

DPDPA COMPLIANCE PLATFORM

The complete control plane for India's data privacy law.

One AI-powered platform for the full DPDPA lifecycle – consent, discovery, DSAR, vendor risk, AI governance, breach response, and board-ready reporting. Built by CYBERSEC Enterprises. Recognised by MeitY among India's top 6 DPDPA solutions.

30+ MODULES IN ONE PLATFORM	7,000+ PRE-BUILT INTEGRATIONS	99.9% AI ACCURACY ON PIAS
< 2 wk TIME TO GO-LIVE (SAAS)	500+ ENTERPRISES TRUST DATADEFEND	22 INDIAN LANGUAGES SUPPORTED

• THE DPDPA MOMENT

Compliance is no longer a project. It's a control plane.

India's Digital Personal Data Protection Act, 2023 and the Draft Rules, 2025 reset the cost of getting privacy wrong. Penalties run up to **₹250 Crore** per contravention, deadlines for breach notification compress to **72 hours**, and the May 13, 2027 enforcement window leaves no room for spreadsheets, point tools, or "we'll figure it out at audit." DataDefend collapses the entire DPDPA obligation set – consent, discovery, DSAR, vendor risk, AI governance, retention, breach, grievance, SDF, cross-border – into one platform.

THE FOUR PROBLEMS MOST ORGANISATIONS STILL HAVE



No idea where personal data lives

Names, Aadhaar, PAN, health and financial data are spread across hundreds of databases, SaaS apps, file shares, and vendor systems. Without an automated map, ROPA is fiction and breach scope is unknowable.



Manual consent & DSAR processes

Spreadsheets and inboxes don't scale to lakhs of data principals. One missed 30-day SLA becomes a regulatory finding, a fine, and a public trust event.



Unmanaged third-party risk

Processors and sub-processors touch your personal data without DPAs, without scoring, without continuous monitoring. Their breach becomes *your* compliance failure under DPDPA.



AI & ML models in a regulatory blind spot

AI systems consume personal data without consent linkage, lineage, or risk classification. The new DPDPA regime – and the world's tightening AI rules – require formal AI governance, not goodwill.

₹250 Cr

Max DPDPA penalty

72 hrs

Breach notify window

30 days

DSAR response SLA

May 2027

Enforcement deadline

• EIGHT FUNCTIONAL DOMAINS · 30+ MODULES

What's inside DataDefend.

