PUBLIC

PREPARED BY

Intelliroot
SECURITY SIMPLIFIED

BROCHURE · 2026

PRIVIO . India's Complete Data Protection Compliance Platform

End-to-end DPDP Act compliance — consent lifecycle and multilingual notices, vendor DPA e-signature, breach notification, and no-code workflow automation. Deployed as managed SaaS or entirely inside your client's network.

CONSENT | DP RIGHTS | VENDORS & DPA | BREACH | AUDIT | AUTOMATION

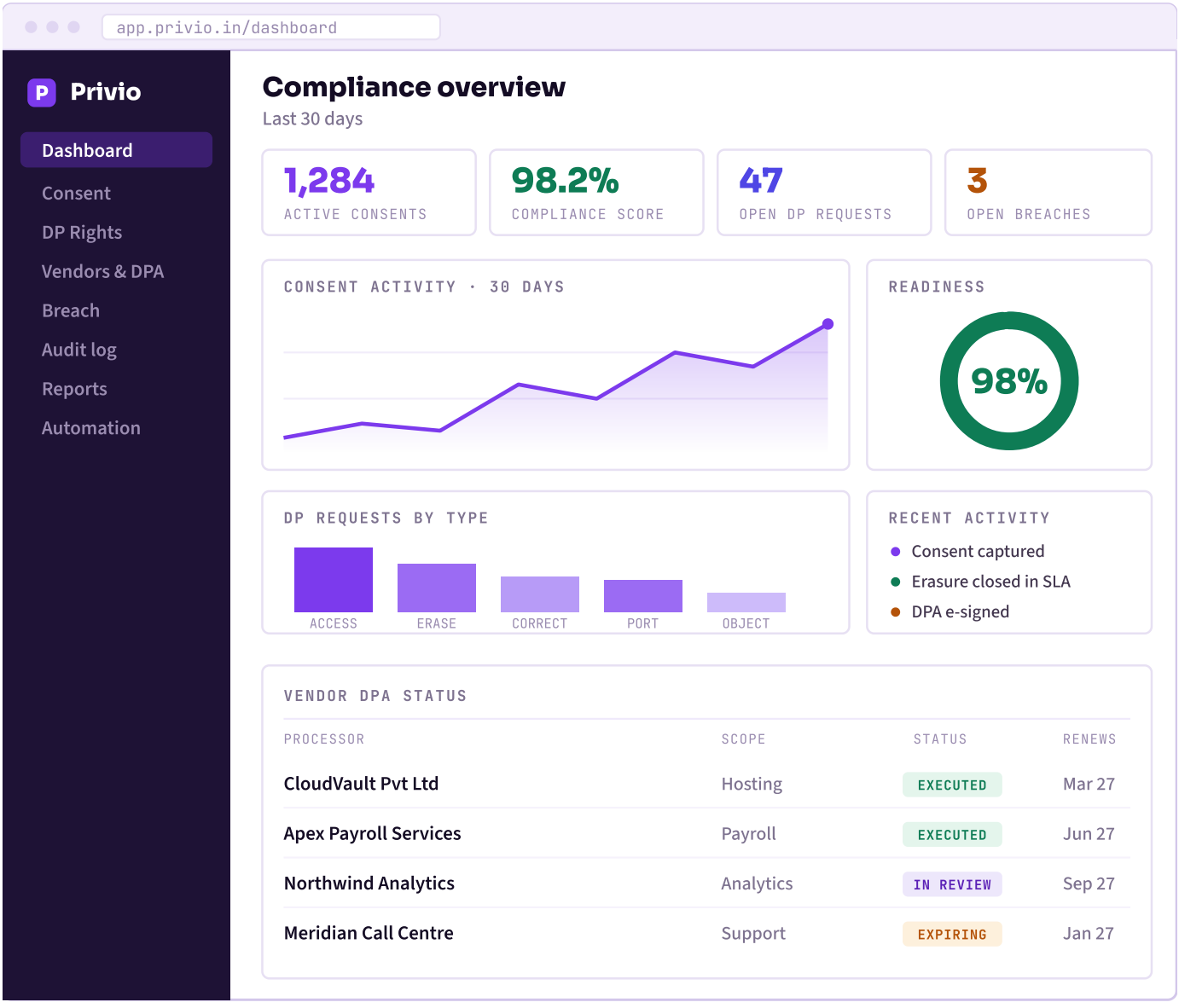
COMPLIANCE MODULES	DEPLOYMENT	FIRST REPORT
11	SaaS or on-prem	Under 30 min

SECTION 01

One platform, every obligation

Built ground-up for the Digital Personal Data Protection Act — not a GDPR product retrofitted to India. Every module writes to a shared, immutable audit backbone, so a compliance report is a query, not a project.

