



PrivaTrust

PrivaTrust

Unified Privacy
& Data Governance Platform



Product Overview

PrivaTrust is eMudhra's unified privacy and data-governance platform. It brings consent management, third-party / vendor consent governance, Data Subject Access Request (DSAR) automation, Data Principal rights management, data discovery & classification, and find-and-fix remediation into a single platform — a privacy control plane that governs how personal data is collected, used, and honoured without replacing the systems that process it.

- PrivaTrust ships with pre-built controls, templates, and workflows for major privacy regulations worldwide — including GDPR, India's DPDP Act 2023, CCPA/CPRA, HIPAA, LGPD, PIPEDA, PDPA, POPIA, APPI, PIPL, and more. It is delivered **with full feature** parity across on-premises, private-cloud, hybrid, SaaS multi-tenant, and air-gapped deployments, and is available on a **modular** purchase basis.

Why PrivaTrust

- **One integrated suite** — six privacy modules in a single platform, no multi-vendor stitching.
- **On-premises & air-gapped with full parity** — data never has to leave your infrastructure; classification runs in-deployment.
- **DPDP-native and globally ready** — pre-built templates and Data-Protection-Board workflows, plus the major global regimes.
- **Real-time enforcement** — sub-100 ms consent verification, signed webhook propagation, and pre-consent cookie blocking.
- **Find AND fix** — discovery and classification feed remediation that encrypts, masks, and restricts access, with proof-of-fix.

PrivaTrust at glance

Attribute	Detail
Deployment models	On-premises, private cloud, hybrid, SaaS multi-tenant, and air-gapped
Purchase model	Modular — each module deployable independently
Architecture	Modular, microservices-based, event-driven; database-per-tenant isolation
Localization	25+ languages, white-label options, SI-partner ready
Data residency	Customer-controlled — on-premises and air-gapped keep data inside your infrastructure; classification SLMs run in-deployment
Feature parity	Full feature parity across every deployment model

Module Scope

Module	Summary
Consent Management (CMP)	Centralised, purpose-based consent capture, preference management, cookie consent, and lifecycle governance across every channel
Third-Party / Vendor Consent	Govern processors and partners: onboarding, due-diligence approval, DPA lifecycle, purpose mapping, and rights cascade
DSAR Management	End-to-end automation of Data Subject Access Request intake, verification, fulfilment, and closure
Data Principal Rights Mgmt (DPRM)	Rights catalogue, legal-basis & retention governance, SLA, grievance, RoPA, and DPIA
Data Discovery & Classification (DDC)	Discovery and classification across 50+ sources using a hybrid regex + Small Language Model engine
Remediation Hub	Find-and-fix remediation with encryption, masking, access control, and proof-of-fix

Module Capabilities

Module 1 — Consent Management (CMP)

- **Policy Centre** — region-driven setup: select a region and the applicable regulations auto-populate, rights auto-populate per regulation, then define purposes (with legal bases and data categories) and map vendors — all under DPO approval and version control.
- Consent profile creation with purpose-based capture via a guided six-step wizard; versioned publish lifecycle (Draft Review Approved Published).
- No-code banner & preference-modal builder; a persistent **preference centre** for ongoing self-service.
- Multi-channel capture — web SDK, mobile SDKs (iOS / Android / React Native), API / headless, agent-assisted, and email / SMS.
- Geo-targeted banners; consent expiry, re-consent and re-validation campaigns; guardian / minor consent.
- Cookie & tracker scanning with a pre-consent cookie blocker; granular consent withdrawal with real-time propagation.
- Consent Verification API for real-time allow/deny decisions; immutable consent records; machine-readable **consent receipts**; full audit trail.

