VISHWAAS

VISHWAAS AI

Privacy & Consent Management Portal

Complete Product Feature List

15 Modules • 225 Features • ~95 API Endpoints

Full DPDP Act 2023 + Rules 2025 Compliance Coverage

Version 1.0 • March 2026 • Confidential

Table of Contents

1. Product Overview

VISHWAAS AI is a comprehensive Privacy & Consent Management Portal built to help organizations comply with India's Digital Personal Data Protection Act, 2023 (DPDP Act) and DPDP Rules 2025. It is a product under the Cross Identity brand family — a converged Identity and Access Management platform.

The product provides 15 functional modules with 200+ individual features spanning consent lifecycle management, privacy notices, data principal rights, breach management, data protection impact assessments, vendor governance, compliance dashboards, and consumer self-service — all anchored on a cryptographically non-repudiated, tamper-proof consent ledger.

Total Features: 207 features across 15 modules

Total API Endpoints: ~95 RESTful APIs

Total Database Tables: ~27 tables across 2 schemas (app + audit)

Supported Languages: 23 (English + 22 scheduled Indian languages)

DPDP Act Coverage: Sections 5, 6, 8, 9, 10, 11, 12, 13, 14; Rules 3, 4, 7, 8, 10, 14

2. Complete Feature List by Module

MODULE 1: MULTI-TENANCY & TENANT MANAGEMENT

Core platform infrastructure enabling multiple organizations to share the VISHWAAS AI platform with complete data isolation.

#	Feature	Description	DPDP Ref
1.1	Tenant Provisioning	Create and configure new tenant organizations with unique slug, domain, plan tier, and branding	
1.2	Row-Level Security (RLS)	PostgreSQL RLS policies ensure every database query is scoped to the authenticated tenant; cross-tenant data leakage is impossible at the database level	
1.3	Tenant Configuration (JSONB)	Per-tenant settings: branding (logo, colors, portal URL), default language, timezone, retention policies, DPBI registration ID, SDF flag	Section 10
1.4	Plan-Based Feature Gating	Three-tier plan (Starter, Professional, Enterprise) controls which modules are available to each tenant	
1.5	Per-Tenant Encryption Keys	Each tenant gets a unique AES-256 encryption key (via AWS KMS) for field-level PII encryption; key rotation supported	Section 8(4)
1.6	Custom Domain Support	Tenant can configure a custom domain (privacy.acme.com) for their Data Principal portal	
1.7	Tenant Suspension & Deactivation	Admins can suspend (read-only) or deactivate (no access) tenants; data preserved per retention policy	
1.8	Significant Data Fiduciary (SDF) Mode	Toggle that enables additional SDF-specific features: mandatory DPIA, DPO appointment, independent audit interface	Section 10

MODULE 2: AUTHENTICATION & IDENTITY ACCESS MANAGEMENT

Passwordless email OTP authentication for all users (admin and consumers) with JWT sessions, RBAC, and API key management. Integrates with Cross Identity IAM platform.

#	Feature	Description	DPDP Ref
2.1	Email OTP Login (Admin)	Admin users authenticate via email → 6-digit OTP → JWT token. No passwords stored anywhere.	
2.2	Email OTP Login (Data Principal)	Consumer portal login via email OTP with organization-branded email templates	
2.3	OTP Generation (Cryptographic)	6-digit OTP generated via crypto.randomInt; stored in Redis with 10-minute TTL	
2.4	OTP Rate Limiting	Max 3 OTP requests per email per 5 minutes; max 5 verification attempts per OTP	
2.5	OTP Email Delivery	Branded HTML email via Nodemailer; MailHog for Dev/QA, AWS SES for production	
2.6	JWT Access Tokens (RS256)	15-minute access tokens signed with RSA-2048; contains user ID, tenant, roles, user type	
2.7	JWT Refresh Tokens	7-day refresh tokens stored in Redis; rotation on each refresh; revocation on logout	
2.8	Session Management	Configurable session timeouts, concurrent session limits, device-level tracking	
2.9	11 System Roles (RBAC)	Pre-defined roles: Super Admin, DPO, Privacy Manager, Legal Officer, IT Admin, Grievance Officer, Dept Manager, Processor Liaison, Data Principal, Auditor, Training Admin	Section 10(2)
2.10	Fine-Grained Permissions (CASL)	18 resources × 6 actions = 108 permissions; attribute-based conditions; per-role mapping	
2.11	Permission Guards	@CheckPermission(resource, action) decorator on every API endpoint	
2.12	API Key Management	Create, revoke, and scope API keys for system-to-system integration; SHA-256 key hashing	
2.13	User Provisioning	Create, update, deactivate internal users with role assignment; soft delete support	
2.14	Cross Identity SSO Integration	OAuth 2.0 / OIDC integration with Cross Identity for federated single sign-on	
2.15	Login Audit Trail	Every login attempt (success/failure) logged to immutable audit ledger with IP, user agent, timestamp	Section 8(4)
2.16	Account Lockout	Automatic lock after 5 failed OTP verifications; configurable lockout duration	