11	22	< 2 hrs	< 30 min
CORE COMPLIANCE MODULES	INDIAN LANGUAGES FOR NOTICES	TYPICAL CLIENT DEPLOYMENT	GO-LIVE TO FIRST COMPLIANCE REPORT



WHY IT MATTERS

Most teams can describe their consent process. Far fewer can **produce the evidence on demand** — who consented, to what version of which notice, on what date, and what changed since. That is the gap Privio closes.

SECTION 02

Everything the Act demands, in one place

Eight capability areas covering every obligation a Data Fiduciary faces — from the first notice shown to a data principal, through to the report a regulator asks for.

CAPABILITY	WHAT IT DOES
Consent lifecycle	Granular, versioned consent records with full chain of custody. Consent-form builder, multilingual notices in 22 Indian languages via Bhashini, branded receipts, and re-consent flows. CONSENT REGISTER · FORM BUILDER · 22 LANGUAGES · RECEIPTS
Data principal rights	One queue for every right the Act confers — access, erasure, correction, portability, restriction, objection and the right to know — with per-request SLA countdowns. SLA TIMERS · AUTO NOTIFICATIONS · AUDIT LOGS
Vendor risk & DPA	Version-controlled DPA templates, internal review and multi-approver sign-off, redline negotiation, dual e-signature with an executed PDF, and automatic re-signature when the data scope drifts. E-SIGNATURE · REDLINING · RISK SCORING
Breach notification	Structured incident recording, authority notification inside the statutory window, automated dispatch with delivery confirmation, and a complete response timeline. AUTHORITY EMAIL · DELIVERY STATUS · INCIDENT TIMELINE
Reports & audit log	One-click PDF compliance reports with executive summaries, immutable event history with actor attribution, and regulator-ready exports. COMPLIANCE PDF · AUDIT TRAIL · CERTIFICATION BLOCK
Scope & purpose mapping	Define and version processing scopes, map data elements to legal purposes, flag cross-border transfers, and detect automatically when a scope change requires fresh consent. SCOPE VERSIONING · RE-CONSENT TRIGGER
Self-service portal	White-labelled public portal where data principals manage consents and raise requests — token verified, no account required. WHITE-LABEL · TOKEN AUTH · CONSENT CENTRE
Automation & API	No-code workflow builder with durable execution, AI nodes, reusable sub-workflows, human-task steps and webhooks — plus a full REST API to embed consent capture into any app or CRM. WORKFLOW BUILDER · AI NODES · WEBHOOKS · REST API

BUILT FOR INDIA'S REGULATORY REALITY

Pre-mapped to the obligations that actually bite: **consent and notice, the rights queue, processor contracts, and the breach clock** — with the evidence trail each of them assumes you are keeping.

SECTION 03

Purpose-built modules, one audit backbone

Each module answers a specific obligation. All of them write to the same immutable event log, which is what makes a cross-module report possible at all.

01 · CONSENT ENGINE

Capture to withdrawal

- Purpose-level consent records
- Notices in 22 languages
- Form builder and receipts
- Re-consent on scope change
- Self-service withdrawal

02 · DP RIGHTS HUB

One queue, every right

- Access, erasure, correction
- Portability and restriction
- Objection and right to know
- SLA countdown per request
- Full history per request

03 · VENDOR HUB

Processors under contract

- Versioned DPA templates
- Dual e-signature, executed PDF
- Review and multi-approver flow
- Redline negotiation
- Questionnaires and risk scoring

04 · BREACH CENTRE

The clock, managed

- Severity classification
- Automated authority notice
- Delivery confirmation
- Affected-principal counts
- Response report as PDF

05 · AUDIT LOG

Nothing changes quietly

- Actor, target and timestamp
- Before and after deltas
- IP and session attribution
- Filter by type, actor, date
- Event drill-down

06 · REPORTS

Evidence on demand

- Compliance posture report
- Vendor risk summary
- Breach documentation
- Consent trend analytics
- Signed certification block

OBLIGATIONS COVERED

- Notice, consent and withdrawal
- Data Fiduciary obligations and security safeguards
- The data principal rights set, end to end
- Children's data and verifiable parental consent
- Personal data breach notification
- Cross-border transfer records

DEPLOYMENT OPTIONS

- **Managed SaaS** — zero infrastructure overhead
- **On-premise** — data never leaves the client network
- **Private cloud** — AWS, Azure or GCP
- **Containerised** — portable and scalable
- **White-label OEM** — partner branding throughout
- Multi-tenant: many client organisations, one deployment

SECTION 04

How we compare to the alternatives

A feature-by-feature comparison against leading global privacy tools and the manual approach, judged on India-specific requirements rather than on GDPR feature parity.

