VISHWAAS

Vishwaas AI

Privacy & Consent Management Portal

Product Feature Explanatory Document

Admin Portal • Data Principal Portal • March 2026

Introduction

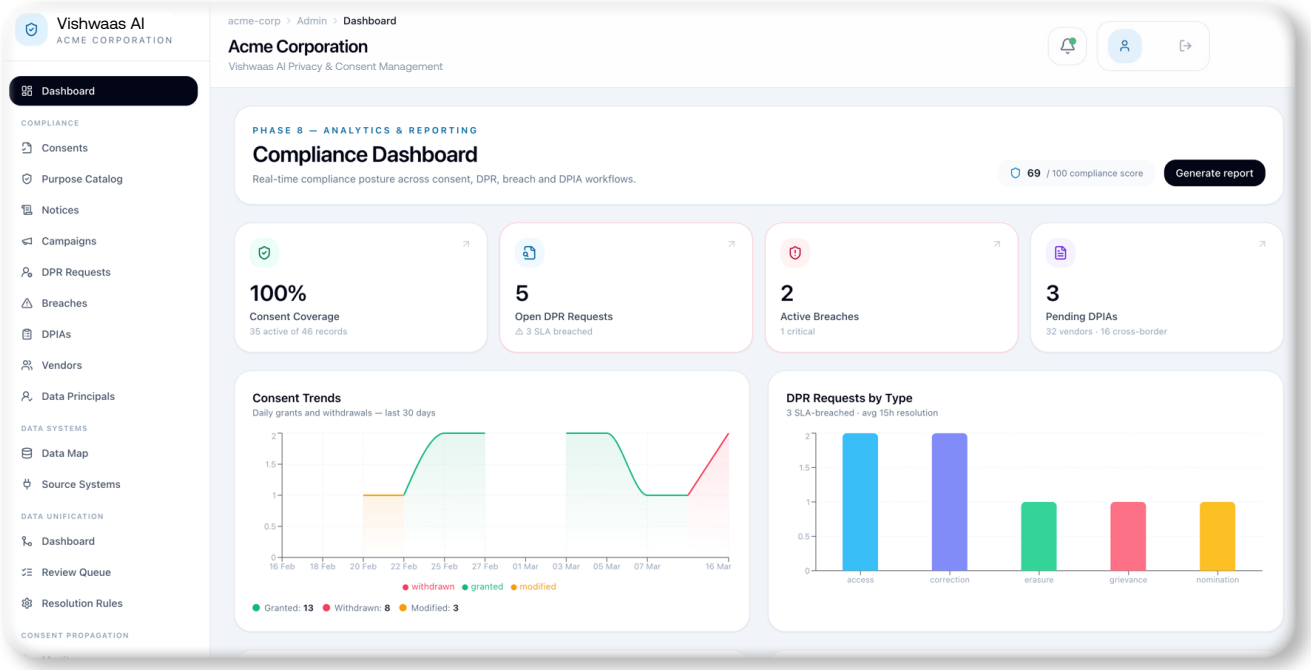
This document describes every menu option available in Vishwaas AI — both the Admin Portal and the Data Principal Portal. For each menu option, it explains what the section is for and what actions are available within it, accompanied by a screenshot for visual reference.

Part 1 covers the Admin Portal, used by DPOs, Privacy Managers, Grievance Officers, IT Admins, and other internal staff. Part 2 covers the Data Principal Portal, used by customers and end users to manage their own privacy preferences.

Part 1 — Admin Portal

The Admin Portal is the primary workspace for all internal users of Vishwaas AI. It is accessible at the organisation's configured Vishwaas AI domain and provides role-based navigation across all 23 compliance, governance, and configuration modules.