Module 2 — Third-Party / Vendor Consent Management

- Central vendor & partner registry with multi-track onboarding — DPO-led, invite-to-complete (vendor self-onboarding), and discovered-queue (from cookie/tracker scans).
- Staged due-diligence approval workflow with configurable assignees and SLAs.
- DPA lifecycle — signed-agreement upload with hashing, expiry alerts, and sub-processor tracking.
- Legitimate-interest assessment (LIA); certification capture (ISO 27001, SOC 2, PCI-DSS); cross-border transfer safeguards (SCC / BCR / adequacy).
- Purpose mapping with consent or legitimate-interest enforcement tracks; role-scoped vendor self-service portal.
- Vendor DSAR cascade — fan rights requests out to vendors as tracked sub-tasks with per-vendor SLAs.
- Periodic re-assessment and continuous monitoring (DPA-expiry alerts, annual LIA re-review, completeness tracking).

Module 3 — DSAR Management

- Self-service DSAR intake portal with configurable request types and requester status tracking.
- MFA-based identity verification for requesters (email, phone, knowledge-based).
- Automated discovery of a requester's data across all connected sources, located via the data-subject correlation graph.
- Workflow orchestration with maker-checker approval; full statutory rights execution under DPRM policy.
- Per-regulation SLA deadline tracking — e.g. 30 days (GDPR), DPDP-Act timelines — with breach alerts and escalation.
- Legal-hold exclusions; regulator-specific response packs; full audit trail of the DSAR lifecycle.
- Reduces 20+ hours of manual effort to minutes per request.

Module 4 — Data Principal Rights Management (DPRM)

- Full rights catalogue across regulations — access, correction/rectification, erasure, portability, restriction, objection, opt-out of automated decision-making, grievance redressal, and nomination.
- Legal-basis lifecycle across all six lawful bases; retention schedules with retention-conflict (legal-hold) handling.
- Per-regulation SLA configuration that drives the DSAR clock; grievance-redressal workflow with Data-Protection-Board escalation tracking.
- **RoPA** (Records of Processing Activities) generated from consent, discovery, and vendor data.
- **DPIA** (Data Protection Impact Assessment) workflow with reviewer sign-off for high-risk processing.

Module 5 — Data Discovery & Classification (DDC)

Classification engine

- Hybrid engine combining regular-expression / pattern matching with Small Language Model (SLM) classification — selectable as regex-only, SLM-only, or hybrid.
- Six purpose-built SLMs run CPU-based and in-deployment — no data leaves the perimeter for classification — and can be fine-tuned on your own data.
- 99%+ classification accuracy; self-learning that reduces false positives over time; custom taxonomy support.
- Automated tagging of PII, PHI, and sensitive data; sensitivity classes (Critical / High / Medium / Low) and automated risk scoring per finding.

Scan modes (7) & sources

- Seven scan modes — Full, Incremental, Hyper, Targeted, Scheduled, On-Demand, and Real-Time.
- 50+ data sources — relational databases (MySQL, PostgreSQL, Oracle, MSSQL), NoSQL, file shares (SMB/NFS), cloud object storage (S3, Azure Blob, GCP), SharePoint/OneDrive, and SaaS connectors.
- Data mapping / lineage and a data-subject correlation (identity graph); searchable data catalog.

Module 6 — Remediation Hub

- **Find AND fix** — remediate vulnerabilities and sensitive-data exposure directly from within the platform.
- Encryption and masking of identified sensitive data; KMS / Vault integration for encryption-key management.
- Access restriction and least-privilege enforcement; policy enforcement with IAM + MFA.
- Policy-driven workflow with dry-run simulation and reversible (rollback) actions; SLA-linked remediation deadlines.
- Proof-of-fix audits with closure evidence; consent-triggered remediation workflows.

Security & Trust

- **Single sign-on** via SAML 2.0 and OIDC; **multi-factor authentication** — password, Email OTP, KBA, and TOTP authenticator apps (Google / Microsoft Authenticator).
- **Users & Groups** via LDAP/AD sync and form-based creation; **RBAC** (Module Page Action Component) with user entitlements and security-policy configuration.
- **Multi-tenancy** — database-per-tenant isolation with configurable tenant resolution (fixed, product subdomain, customer domain, URL path, or email-domain fallback).
- **Tamper-evident, hash-chained audit logging**; consent receipts and exportable evidence packages.
- **Encryption** in transit (TLS 1.2+/1.3) and at rest; two-tier DEK/KEK key hierarchy with HSM / key-vault integration (PKCS#11).

