Lopam PrivCon

PRIVACY & CONSENT MANAGEMENT SUITE

DPDP ACT 2023
DPDP RULES 2025

Consent you can prove, not just claim.

A platform-agnostic privacy and consent management suite for Data Fiduciaries in any sector. Every consent, withdrawal, rights request and administrative action is written into a cryptographically chained record, so compliance can be demonstrated to a regulator or auditor rather than merely asserted.

CORE CAPABILITIES

Consent management
Purpose and sub-purpose granularity. Withdraw one use without losing the rest; parent withdrawal cascades. Essential purposes protected server-side.
SEC. 6

Notice management
Multiple instruments, independently versioned per language across all 22 Eighth Schedule languages, with a completeness check on required elements.
SEC. 5

Cookie & tracker consent
Category-level banner with client-side blocking, so nothing non-essential runs before the choice is recorded. Banner version captured with every decision.
SEC. 6

Records of processing
RoPA register with maker/checker enforced in the API — an approver can never be the creator. Processor contract repository linked to activities.
SEC. 10, 19(4)

Data discovery & classification
Scans registered databases and file shares, classifies personal data against a configurable taxonomy, and flags findings with no recorded purpose.
SEC. 8–9

Rights & grievances
Access, correction, erasure, nomination and complaints, each on a 30-day clock with overdue tracking and recorded resolution.
SEC. 11–14

Breach & incident register
Severity classification with two-stage regulator notification — immediate alert, then root-cause report — plus separate data principal notification.
SEC. 8(6)

Children's data safeguards
Minor flagging with guardian linkage and recorded verification. Profiling and targeted advertising blocked at the gateway before any service sees the request.
SEC. 9

Impact assessments (DPIA)
Screening questionnaire, likelihood × impact risk scoring, mitigation tracking. An unmitigated high risk blocks an unqualified "proceed".
GOVERNANCE

Token vault & erasure
Format-preserving tokenization. Erasure destroys the individual's key, rendering copies already in downstream stores permanently unreadable.
SEC. 12

Compliance maturity
Weighted self-assessment across practice areas with live scoring, gap counts and evidence attached to each response.
ACCOUNTABILITY

Tamper-evident audit
Every event SHA-256 hashed with its predecessor. Verification walks the chain, recomputes each link and names the first break.
RULE 6

DATA PRINCIPAL SELF-SERVICE PORTAL

Consent view	Every purpose in plain language with its current state — not raw purpose codes.
Partial withdrawal	Switch off any non-essential purpose or sub-purpose individually, at any time.
Personal RoPA extract	What is collected about them, why, who else sees it and for how long — scoped to that individual.
Request & history	Raise access, correction, erasure or grievance requests and follow their progress.
Separate authentication	OTP-based principal login on an isolated path, distinct from staff access in both code and policy.

DPDP PROVISION COVERAGE

PROVISION	REQUIREMENT	HOW IT IS MET
Section 5	Notice to the data principal	Versioned multi-instrument notices, 22 languages, delivery status tracked
Section 6	Granular, withdrawable consent	Purpose/sub-purpose consent store with self-service withdrawal
Sections 7–8	Processor obligations flow-down	Contract register; termination raises a tracked deletion obligation
Section 8(6)	Breach notification	Two-stage Board notification plus separate principal notification, each timestamped
Section 9	Children's personal data	Guardian linkage and verification; profiling refused at the API gateway
Sections 11–14	Data principal rights	Access, correction, erasure, nomination, grievance — SLA tracked
Section 10, 19(4)	Records of processing	RoPA register with server-side maker/checker separation
Rule 6	Tamper-evident audit trail	Per-event SHA-256 hash chain with on-demand verification
Localisation	In-country data residency	On-premises or private-cloud deployment; no mandatory public-cloud dependency

ARCHITECTURE & DEPLOYMENT

Deployment models	On-premises, private cloud, hybrid. Designed for environments where data localisation obligations apply.
Orchestration	Kubernetes / OpenShift-class container platforms; all stateless services horizontally scalable.
Database	ANSI-SQL-compatible enterprise RDBMS (PostgreSQL, Oracle or SQL Server-class). Hash-based partitioning by data principal.
Event backbone	Kafka-compatible distributed log for consent, revocation and audit events, partitioned to preserve per-principal ordering.
Cache	Clustered in-memory cache in front of the consent-status read path.
Resilience	DC and DR sites, active-passive at deployment with an active-active upgrade path; no single point of failure.
Ingestion channels	Adapter matrix covering web, mobile, branch/paper, conversational, core-system terminals, IVR, SMS/USSD, email, kiosk and external Consent Managers.

SECURITY

Encryption	AES-256 at rest, TLS 1.3 in transit. Quantum-resistant algorithms evaluated for phased adoption.
Key management	Envelope encryption — the key manager wraps short-lived data keys rather than encrypting fields directly, so throughput is not bound to key-manager capacity. FIPS 140-3 Level 3 HSM integration via PKCS#11 or KMIP.
Tokenization	Format-preserving surrogates keep field shape and length, so downstream format validation continues to work unmodified.
Access control	Role-based and attribute-based access control; maker/checker on compliance-affecting actions, enforced in the API.
Audit	Hash-chained event log; privileged actions such as revealing a tokenized value are individually recorded.

DESIGN TARGETS AT NATIONAL SCALE

PARAMETER	TARGET
Data principals	500 million (headroom above a 350 million baseline)
Consent validation	100,000 requests/second sustained, 250,000 burst
Read latency	Under 5 ms at p99
Field encryption	200,000 TPS at under 2 ms overhead
Revocation propagation	Under 2 seconds end to end
Availability	99.99%
Retention storage	100+ TB across hot, warm and cold tiers with WORM cold storage

On these figures. The parameters above are architectural design targets that the system is engineered to meet, not benchmark results from a specific installation. Sizing, load validation and infrastructure selection are confirmed during solution design for each deployment. HSM integration, telephony and USSD channel adapters, and core-system message formats are deployment-dependent and configured against the customer's own infrastructure.

INTERFACES & EXPORT

Administrative console	Browser-based, role-governed, with light and dark themes and visual compliance reporting.
Data principal portal	Separate authenticated surface with plain-language consent presentation.
API	REST with an OpenAPI specification published by the running service.
Export formats	CSV, JSON and XML for RoPA, contracts, consent, rights, breaches, discovery findings, assessments and the audit chain. Every export is itself audited; principal identifiers are exported as hashes.