1. Dashboard



What it is

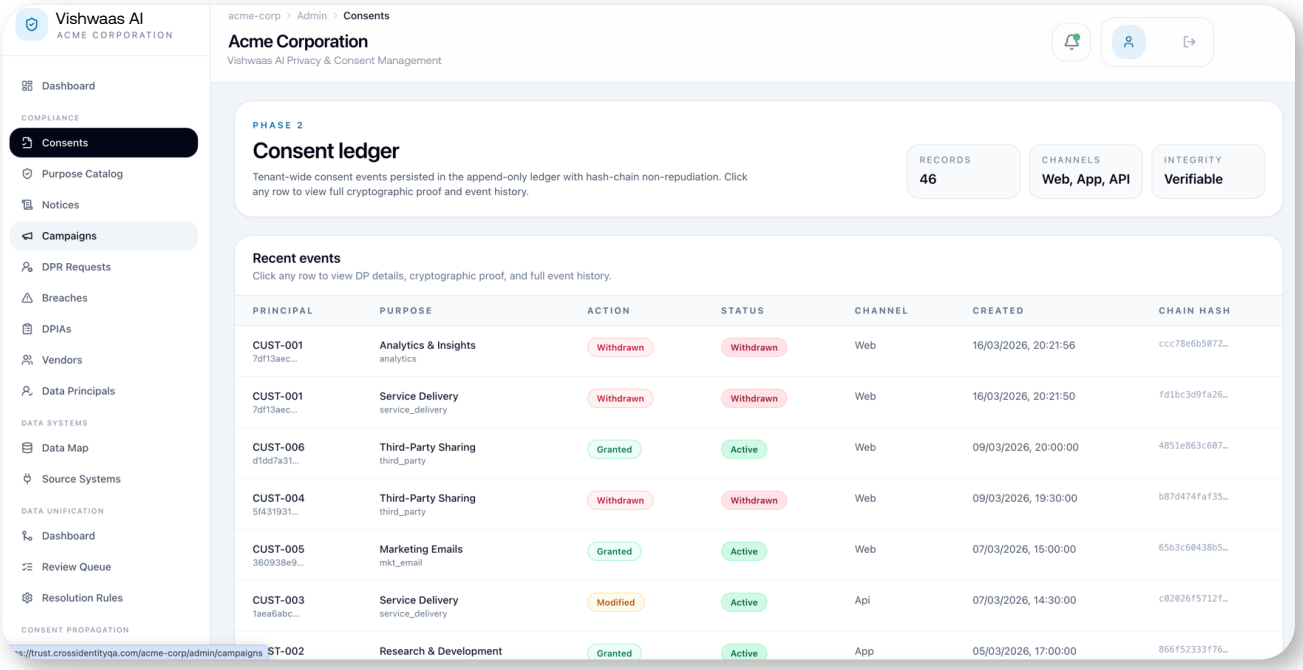
The Dashboard is the first screen an admin sees after logging in. It provides a real-time overview of the organisation's DPDP Act compliance health across all modules in a single view.

What it does

- Displays the overall Compliance Score as a circular gauge from 0 to 100, colour-coded: red (0–40), amber (41–70), green (71–100), with a 7-day trend indicator.
- Shows total Penalty Exposure in Indian Rupees (crores) based on currently open compliance gaps, with a breakdown by DPDP Act section and a Resolve deep-link for each gap.

- Shows key metric cards: Consent Coverage %, open DPR Requests, active Breach Incidents, and pending DPIAs.
- Displays a live activity feed of compliance events across all modules, refreshed every 30 seconds.
- Shows real-time CERT-In (6-hour) and DPB (72-hour) countdown clocks for any active breach incidents.
- For DPO role users: surfaces the DPO Task Queue, listing all pending actions across all modules sorted by urgency (Critical, High, Medium, Low), with inline approve/reject capability.