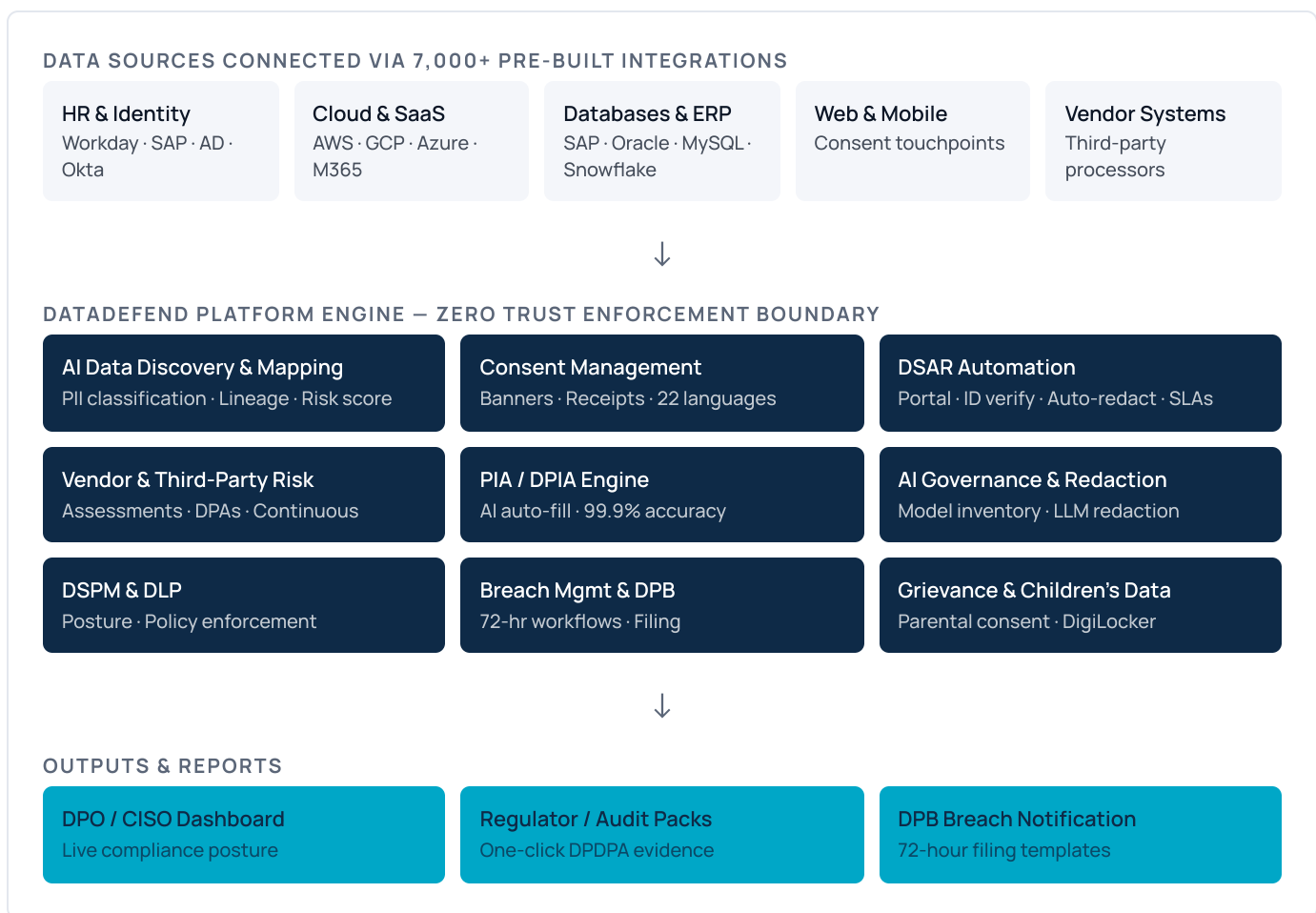
DataDefend is not a single tool with a couple of features – it is a full compliance suite. The platform is organised into eight functional domains, each containing the modules your DPO, CISO, legal team, and engineering leaders touch every day.

01	Compliance & Assessments Dashboard · AI Compliance · AI Governance · Policy Management · Compliance · Risk Management · PIA & DPIA	p. 05
02	Data Governance Data Discovery & Classification · Data Inventory · Data Retention · AI Redaction	p. 06
03	Consent & Notices Consent · Privacy Notices · Cookie & Preferences	p. 07
04	Data Subject Rights DSAR · Grievance Redressal · Children's Data	p. 08
05	Regulatory DPB Tracker · Significant Data Fiduciary · Cross-Border Transfer	p. 09
06	Security & Data Protection Security Safeguards · Breach Management · Vendor Risk · DSPM · DLP · Privacy-Enhancing Tech	p. 10
07	Admin & Operations DPO Management · Analytics · Reports · Alerts · Settings	p. 11
08	Integrations, Deployment & Coverage 7,000+ connectors · SaaS / Private Cloud / On-Premises · DPDPA, RBI, IRDAI, SEBI, ISO 27701, GDPR	p. 12

• HOW DATADEFEND WORKS

AI-powered. Non-invasive. Integration-first.


DataDefend connects to the infrastructure you already run via 7,000+ pre-built connectors – without modifying a single target system. The AI engine scans, classifies, and maps personal data in real time, and every downstream module (consent, DSAR, vendor risk, PIA, AI governance) operates against that live map.




99.9% AI PIA accuracy	7,000+ Connectors day 1	< 8 wks Audit-ready	500+ Enterprise customers
---------------------------------	-----------------------------------	----------------------------------	-------------------------------------

01 Compliance & Assessments


The control room – every obligation, every assessment, one score.