MODULE 3: CONSUMER DATA UNIFICATION & IDENTITY RESOLUTION

Connects to all customer-facing applications, discovers consumer data, resolves identities, and builds a unified Data Principal profile. The foundation for accurate consent management and rights fulfillment.

#	Feature	Description	DPDP Ref
3.1	Connector Framework	Pre-built adapters for CRM, e-commerce, mobile, marketing, support, HR, databases, cloud storage, and custom APIs	
3.2	Salesforce Connector	OAuth 2.0 integration; extracts Contact/Lead records with email, phone, address, custom fields	
3.3	HubSpot Connector	API-based connector for contacts, companies, and engagement data	
3.4	Shopify / E-Commerce Connector	Customer, order, and address data extraction via REST API	
3.5	CleverTap / Marketing Connector	Subscriber data, campaign engagement, and preference sync	
3.6	Freshdesk / Support Connector	Ticket email, customer interactions, and support data categories	
3.7	Darwinbox / HRIS Connector	Employee ID, PII, Aadhaar, PAN, salary data category flags	
3.8	Database Connector (JDBC)	Direct connection to PostgreSQL, MySQL, MongoDB, SQL Server for PII discovery	
3.9	Cloud Storage Connector	S3, Azure Blob, GCS file-level PII pattern scanning	
3.10	Custom REST/GraphQL Connector	Configurable HTTP adapter with field mapping for any API	
3.11	Deterministic Identity Matching	Exact match on normalized email, phone (E.164), Aadhaar hash, PAN, organization customer ID	
3.12	Probabilistic Identity Matching	Fuzzy matching (Jaro-Winkler) on name + DOB + address; configurable threshold (default 85%)	
3.13	Manual Match Review Queue	Privacy Manager reviews and approves/rejects probabilistic matches before merging	
3.14	Identity Graph Construction	Links all external IDs to one canonical Data Principal UUID; maintains source attribution	
3.15	External ID Map	JSONB array mapping: [{system, ext_id}] for every connected system per principal	
3.16	Data Asset Map	Records which source systems hold which data categories for each principal	Section 11
3.17	PII Discovery Scan	Automated scan of connected systems to identify PII columns/fields	Section 8
3.18	Continuous Real-Time Sync	After initial onboarding, connectors sync new/changed records in real-time or on schedule	
3.19	Merge Audit Trail	Immutable log of every identity merge: who confirmed, when, which records linked, confidence score	
3.20	Duplicate Detection & De-duplication	Identifies and flags duplicate principal records within and across source systems	

MODULE 4: CONSENT LIFECYCLE MANAGEMENT

The core module. Manages purpose-specific consent collection, withdrawal, modification, expiry, and renewal with a cryptographically non-repudiated, hash-chained, digitally signed consent ledger.