2. Consents



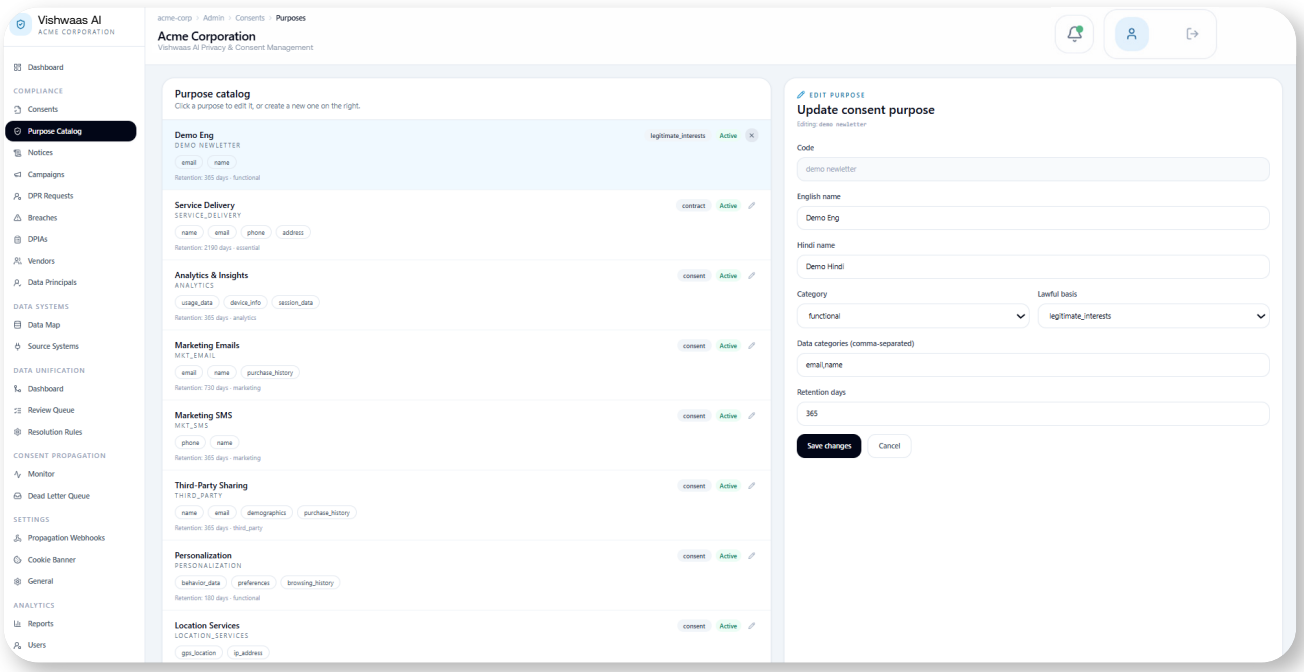
What it is

The Consents section is the central, immutable ledger of every consent decision made by every data principal across all channels and campaigns.

What it does

- Displays a searchable, filterable list of all consent records: principal, purpose, status (granted/withdrawn), channel, date, and language.
- Shows the full detail of any record including the exact notice text shown at the time of consent, in the language the principal viewed it.
- Displays the SHA-256 hash, RSA digital signature, Merkle chain hash, and RFC 3161 trusted timestamp for each record — the cryptographic proof of non-repudiation.
- Provides a Chain Integrity Verification function that re-computes the entire Merkle hash chain and confirms no records have been altered.
- Allows exporting the full consent audit trail as PDF or CSV, and individual records as signed PDF or JSON artefacts for regulatory submission.

3. Purpose Catalog



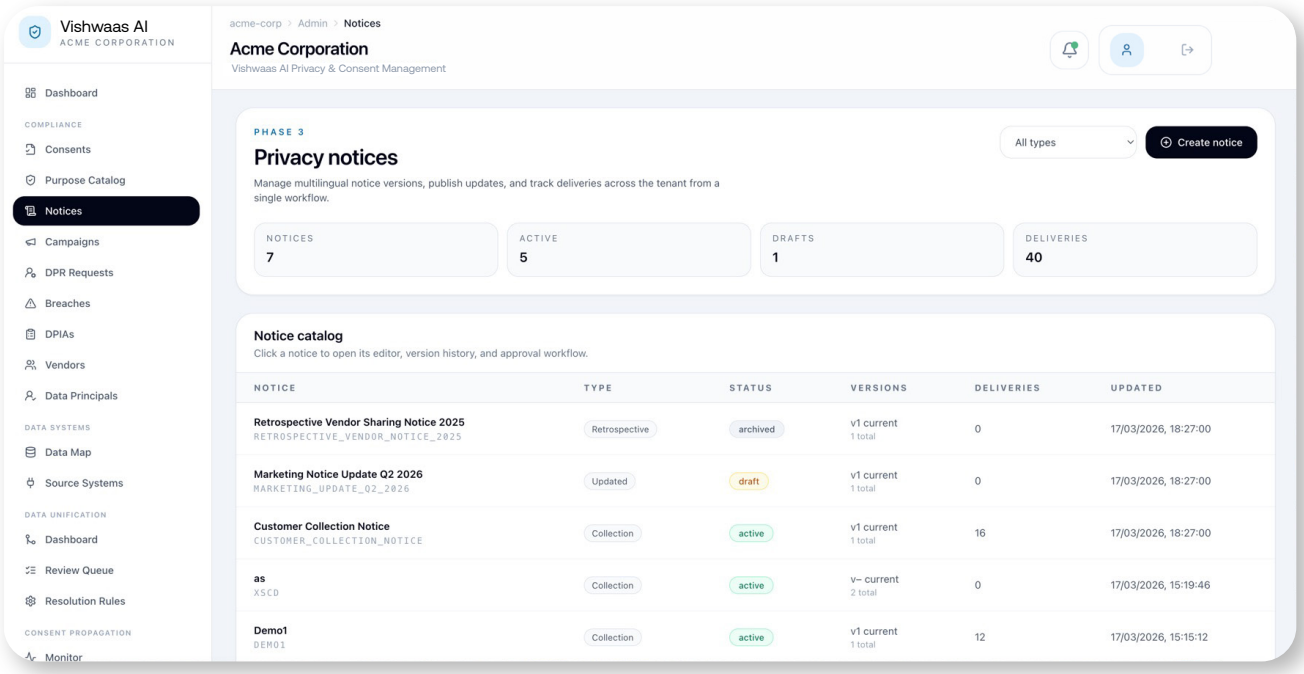
What it is

The Purpose Catalog is where all consent purposes are defined and managed. Every consent record in the system is tied to a purpose defined here.