 **Dashboard** LIVE


Real-time DPDPA posture score across all 10 obligations. Compliance score, active consents, pending DSARs, open violations, and module health surfaced in one view for DPO, CISO, and board.

 **AI Compliance** NEW


Automated mapping of AI/ML systems against the EU AI Act, India's MeitY AI advisories, and DPDPA obligations. Risk tiering, bias & fairness checks, and consent-linkage tests for every model in production.

 **AI Governance** NEW


Living inventory of every model, dataset, and prompt template – with owner, purpose, training-data lineage, approval status, and an audit log of every change for regulator and internal review.

 **Policy Management**


Centralised library of privacy, retention, AI use, vendor, and incident-response policies. Version control, attestation tracking, approval workflows, and automatic distribution to the right business units.

 **Compliance Engine**

Pre-built control catalogues for DPDPA, ISO 27701, GDPR, RBI, SEBI, IRDAI. Maps every implemented control to its source obligation; flags gaps with prioritised remediation tasks.

 **Risk Management**

Continuous risk register – privacy, security, vendor, AI. Likelihood × impact scoring, treatment plans, owners, SLA timers, and trend-over-time charts for board-level risk reporting.

 **PIA & DPIA** 99.9% AI ACCURACY

Privacy and Data Protection Impact Assessments auto-populated by the AI engine using data extracted from your live data map. Pre-built templates cover every DPDPA obligation; assessors review and approve rather than fill from scratch – cutting PIA time from weeks to hours.

WHY THIS MATTERS

Single source of compliance truth
No more siloed spreadsheets across legal, IT, and security teams.

Audit-ready, always
One-click evidence packs for regulator queries and board reviews.

AI & privacy under one roof
Built for the next wave of regulation – not just today's checklist.

Risk you can defend
Quantified, scored, owned. Not vibes.

02 Data Governance

Know what you have, know where it lives, know when to delete it.

OUTCOMES

Living data map from Day 1

No 6-month "data inventory project."

Auto-built ROPA

Always current. Always exportable in regulator format.

Purpose limitation, enforced

Detection & blocking of out-of-purpose access in real time.

Retention without spreadsheets

Policy-driven deletion across structured & unstructured stores.

Data Discovery & Classification

AI engine scans every connected system and classifies PII – Aadhaar, PAN, health, financial, biometric, children's data, sensitive personal data. Each record tagged with sensitivity, purpose, lineage, and risk score.

Data Inventory

The "living ROPA" – every data flow from collection to processing to transfer is auto-mapped, documented, and refreshed as your infrastructure changes. Searchable by purpose, system, principal type, and category.

Data Retention

Retention policies per data category, processing purpose, and regulator. DataDefend monitors timelines, triggers alerts, and dispatches automated deletion workflows across structured DBs and unstructured stores. Enforces the 1-year minimum log retention under DPDP Rules 2025.

AI Redaction NEW

Auto-redact PII from documents, contracts, support tickets, screenshots, and LLM prompts before they leave the trust boundary. Configurable per category – full mask, partial reveal, or pseudonymisation – with a full audit log of every redaction event.

WHAT GETS CLASSIFIED

Direct identifiers

Aadhaar, PAN, passport, voter ID, driving licence, mobile, email

Sensitive PII

Health records, financial accounts, biometric, location, sexual orientation

Children's data

Records of data principals < 18, triggers parental-consent workflows

Behavioural & tracking

Cookies, device IDs, browsing history, marketing attributes

Employment & HR


Payroll, benefits, performance, background checks

Unstructured


Documents, spreadsheets, images, audio transcripts, call recordings

03 Consent & Notices


Verifiable, vernacular, granular – across every touchpoint a citizen sees.

 **Consent** 3.47L ACTIVE

DPDPA-compliant consent banners and preference centres in minutes. Granular per-purpose toggles, full audit trail, and a tamper-proof ledger of cryptographically signed receipts – searchable by principal, purpose, and date for any regulator query.

