1–30 — Foundation and Discovery

| Week | Activities |
|---|---|
| Week 1–2 | **DPDP Gap Assessment:** Evaluate current state against all DPDP obligations. Identify and prioritize gaps by risk level. |
| Week 2–3 | **Data Mapping:** Conduct comprehensive personal data inventory. Map data flows across all systems, third parties, and international transfers. |
| Week 3–4 | **Stakeholder Alignment:** Brief leadership on DPDP obligations, penalties, and compliance roadmap. Assign DPO/Compliance Officer responsibilities. |

### Phase 2: Days 31–60 — Core Controls Implementation

| Week | Activities |
|---|---|
| Week 5–6 | **Consent Management:** Design and implement consent collection interfaces, preference centre, and consent repository across all data touchpoints. |
| Week 6–7 | **Privacy Notices:** Draft clear, plain-language privacy notices for all data collection points. Legal review and sign-off. |
| Week 7–8 | **Data Principal Rights:** Build and test workflows for access, correction, erasure, and grievance requests. Train customer-facing teams. |
| Week 8 | **Vendor Agreements:** Audit and update Data Processing Agreements with all vendors and processors to include DPDP-required clauses. |

## Phase 3: Days 61–90 — Governance, Testing, and Readiness

| Week | Activities |
|---|---|
| Week 9–10 | **DPIA:** Conduct Data Protection Impact Assessments for the three highest-risk processing activities identified in Phase 1. |
| Week 10–11 | **Breach Response Plan:** Develop and document a DPDP-aligned incident response plan including notification templates for the Board and Data Principals. |
| Week 11 | **Security Controls Review:** Map existing cybersecurity controls to DPDP security obligations. Identify and remediate critical gaps. |
| Week 12 | **Tabletop Exercise and Documentation:** Run a simulated breach scenario. Finalize compliance documentation. Conduct board-level compliance briefing. |

## Start With a Free DPDP Readiness Assessment

ThreatSafe offers a complimentary 60-minute DPDP Readiness Assessment call for qualified organizations. In this session, our compliance experts will evaluate your top three compliance risks and provide immediate actionable guidance, no cost, no obligation.

12

# How ThreatSafe Helps


ThreatSafe offers an end-to-end DPDP compliance service, from initial gap assessment to ongoing compliance monitoring. Our team combines legal, technical, and organizational expertise to deliver a compliance program that is defensible, sustainable, and built for your specific business context.

| ThreatSafe Service | What We Deliver |
|---|---|
| **DPDP Gap Assessment** | Comprehensive evaluation of your current posture against all DPDP obligations. Prioritized remediation roadmap with effort estimates. |
| **Data Mapping and Flow Analysis** | End-to-end personal data inventory across systems, third parties, and international transfers. Maintained as a living document. |
| **Consent Management Implementation** | Technical design and deployment of consent collection, repository, and preference management systems. |
| **DPIA Execution** | Facilitated DPIA workshops, risk assessments, and documented DPIA reports for your highest-risk processing activities. |
| **DPO-as-a-Service** | For organizations that need ongoing Data Protection Officer services without a full-time hire — ThreatSafe provides certified DPO expertise on retainer. |
| **Breach Response Planning** | DPDP-aligned incident response plan development, template creation, and tabletop exercise facilitation. |
| **Ongoing Compliance Monitoring** | Quarterly compliance reviews, policy updates, consent health checks, and regulatory update briefings as DPDP Rules are published. |

# Five Things to Do Starting Today

DPDP compliance is not a technology problem, it is a governance, legal, and organizational problem that requires a technology solution. Organizations that treat it as solely an IT project will fail. Those that build it into their operating model will not only comply, they will build genuine competitive advantage through customer trust.

## Here are the five most important actions to take immediately:

01 **Conduct a DPDP Gap Assessment:** You cannot build a compliance program without knowing where you stand. Start with ThreatSafe's gap assessment methodology or engage ThreatSafe directly.

02 **Map your data flows:** You cannot protect or govern what you cannot see. Commission a comprehensive data mapping exercise that covers all systems, vendors, and international transfers.

03 **Audit your consent mechanisms:** Review every data collection point in your products and services. Replace bundled or implied consent with purpose-specific, freely given consent mechanisms.

04 **Review vendor contracts:** Identify every vendor that processes personal data on your behalf and ensure your contracts include DPDP-compliant Data Processing Agreement clauses.

05 **Build your breach response plan now:** A breach without a response plan is a compliance catastrophe. Draft your notification templates, identify your response team, and run a tabletop exercise before you need it.

# About ThreatSafe

ThreatSafe is a next-generation cybersecurity company offering VAPT, compliance advisory, virtual CISO services, blockchain investigation, and security training company. We are a CERT-In empanelled organization trusted by enterprises across BFSI, healthcare, e-commerce, and government to build and sustain robust security programs.


## Our DPDP Advisory Services

- DPDP Gap Assessment and Remediation Roadmap
- Data Mapping and Flow Analysis
- Consent Management System Design and Implementation
- Data Protection Impact Assessments (DPIA)
- DPO-as-a-Service for organizations requiring ongoing privacy leadership
- Breach Response Planning and Tabletop Exercises
- Employee DPDP Awareness Training via CeroLabs
- Vendor and Third-Party DPDP Compliance Audits

*This whitepaper is published for informational purposes. It does not constitute legal advice. Organizations should consult qualified legal counsel for advice specific to their situation.*

*© 2026 ThreatSafe.ai All rights reserved.*