Performance & Scale

- Consent verification designed for **~10,000 requests per second sustained**, with the Consent Verification API responding in **under 100 ms at p95**.
- Data discovery sized for **100 GB–1 TB+** corpora, scanned in parallel across CPU worker pods.
- Horizontal scaling and auto-scaling; high-availability and disaster-recovery topologies supporting **99.9% and 99.99%** availability.

Regulatory Coverage

- **GDPR** — European Union / United Kingdom · **DPDP Act 2023** — India (with Data-Protection-Board workflows)
- **CCPA / CPRA** — California, US · **CDPA** — Virginia, US · **HIPAA** — US healthcare · **PCI-DSS** — cardholder data
- **LGPD** — Brazil · **PIPEDA** — Canada · **PDPA** — Singapore & Thailand · **POPIA** — South Africa
- **APP / Privacy Act** — Australia · **APPI** — Japan · **PIPL & CSL** — China · **PDPL** — UAE & Saudi Arabia · **NDPR** — Nigeria
- Sector mandates — **RBI** (India banking), **TRAI** (India telecom)
- Pre-built compliance templates, assessment frameworks, and automated controls per regulation.

Integration

- ERP — SAP · CRM — Salesforce · ITSM — ServiceNow
- Key & secrets management — KMS, HashiCorp Vault · Identity — IAM, MFA, PAM systems
- Notification gateways — SMTP, SMS, Microsoft Teams
- Custom Connector SDK and governance integrators for enterprise and core systems.

Use Cases By Industry

Industry	How PrivaTrust helps
Banking & Financial Services	RBI data-localisation, customer-PII protection, DPDP/RBI compliance, and core-banking / lending / insurance data coverage
Healthcare & Life Sciences	PHI protection across EHR, HIPAA compliance, patient consent for clinical trials, and pharma / health-tech data
E-Commerce & Retail	Large-volume customer consent, cookie compliance at scale, DSAR automation, and payment / marketing data compliance
Technology & SaaS	Privacy-by-design, multi-tenant data isolation, and enterprise customer compliance reporting
Telecommunications	Subscriber consent management, TRAI & DPDP compliance, CDR / location-data discovery, and DPIA automation for new services
Government & Public Sector	Air-gapped deployment, citizen-data protection, DPDP compliance, and sovereign data governance across departments

Platform Heritage

PrivaTrust is built on eMudhra's 15+ years of digital-trust, PKI, and identity expertise as India's largest Certifying Authority. Native integration points with eMudhra's identity (SecurePass), signing (emSigner), and certificate-lifecycle (CertiNext) platforms allow unified policy enforcement across the digital-trust stack.

About eMudhra

eMudhra is a global trust-services and digital-identity company, operating across 35+ countries and serving enterprise, government, and financial-sector customers worldwide. As India's largest Certifying Authority with a 37.9% market share in Digital Signature Certificates, eMudhra is a licensed Certifying Authority, Trust Service Provider, and Qualified Trust Service Provider across multiple jurisdictions.

The eMudhra portfolio spans the full digital-trust stack — Public Key Infrastructure (emCA, emSign), Certificate Lifecycle Management (CertiNext), enterprise eSignature (emSigner), Converged Identity and Access Management (SecurePass), identity verification and KYC (ID Broker), and Privacy & Data Governance (PrivaTrust) — with post-quantum-cryptography readiness built in.

eMudhra has been recognised by Gartner, IDC, Frost & Sullivan, and G2 across eSignature, PKI, CLM, and Digital Trust categories. For more information, visit emudhra.com.