#	Feature	Description	DPDP Ref
4.1	Consent Purpose Definition	Create purposes with multilingual name/description (22 languages), category, lawful basis, data categories, retention, and processor linkage	Section 6
4.2	Purpose Categories	Six categories: Essential, Functional, Analytics, Marketing, Third-Party Sharing, Employment	Section 6
4.3	Lawful Basis Selection	Two DPDP bases: Consent (requires affirmative opt-in) and Legitimate Use (employment, legal, emergency)	Section 4, 7
4.4	Granular Purpose-Specific Consent	Each purpose requires separate, independent consent; no bundled consents	Section 6
4.5	Affirmative Action Requirement	No pre-ticked boxes; consent requires explicit opt-in toggle or click	Section 6
4.6	Multilingual Consent Collection	Consent forms rendered in 22 Indian languages + English; auto-detect user locale	Section 5; Rule 3
4.7	Multi-Channel Consent	Collect consent via web, mobile app, API, offline (digitized), email, SMS	Section 6
4.8	Consent Text Snapshot	Captures exact text shown to user at consent time (in their language) for legal defensibility	
4.9	Consent Withdrawal (Easy)	One-click withdrawal; process equally simple as consent collection per DPDP requirement	Section 6(4)
4.10	Granular Modification	Data Principals modify consent per-purpose without affecting other consents	Section 6
4.11	Consent Expiry Management	Configurable validity periods per purpose; auto-expiry with advance renewal campaigns	
4.12	Consent Renewal Campaigns	Automated email/notification campaign 7 days before consent expiry	
4.13	Children's Consent (Verifiable Parental)	Parental/guardian consent for under-18 via DigiLocker, Aadhaar eKYC, or authorized tokens	Section 9; Rule 10
4.14	Guardian Linkage	Minor Data Principal linked to parent/guardian Data Principal with verified relationship	Section 9
4.15	Legacy Consent Migration	Re-obtain DPDP-compliant consent for pre-Act data with automated retrospective notice campaigns	Rule 3
4.16	Bulk Consent Collection	CSV upload or batch API for collecting consent for multiple principals simultaneously	
4.17	Consent Status API (Real-Time)	GET /consent/status/{dp_id}/{purpose} — < 50ms response from Redis cache	
4.18	Batch Status Check	POST /consent/batch-status for checking 1000+ records before mass campaigns	
4.19	SHA-256 Record Hashing	Every consent record content is SHA-256 hashed for integrity	
4.20	Merkle Hash Chain	Each record's chain_hash = SHA-256(record_hash + previous.chain_hash); tamper-evident chain	
4.21	RSA Digital Signatures	Every consent record signed with server's RSA-2048 private key; auditor-verifiable	
4.22	RFC 3161 Trusted Timestamps	External timestamp authority token on each record for legal time proof	
4.23	Append-Only Storage	consent_records table: INSERT + SELECT only at DB level; no UPDATE/DELETE grants	

4.24	Chain Integrity Verification	On-demand or batch verification: recalculate all hashes, report any broken links	
4.25	Consent Artifact Export	Export individual consent artifacts as signed PDF/JSON for regulatory submission	
4.26	Consent Audit Trail Export	Export full audit trail as PDF/CSV for DPBI inspection or independent audit	Rule 4
4.27	7-Year Consent Retention	Consent records retained for minimum 7 years per DPDP Rules for Consent Managers	Rule 4
4.28	Consent Propagation (Push)	Real-time webhooks to all downstream systems on consent change	
4.29	Consent Propagation (Pull)	High-performance status API for point-of-use verification by downstream systems	
4.30	Consent Propagation (Enforce)	SDK middleware / API Gateway plugin that blocks data access without valid consent	
4.31	Connector-Specific Actions	Each consent change translates to native system action (Salesforce DoNotEmail, CleverTap unsubscribe, etc.)	

MODULE 5: PRIVACY NOTICE MANAGEMENT

Create, version, translate, deliver, and track multilingual privacy notices compliant with DPDP Act Section 5 and Rule 3.