 **Privacy Notices**

Branded, multilingual privacy notices generated from a single source of truth. Notice content stays in sync with your live data map and processing purposes – change a purpose, every notice updates.

 **Cookie & Preferences**

Auto-scan every cookie and tracker on your web properties. Deploy a compliant banner with granular categories (necessary, analytics, marketing), record consent into the central ledger, and propagate signals through GTM, Adobe Experience Platform, Tealium, and Segment.

DESIGNED FOR

CMOs & product
Banner SDKs that don't break conversion or A/B tests.

DPOs & legal
Receipts that hold up in a regulator review.

Engineering
REST, webhooks, SDKs for web, iOS, Android, server-to-server.

22 INDIAN LANGUAGES, OUT OF THE BOX

- HINDI
- BENGALI
- MARATHI
- TELUGU
- TAMIL
- GUJARATI
- KANNADA
- ODIA
- MALAYALAM
- PUNJABI
- ASSAMESE
- URDU
- SANSKRIT
- MAITHILI
- SANTALI
- KASHMIRI
- NEPALI
- KONKANI
- SINDHI
- DOGRI
- MANIPURI
- BODO

ANATOMY OF A DATADEFEND CONSENT RECEIPT

FIELD	WHAT IT CAPTURES
Principal identifier	Pseudonymous ID linked to the data principal record
Purpose & notice version	Declared processing purposes scoped to your ROPA, plus the exact privacy notice version shown at the moment of consent
Timestamp, channel & signature	Cryptographic signature, locale, channel (web, mobile, IVR, branch, partner), and tamper-evident ledger entry

04 Data Subject Rights

Every right under the DPDPA – fulfilled, redressed, audit-logged.

SLAS YOU CAN DEFEND

30-day DSAR window

Extendable to 45 days under DPDPA – auto-tracked, never missed.

Grievance escalation

Mandatory ladder to the DPB if unresolved.

Parental verification

DigiLocker, govt-authorized sources, existing records.



DSAR

3 PENDING

Branded principal portal supporting access, correction, erasure, nomination, and grievance requests. Identity verification automated. DataDefend locates all personal data of the requester across every connected system, auto-redacts third-party data, and packages the response. For erasure, deletion workflows dispatch to all relevant systems automatically.



Grievance Redressal

4 OPEN

A dedicated grievance officer console with case management, escalation paths, communication templates, and a complete record of resolution timelines. Escalates automatically to the Data Protection Board if statutory windows are breached.



Children's Data

Workflows for verifying parental consent for users under 18, as mandated by DPDP Rules 2025. Supports self-declaration by the child with subsequent parent verification via DigiLocker, existing records, or government-authorized sources. Behavioural tracking and targeted advertising are blocked for child accounts by policy – every event audited.

A DSAR, END TO END

1 · **Submit**
Principal portal, vernacular

2 · **Verify**
Auto ID check

3 · **Discover**
PII across systems

4 · **Redact**
Third-party data masked

5 · **Fulfil**
Package + audit log

05

Regulatory

Filings, classifications, and cross-border transfers under DPDPA.



DPB Tracker

Central register of every interaction with the Data Protection Board – breach notifications, regulatory queries, advisories, deadlines, and filings. Each item has owner, status, evidence pack, and full correspondence log. No more "where is that email?" during an inquiry.



Significant Data Fiduciary

Built-in workflows for the additional obligations that apply to SDFs under DPDPA: independent DPO appointment, annual data audit, DPIA for high-risk processing, and government-notified algorithmic transparency. Status surfaced on the compliance dashboard.



Cross-Border Transfer

Country-by-country adequacy register reflecting the government's notified list of restricted jurisdictions. Standard Contractual Clauses library, transfer impact assessments, and consent capture for transfers that require it – with continuous monitoring as the notified list changes.

TRACKS FOR YOU

DPB filings

72-hr breach forms · advisories · queries.

Notified-jurisdiction list

Auto-refresh as government updates.