CAPABILITY	PRIVIO	GLOBAL SUITES	ERP MODULES	POINT TOOLS	MANUAL
DPDP-native consent model Purpose-level records built to the Indian Act, not mapped from GDPR	✓	-	✗	-	✗
Notices in 22 Indian languages Bhashini-backed translation with versioned notice records	✓	✗	✗	✗	✗
Breach notification workflow Authority dispatch inside the statutory window, with delivery proof	✓	-	✗	✗	✗
Vendor DPA e-signature and redlining Negotiate, approve and execute without leaving the platform	✓	-	-	✗	✗
On-premise deployment Data never leaves the client network — decisive for regulated sectors	✓	✗	-	✗	-
Immutable audit trail across modules One event log behind consent, rights, vendors and breach	✓	✓	-	✗	✗
White-label multi-tenant OEM Serve many client organisations from one deployment, branded per tenant	✓	✗	✗	✗	✗
India-local implementation support Advisory, onboarding and ongoing regulatory guidance in your timezone	✓	-	✗	-	✗
Pricing built for the Indian market Rupee pricing, per seat, per client or OEM licence	✓	✗	-	-	-

✓ Fully supported - Partial, or needs custom configuration ✗ Not available

VS. GLOBAL PRIVACY SUITES

Built for GDPR and mapped onto India afterwards. India-specific obligations need costly custom configuration, there is no on-premise option, and dollar pricing puts them out of reach for the mid-market.

VS. ERP COMPLIANCE MODULES

Generic tools cover audit and risk basics but lack a consent lifecycle, a rights queue, processor questionnaires and regulator-ready breach documentation.

VS. SPREADSHEETS

Manual tracking cannot produce an immutable trail, an SLA timer or an authority notification. One incident exposes the whole gap at once.

Comparison based on publicly available feature information. Competitor capabilities vary by edition, region and configuration.

SECTION 05

Built on trust, deployed for scale

Whether you are a consulting firm, a system integrator or an enterprise reseller, the platform is designed to be embedded into your compliance practice rather than sold alongside it.

PRINCIPLE	WHAT IT MEANS IN THE PRODUCT
Privacy by design	Consent and data flows built around minimisation and purpose limitation from the first schema, not retrofitted after a gap assessment.
Immutable audit records	Every action carries actor identity, timestamp, IP and change delta. Nothing can be edited quietly, which is the point of keeping a log at all.
Data residency ready	On-premise deployment keeps client data inside the client's own infrastructure — usually the deciding factor in regulated sectors.
API first	Full REST API with key management, so consent capture embeds into an existing CRM, app or customer portal instead of becoming a second system.
Multi-tenant	Many client organisations from one deployment, with logo, organisation name and portal colours set per tenant.
Regulator-ready output	One-click PDFs with certification blocks, reference identifiers and assessment dates, formatted for submission rather than for a slide.

ONBOARDING — FOUR STEPS

1. **Demo and scoping call**
   Thirty minutes across every module. Scope the client requirement and the deployment model.
2. **Agreement and access**
   Sign the reseller or OEM agreement. Receive a sandbox and partner documentation.
3. **Client deployment**
   Deployed in under two hours. Configure branding, mail and data scopes.
4. **Go live and first report**
   Users trained, and the first compliance report generated within thirty minutes.

WHAT'S INCLUDED

- **All 11 modules** — consent, rights, vendors and DPA, breach, audit, reports, portal, automation, notices, cookies, scope mapping
- **Built to scale** — millions of consent records, with keyset pagination and in-process caching
- **Role-based access** — DPO, admin, reviewer and read-only roles with granular permissions
- **White-label branding** — logo, organisation name and portal colours throughout
- **Dedicated partner support** — a shared channel, an onboarding engineer and quarterly reviews

NEXT STEP

A scoping conversation takes thirty minutes and commits you to nothing. We will map the modules onto your client's obligations and agree a deployment model.

PARTNERSHIP ENQUIRIES
contact@intelliroot.com

REQUEST A DEMO
www.intelliroot.com

© 2026 · All rights reserved · Confidential — for authorised partners only