#	Feature	Description	DPDP Ref
5.1	Notice Builder (Rich Text)	TipTap WYSIWYG editor for authoring privacy notice content with formatting, links, and structure	Section 5; Rule 3
5.2	Multilingual Content (22 Languages)	Tab-based editor for creating notice content in all 22 Indian languages + English	Rule 3
5.3	Notice Types	Collection Notice, Retrospective Notice (for pre-Act data), Updated Notice	Rule 3
5.4	Version Control	Every notice edit creates a new version; full version history with diff capability	
5.5	Approval Workflow	Draft → Submit for Review → Approve (Legal/DPO) → Published; rejection with comments	
5.6	Effective Date Management	Schedule notice activation; auto-archive previous version on publish	
5.7	Purpose Linkage	Link specific consent purposes to each notice; consent forms reference the displayed notice version	Section 5
5.8	Required Content Enforcement	System ensures notice includes: data collected, purpose, rights exercise method, DPBI complaint process, contact details	Rule 3
5.9	Content Hash Integrity	SHA-256 hash of notice content for tamper detection	
5.10	Public Notice Endpoint	GET /notices/public/:code?lang=hi — embeddable on any website/app	
5.11	Delivery Tracking	Record when each notice was served to each Data Principal, via which channel, in which language	
5.12	Delivery Proof Hash	Non-repudiated proof of notice delivery with timestamp and channel metadata	
5.13	Acknowledgment Tracking	Track when Data Principal acknowledged/read the notice	
5.14	Retrospective Notice Campaigns	Automated bulk notices to existing Data Principals for legacy pre-Act data	Rule 3
5.15	Notice Delivery Statistics	Dashboard showing: notices served, acknowledgment rates, language distribution	

MODULE 6: DATA PRINCIPAL SELF-SERVICE PORTAL

Consumer-facing portal where Data Principals manage their privacy — view/modify consents, submit rights requests, view notices, and manage nominees. Mobile-responsive and available in 22 languages.

#	Feature	Description	DPDP Ref
6.1	Portal Email OTP Login	Secure passwordless login for Data Principals via email OTP	
6.2	DigiLocker Login (Placeholder)	Future integration for Aadhaar/DigiLocker-based identity verification	Rule 10
6.3	22-Language Portal UI	Full portal interface available in all 22 Indian languages with manual language selector	Rule 3
6.4	Organization Branding	Portal displays tenant's logo, colors, and name — white-labeled experience	
6.5	Consent Dashboard	Card-based view of all consent purposes with ON/OFF toggles, descriptions, and dates	Section 6, 11
6.6	One-Click Consent Toggle	Toggle consent ON (grant) or OFF (withdraw) with immediate visual feedback and real-time propagation	Section 6(4)
6.7	View Notice from Consent Card	Each consent card links to the exact privacy notice version that was displayed	Section 5
6.8	Withdraw All Consents	Single action with confirmation dialog to withdraw all active consents simultaneously	Section 6(4)
6.9	Download My Data	Triggers an access request and provides a downloadable summary of all personal data held	Section 11
6.10	Submit Rights Request	Form to submit access, correction, erasure, or grievance requests with type selector and description	Section 11-14
6.11	Request Tracking Dashboard	List of all submitted requests with tracking number, status, and SLA deadline	Section 13
6.12	Request Detail & Timeline	View full activity timeline for each request: status changes, staff responses, documents	
6.13	Nominee Registration	Designate a trusted person to exercise privacy rights in case of death or incapacity	Section 14
6.14	Nominee Management	Update or remove nominee; view current nominee details	Section 14
6.15	Privacy Notice Library	View all privacy notices delivered, in preferred language, with delivery dates	Section 5
6.16	Consent Expiry Notifications	Automated notifications when consents are approaching expiry with renewal option	
6.17	Mobile-Responsive Design	Fully responsive layout optimized for mobile devices (375px+)	
6.18	Accessibility (WCAG 2.1 AA)	Screen reader support, keyboard navigation, contrast ratios	

MODULE 7: DATA PRINCIPAL RIGHTS (DPR) MANAGEMENT

Full workflow engine for managing Data Principal rights requests: access, correction, erasure, nomination, grievance, and portability — with SLA tracking, identity verification, erasure orchestration, and DPBI escalation.