SDF designation

Triggers the extra obligation set automatically.

Regulator changes







Alerts when DPDPA Rules, RBI, SEBI, IRDAI move.

THE 10 DPDPA OBLIGATIONS, ALL IN ONE PLACE

- 1 **Lawful, fair processing** with valid consent or legitimate use.
- 2 **Notice** in clear language, before consent is taken.
- 3 **Purpose limitation** & data minimisation.
- 4 **Accuracy** of personal data on record.
- 5 **Storage limitation** – retention only as long as needed.
- 6 **Security safeguards** appropriate to risk.
- 7 **Breach notification** to the DPB & affected principals.
- 8 **Children & persons with disability** protections.
- 9 **Data principal rights** & grievance redressal.
- 10 **SDF** additional obligations where notified.

06 Security & Data Protection

The technical safeguards DPDPA mandates — and a posture you can actually measure.

<p> Security Safeguards</p> <p>Pre-built control library mapping DPDPA's "reasonable security safeguards" obligation to ISO 27001, NIST CSF, and CIS controls. Evidence collection automated from your SIEM, IAM, EDR, and ticketing systems.</p>	<p> Breach Management 1 OPEN</p> <p>Incident triage console with 72-hour timer, DPB notification template, principal communications, root-cause tracking, and post-incident lessons-learned. Pulls scope automatically from the live data map.</p>	<p> Vendor Risk 5 ACTIVE</p> <p>Automated questionnaires to processors and sub-processors, risk scoring, DPA contract library, continuous monitoring, and renewal alerts. Replaces point-in-time spreadsheet reviews with a living vendor posture.</p>
<p> DSPM <small>DATA SECURITY POSTURE</small></p> <p>Continuous discovery of misconfigured stores, overexposed datasets, shadow data, and risky access patterns across cloud and on-prem. Each finding ranked by data sensitivity from the AI classifier.</p>	<p> Data Loss Prevention</p> <p>Egress controls for email, endpoint, SaaS, and cloud storage — driven by classifier output, not regex. Blocks Aadhaar / PAN / cardholder / health data leaving sanctioned channels and routes incidents into the breach workflow when needed.</p>	<p> Privacy-Enhancing Tech <small>NEW</small></p> <p>Built-in toolkit for tokenisation, pseudonymisation, format-preserving encryption, differential privacy, and secure multi-party computation. Apply at ingest, at rest, or at query time — without re-architecting downstream systems.</p>

POSTURE, NOT POINT-IN-TIME

Every module above feeds a single, real-time **Data Protection Posture Score**. Roll it up to the board. Drill it down to a vendor, a database, an AI model, or a single record. When a control degrades, the score moves before the regulator does.

<p>72 hr</p> <p>Breach SLA tracked automatically</p>	<p>100%</p> <p>Vendor coverage with DPA library</p>	<p>6 PETs</p> <p>Privacy-enhancing techniques shipped</p>	<p>24/7</p> <p>DSPM scanning across cloud + on-prem</p>
---	--	--	--

07

Admin & Operations

The day-to-day surface for DPOs, compliance teams, and platform admins.



DPO Management

Profiles for primary DPO, deputies, grievance officers, and business-unit privacy champions. Delegation, vacation cover, and signing authority captured – so the DPB sees the right name on every notification.



Analytics

Trends across consents, DSARs, violations, vendor scores, and AI model risk. Cohorts by business unit, region, and data principal type. Slice by month, quarter, or campaign for board reporting.



Reports

Pre-built templates for board, DPO, CISO, internal audit, and external auditor. Scheduled delivery, digital-signed PDF exports, and one-click "evidence pack" bundles for regulator queries.



Alerts

7 UNREAD

Unified alert centre across consent violations, DSAR deadlines, breach detections, vendor risk changes, and compliance-score deltas – routed to Slack, Teams, PagerDuty, Opsgenie, email, or SMS.



Settings · API & Keys · SSO & RBAC

SAML 2.0 / OAuth 2.0 / OIDC SSO with Azure AD, Okta, Google Workspace, Ping. Role-based access control separates DPO, CISO, legal, business-unit, and read-only roles. Full REST API + webhooks for everything the UI does – so your IT, DevOps, and compliance pipelines can automate against DataDefend natively.

OPERATIONAL TRUTHS

Tenant isolation

Each customer cryptographically isolated.

Audit log is immutable

Tamper-evident, signed, exportable.

99.9% uptime

SLA backed across SaaS deployments.

Bring your own KMS

AWS KMS, Azure Key Vault, HSM-backed keys.

08

Integrations & Technology Fit

7,000+ connectors. Zero modification to your target systems.

DataDefend is built to drop into the infrastructure you already run. Pre-built connectors cover every data source category, and the platform exposes a full REST API and webhooks so your IT, DevOps, and compliance teams can automate everything they need – with zero modification to target systems.

CATEGORY	SUPPORTED TECHNOLOGIES
ERP & CRM	SAP S/4HANA, SAP ECC, Oracle ERP, Microsoft Dynamics 365, Salesforce, HubSpot, Zoho CRM – schema-aware PII scanning and real-time data lineage mapping.
Databases	MySQL, PostgreSQL, Oracle DB, MS SQL Server, MariaDB, MongoDB, Redis, ClickHouse, Cassandra, Snowflake, BigQuery, Amazon Redshift.
Cloud & infrastructure	AWS (S3, RDS, DynamoDB, Redshift, Lambda), GCP (GCS, BigQuery, Cloud SQL), Azure (Blob, Azure SQL, Cosmos DB), Alibaba, Oracle Cloud – with cross-region residency mapping.
HR & workforce	SAP SuccessFactors, Workday, Oracle HCM, BambooHR, ADP, Darwinbox, greythR – with Joiner-Mover-Leaver lifecycle triggers.
Identity & directory	Active Directory, Entra ID, Okta, Google Workspace, Ping, OneLogin – SAML 2.0 / OAuth 2.0 / OIDC.
Web & tag management	Google Tag Manager, Adobe Experience Platform, Tealium, Segment – automatic cookie and tracker scanning with consent-signal propagation.
ITSM & ticketing	ServiceNow, Jira Service Management, BMC Remedy, Freshservice, Zendesk – DSAR, PIA, vendor, and breach workflows wired into your existing SLAs.
Communication	Microsoft Teams, Slack, Google Chat, PagerDuty, Opsgenie – plus REST API + webhooks for custom automation.
SIEM & SOC	Splunk, IBM QRadar, Microsoft Sentinel, Elastic SIEM, Datadog, Sumo Logic – syslog/CEF/JSON streaming of all DataDefend compliance events.
File & document stores	SharePoint, OneDrive, Google Drive, Box, Dropbox, Confluence, network file shares – unstructured PII discovery with classification.
AMI & IoT (utilities)	Smart meter platforms, IoT device management – edge-enforced consent and retention for consumer energy data.

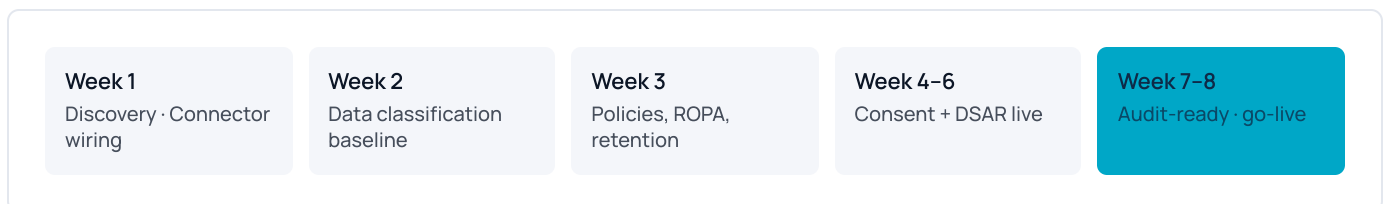
• DEPLOYMENT & ONBOARDING

Pick the topology that fits your data-residency posture.