#	Feature	Description	DPDP Ref
7.1	Request Submission (Admin/Portal)	Staff or Data Principals submit rights requests with type, description, and data categories	Section 11-14
7.2	Auto-Generated Request Number	Sequential tracking number: DPR-YYYY-NNNNN for human-readable reference	
7.3	Request Types (6)	Access, Correction, Erasure, Nomination, Grievance, Portability	Section 11-14
7.4	Automatic SLA Calculation	SLA deadline = created_at + 90 days (configurable per tenant)	DPDP Rules
7.5	Identity Verification (Email OTP)	Verify Data Principal identity via email OTP before processing sensitive requests	
7.6	Identity Verification (Aadhaar)	Future: Aadhaar eKYC verification for high-assurance identity confirmation	Rule 10
7.7	Request Assignment	Route requests to appropriate staff member or department	
7.8	Priority Levels	Low, Normal, High, Urgent — with priority-based SLA escalation	
7.9	Status Workflow Engine	Submitted → Identity Verification → In Progress → Pending Approval → Completed/Rejected/Escalated	
7.10	Activity Timeline	Chronological log of every action: status changes, comments, document uploads, assignments	
7.11	Internal Comments & Documents	Staff can add notes, attachments, and internal communications per request	
7.12	Data Discovery for Access Requests	Automated scan across connected systems to locate all personal data for the requesting principal	Section 11
7.13	Erasure Orchestration	Creates parallel erasure jobs for every connected system that holds the principal's data	Section 12
7.14	48-Hour Pre-Erasure Notification	Sends advance notification to Data Principal before data deletion begins	Rule 8
7.15	Per-System Erasure Tracking	Status tracking per target system: pending, notified, in progress, completed, failed, retained	
7.16	Retention Override Documentation	When erasure conflicts with legal retention, the override reason and specific law reference are documented	Section 8(7)
7.17	Erasure Evidence Hash	SHA-256 hash of deletion confirmation from each system for audit proof	
7.18	DPBI Escalation	DPO can escalate unresolved grievances to Data Protection Board with full evidence package	Section 13, 27
7.19	SLA Monitoring Dashboard	Color-coded SLA indicators: green (>30d), yellow (<30d), red (<7d), bold-red (overdue)	
7.20	SLA Breach Alerts	BullMQ cron job checks hourly; alerts assigned staff and DPO on approaching/past SLA	
7.21	Bulk Assignment	Assign multiple requests to a staff member in one action	
7.22	Request Resolution	Complete request with resolution notes; notify Data Principal of outcome	
7.23	Request Rejection (with Reason)	Reject request with documented reason; Data Principal notified	

7.24	DPR Status Email Notifications	Email updates to Data Principal at key stages: received, in progress, completed	

MODULE 8: BREACH MANAGEMENT

Incident intake, automated risk assessment, DPBI notification workflow, mass Data Principal alerts, remediation tracking, and post-incident reporting.

#	Feature	Description	DPDP Ref
8.1	Incident Intake Form	Multi-step form: Incident Details → Impact Assessment → Immediate Actions	Section 8(6)
8.2	Auto-Generated Incident Number	BRI-YYYY-NNNNN tracking format	
8.3	Severity Classification	Critical, High, Medium, Low — with automated severity suggestion based on impact	
8.4	Breach Type Taxonomy	Unauthorized Access, Data Loss, Unauthorized Disclosure, System Compromise, Accidental Deletion	
8.5	Automated Risk Assessment	Scoring engine: severity × data types affected × principals count × system exposure	
8.6	Data Categories Affected	Checkbox selection: names, emails, Aadhaar, PAN, health, financial, children's data, etc.	
8.7	Affected Systems Mapping	Multi-select of connected systems involved in the breach	
8.8	DPBI Notification Workflow	Pre-formatted notification document generation; submission tracking; DPBI reference number storage	Section 8(6); Rule 7
8.9	Data Principal Mass Notification	Email/SMS notification to all affected Data Principals via BullMQ queue	Section 8(6)
8.10	Remediation Action Items	Add, assign, and track corrective actions with completion status and evidence	
8.11	Root Cause Analysis	Structured root cause documentation linked to remediation plan	
8.12	Investigation Timeline	Chronological log of all investigation activities, findings, and decisions	
8.13	Breach Closure Report	Comprehensive final report with incident summary, impact, actions taken, and lessons learned	
8.14	Breach Dashboard & Metrics	Active incidents, severity distribution, average resolution time, monthly trends	

MODULE 9: DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Guided assessment workflows with risk auto-calculation, mitigation planning, and DPO approval chains. Mandatory for Significant Data Fiduciaries.

#	Feature	Description	DPDP Ref
9.1	Guided Questionnaire Wizard	Step-by-step DPIA questionnaire aligned with DPDP Act requirements	Section 10(2)
9.2	Risk Auto-Calculation	Algorithm: data sensitivity × volume × processing nature × impact potential → 0-100 score	
9.3	Risk Level Classification	Low (0-25), Medium (26-50), High (51-75), Critical (76-100)	
9.4	Identified Risks Registry	Structured list of risks with likelihood, impact, and planned mitigation for each	
9.5	Mitigation Plan Tracking	Define controls, assign owners, set deadlines, track implementation status	
9.6	Approval Chain	Creator → DPO Review → Approve/Reject with comments	Section 10(2)
9.7	Periodic Review Scheduling	Set next review date; automated reminders for reassessment	
9.8	Risk Visualization	Radar chart showing risk dimensions; trend over time for repeat assessments	
9.9	Purpose & Data Category Linkage	Link DPIA to specific consent purposes and data categories being assessed	
9.10	DPIA Export (PDF)	Generate printable DPIA report for Board of Directors or independent auditor	Section 10(2)(b)

MODULE 10: VENDOR & DATA PROCESSOR MANAGEMENT

Onboard, assess, and continuously monitor third-party data processors with DPA management and cross-border transfer tracking.

#	Feature	Description	DPDP Ref
10.1	Vendor Onboarding	Register new vendors with company details, type (processor/sub-processor/joint controller), country, contacts	Section 8(2)
10.2	Privacy Risk Assessment	Structured questionnaire for evaluating vendor's privacy practices; auto-calculated risk score	
10.3	Risk Level Classification	Low, Medium, High, Critical — with configurable thresholds	
10.4	DPA Repository	Upload and store signed Data Processing Agreements with expiry tracking	Section 8(2)
10.5	DPA Expiry Alerts	Automated notifications when DPA approaches expiration date	
10.6	Purpose-Sharing Linkage	Map which consent purposes are shared with each vendor	
10.7	Cross-Border Transfer Detection	Auto-flag vendors in countries outside India; check against government blacklist	Section 16; Rule 14
10.8	Government Blacklist Auto-Check	Configurable list of restricted countries; automatic transfer blocking for blacklisted destinations	Rule 14
10.9	Consent Propagation to Processors	Real-time consent change notifications pushed to processor systems	Section 8(7)
10.10	Processor Compliance Attestation	Vendors submit periodic compliance attestations via processor liaison portal	
10.11	Continuous Monitoring	Scheduled reassessment reminders; compliance status dashboard per vendor	
10.12	Vendor Status Lifecycle	Pending Review → Approved → Active → Suspended → Terminated	

MODULE 11: DATA INVENTORY, DISCOVERY & RETENTION

Automated personal data discovery, classification, data flow mapping, RoPA generation, and retention policy enforcement across all connected systems.

#	Feature	Description	DPDP Ref
11.1	Automated Data Discovery	Scan connected databases, file storage, SaaS apps, and APIs for PII	Section 8
11.2	AI-Powered PII Classification	Auto-detect and categorize: names, emails, phones, Aadhaar, PAN, health, financial, biometric data	
11.3	Data Flow Mapping (Visual)	Interactive diagram showing how personal data flows between systems, including cross-border transfers	
11.4	Data Asset Registry	Catalog of all systems holding personal data with: owner, department, classification, scan date, record count	
11.5	Record of Processing Activities (RoPA)	Auto-generated RoPA from data inventory with purpose, legal basis, retention, and processor details	Section 8
11.6	Retention Policy Engine	Define retention rules per data category; automated enforcement with deletion scheduling	Section 8(7); Rule 8
11.7	Auto-Deletion on Consent Withdrawal	When consent is withdrawn and retention period expires, trigger automated deletion across systems	Section 8(7)
11.8	Inactivity-Based Retention	For platforms in Third Schedule: auto-delete after 3 years of Data Principal inactivity	Rule 8
11.9	1-Year Log Retention	Processing logs retained for minimum 1 year per Seventh Schedule	Rule 8
11.10	Data Classification Labels	Public, Internal, Confidential, Restricted — applied to each data asset	