DataDefend is platform-agnostic. The AI engine, policy model, and full feature set are identical across all three options. Every enterprise deployment ships with a dedicated Project Manager and an On-Premises Implementation Resource.

MODEL	DESCRIPTION	BEST FOR
SAAS	Fully managed multi-tenant deployment on the DataDefend cloud. Zero infrastructure to operate. Automatic upgrades, patching, 99.9% SLA. Go live in under 2 weeks.	Fastest time-to-value · SaaS-first compliance teams · mid-market enterprises seeking rapid DPDPA certification.
PRIVATE CLOUD	DataDefend deployed in your own AWS, GCP, or Azure VPC — isolated single-tenant environment. All personal data and compliance records stay within your cloud boundary. Managed by DataDefend engineering.	Regulated workloads requiring data residency within India · cloud-first policies with strict isolation.
ON-PREMISES	Full control plane and data plane deployed within your own data centre or private network. No data leaves your perimeter. DataDefend's on-prem resource handles installation, configuration, and go-live alongside your IT team.	BFSI · defence · government · healthcare · critical infrastructure · sovereign data & air-gapped requirements.

ONBOARDING TIMELINE



Timelines reflect the SaaS deployment with a single business unit at scope. Private Cloud and On-Prem add 1-3 weeks for environment provisioning depending on your change-management calendar.

● FRAMEWORKS MAPPED

One platform. Six regulatory regimes. Zero spreadsheets.

FRAMEWORK / REGULATION	DATADefEND COVERAGE
DPDP Act 2023 & Rules 2025	Full coverage of all 10 mandatory obligations – consent, principal rights, security safeguards, vendor management, breach notification, retention, grievance redressal, parental consent, SDF, ROPA. Enforcement tracking to May 13, 2027.
RBI guidelines (data localisation)	Payment data localisation controls, residency mapping, cross-border transfer consent aligned with RBI Payment System Data Storage directives.
SEBI cybersecurity & data framework	Investor and client data classification, third-party vendor risk, and breach notification workflows aligned with SEBI's cybersecurity and data privacy circulars.
IRDAI data privacy guidelines	Policyholder and beneficiary data governance, health data classification, sensitive personal data consent, and vendor risk for insurance intermediaries.
ISO 27001 / ISO 27701	Privacy Information Management System (PIMS) control mapping with automated evidence collection. ISO 27701 annex controls mapped directly to DataDefend modules.
GDPR (cross-border transfers)	Standard Contractual Clauses template library, cross-border transfer impact assessments, adequacy decision monitoring for India ↔ EU transfers.
EU AI Act & MeitY AI advisories	AI system inventory, risk-tier classification, bias & fairness testing, transparency disclosures, and consent-linkage for training datasets.

<p>10/10 DPDPA obligation pillars covered</p>	<p>7 Frameworks mapped out-of-the-box</p>	<p>1-click Audit evidence pack export</p>
--	--	--

• BUSINESS IMPACT

What DataDefend changes for your business.



90% less manual compliance overhead

PIA filling, DSAR fulfilment, vendor questionnaires, consent banner upkeep, audit report generation – all automated. Legal & compliance teams shift from reactive firefighting to proactive governance, without growing headcount.



Audit-ready in under 12 weeks

Pre-built DPDPA templates, AI-automated assessments, and a dedicated implementation resource get you from zero to defensible well ahead of the May 2027 deadline.



Third-party risk under control

Continuous, scored, contracted vendor oversight replaces point-in-time questionnaires. A processor breach stops being your compliance failure under DPDPA.



One platform, not nine tools

DataDefend replaces standalone consent tools, DSAR trackers, spreadsheet inventories, ad-hoc vendor assessments, and cookie management – cutting TCO and producing a posture board, regulators, and customers can see in real time.

Start with a no-cost DPDPA readiness assessment.

Our team will benchmark your current posture against all 10 DPDPA obligations, identify the gaps that matter most, and map a 12-week path to audit-ready.

[Book an assessment →](#)