MODULE 12: COMPLIANCE DASHBOARD & REPORTING

Real-time executive dashboard with compliance metrics, risk heatmaps, trend analytics, and regulatory report generation.

#	Feature	Description	DPDP Ref
12.1	Compliance Overview Dashboard	4 key metric cards: Consent Coverage %, Open DPR Requests, Active Breaches, Pending DPIAs	
12.2	Consent Trends Chart	LineChart: grants vs withdrawals over 7/30/60/90 day periods	
12.3	DPR SLA Compliance Chart	BarChart: on-time vs overdue by request type; SLA compliance percentage	
12.4	Breach Metrics	Severity distribution, status breakdown, average resolution time, monthly trend	
12.5	Risk Heatmap	Matrix: departments × data categories color-coded by risk score	
12.6	Real-Time Activity Feed	Live event stream (30s polling): latest consent actions, DPR updates, breach events	
12.7	Vendor Risk Summary	Aggregated vendor risk scores with drill-down to individual assessments	
12.8	Compliance Report Generator	Generate PDF/Excel reports: Compliance Summary, Consent Audit, DPR Summary, Breach Report	Section 10(2)
12.9	Report Scheduling	Schedule automated weekly/monthly compliance reports delivered via email	
12.10	Audit-Ready Evidence Packages	Export comprehensive evidence packages for DPBI inspection or independent audit	Section 10(2)(b)
12.11	Board of Directors Report	Executive summary report for SDF Board reporting requirements	Section 10
12.12	Custom Date Range Filtering	All dashboards and reports support custom date range selection	

MODULE 13: COOKIE CONSENT MANAGEMENT

Embeddable JavaScript widget for website cookie consent with automatic scanning, category management, and sync with the consent ledger.

#	Feature	Description	DPDP Ref
13.1	Cookie Scanner	Automated website scan that discovers and categorizes all cookies	
13.2	Cookie Categorization	Essential (always on), Functional, Analytics, Marketing — mapped to consent purposes	
13.3	Customizable Consent Banner	Bottom/top bar or modal; organization branding (logo, colors); configurable via data attributes	
13.4	Multilingual Banner	22 Indian languages + English with auto-detect and manual selector	Rule 3
13.5	Granular Category Toggles	Individual ON/OFF toggles per cookie category; Essential always ON (disabled)	Section 6
13.6	Accept All / Accept Selected / Reject All	Three action buttons per DPDP consent requirements	Section 6
13.7	Cookie Blocking Until Consent	Client-side interception prevents non-essential cookies from loading until consent granted	
13.8	Consent Ledger Sync	Every banner action posts to VISHWAAS AI consent API; appears in consent records with hash chain	
13.9	Consent Cookie Storage	Local browser cookie (ct_consent) stores consent state for returning visitors	
13.10	Privacy Notice Link	Banner includes link to full privacy notice in selected language	Section 5
13.11	Lightweight Widget	Vanilla TypeScript; ~20KB gzipped; loaded via single script tag	
13.12	Preference Center Reopener	Floating button or link to reopen consent preferences after initial decision	

MODULE 14: NOTIFICATIONS, EVENTS & WEBHOOKS

Event-driven architecture with Kafka streaming, webhook dispatch, and multi-channel notifications (email, SMS, in-app) for all privacy actions.

#	Feature	Description	DPDP Ref
14.1	Kafka Event Streaming	7 topics: consent, notice, dpr, breach, audit, webhook dispatch, notification dispatch	
14.2	Standard Event Envelope	JSON schema: event_id, type, tenant_id, actor, resource, data, metadata, timestamp	
14.3	Immutable Audit Ledger Consumer	Consumes all events; writes to audit.events with hash chain + digital signature	Section 8(4)
14.4	Audit Chain Verification	On-demand integrity verification of the entire audit event chain per tenant	
14.5	Audit Chain Checkpoints	Periodic checkpoint records for external auditor verification starting points	
14.6	Webhook Registration	Register webhook endpoints per tenant with event type subscription and HMAC secret	
14.7	HMAC-SHA256 Webhook Signing	Every webhook payload signed with X- VISHWAAS AI-Signature header for authenticity	
14.8	Webhook Retry (Exponential Backoff)	3 retries: 1s, 5s, 30s; failed deliveries logged and alerted	
14.9	Webhook Dead Letter Queue	Persistently failed webhooks stored for manual retry or investigation	
14.10	Webhook Test Endpoint	Send test event to verify webhook configuration before going live	
14.11	9 Webhook Event Types	consent.granted, consent.withdrawn, consent.expired, dpr.request.created, dpr.request.completed, breach.reported, breach.dpbi_notified, notice.published, vendor.status_changed	
14.12	Email Notifications (Nodemailer)	OTP delivery, DPR status updates, breach alerts, consent expiry reminders, DPIA review requests	
14.13	MailHog Integration (Dev/QA)	All emails captured by MailHog (localhost:8025) for testing and verification	
14.14	SMS Notifications (Future)	Pluggable SMS provider for OTP and critical alerts	
14.15	In-App Notification Center	Bell icon with notification drawer showing latest events relevant to the current user's role	

MODULE 15: TRAINING & AWARENESS

Privacy awareness e-learning, role-specific training tracks, policy acknowledgment, and completion tracking for organizational compliance culture.

#	Feature	Description	DPDP Ref
15.1	E-Learning Module Library	Built-in privacy awareness courses covering DPDP Act, consent handling, breach response, data rights	
15.2	Role-Specific Training Tracks	Customized course paths for IT, HR, Marketing, Legal, and Leadership roles	
15.3	Course Assignment	Assign courses to individual users, departments, or roles; bulk assignment	
15.4	Completion Tracking	Dashboard showing completion status per user, department, and course with percentage metrics	
15.5	Automated Reminders	Email reminders for overdue training assignments	
15.6	Policy Acknowledgment Workflow	Require employees to read and digitally acknowledge privacy policies; non-repudiated log of acknowledgment	
15.7	Training Compliance Reports	Generate reports showing organizational training completion rates for audit/Board submission	
15.8	Certificate Generation	Auto-generate completion certificates for successfully finished courses	

3. Feature Count Summary

Module	Feature Count	Category
Module 1: Multi-Tenancy & Tenant Management	8	Platform Infrastructure
Module 2: Authentication & IAM	16	Security & Access
Module 3: Consumer Data Unification & Identity Resolution	20	Data Foundation
Module 4: Consent Lifecycle Management	31	Core Compliance
Module 5: Privacy Notice Management	15	Core Compliance
Module 6: Data Principal Self-Service Portal	18	Consumer Experience
Module 7: Data Principal Rights (DPR) Management	24	Core Compliance
Module 8: Breach Management	14	Incident Response
Module 9: Data Protection Impact Assessment (DPIA)	10	Governance
Module 10: Vendor & Data Processor Management	12	Governance
Module 11: Data Inventory, Discovery & Retention	10	Data Foundation
Module 12: Compliance Dashboard & Reporting	12	Analytics & Reporting
Module 13: Cookie Consent Management	12	Consent Collection
Module 14: Notifications, Events & Webhooks	15	Integration & Infrastructure
Module 15: Training & Awareness	8	Organizational Compliance
TOTAL	**225**	**15 Modules**

— End of VISHWAAS AI Feature List —

VISHWAAS

Contact Us

+1 888 208 5076 / +91 901 926 6824

sales@crossidentity.com

www.crossidentity.com

Release Date - 16/03/2026 Version 1.0