What it does

- Lists all consent purposes with their name, category, lawful basis, status, and the number of consents recorded against each.
- Allows creating a purpose with: a multilingual name and description (22 Indian languages and English), category (Essential, Functional, Analytics, Marketing, Third-Party Sharing, or Employment), lawful basis (Consent or Legitimate Use), data categories, retention period, and linked processors.
- Provides a minor_restricted flag per purpose: when enabled, the API blocks consent for this purpose from a minor principal unless guardian approval exists.
- Links purposes to privacy notices. Editing a published purpose triggers a re-consent workflow for affected principals.

4. Notices



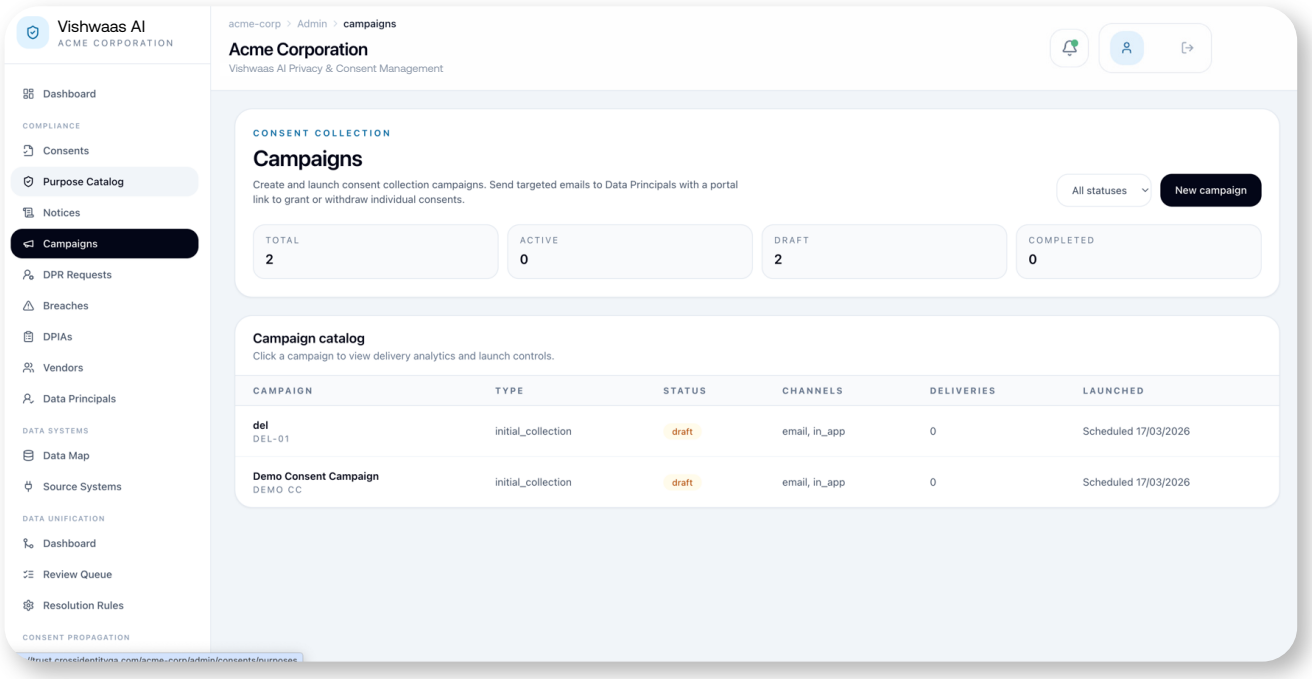
What it is

The Notices section is where the organisation creates, versions, and manages its privacy notices in compliance with Section 5 of the DPDP Act and Rule 3 of the DPDP Rules 2025.

What it does

- Lists all notices with version number, status (Draft, Under Review, Published, Archived), effective date, and linked purposes.
- Provides a rich-text builder with tab-based multilingual authoring for all 22 Indian languages and English simultaneously.
- Supports three notice types: Collection Notice, Retrospective Notice (for pre-Act legacy data under Rule 3), and Updated Notice.
- Enforces a Rule 3 compliance checklist: all 7 required elements must be present before the notice can be published.
- Runs an approval workflow: Draft → Submitted for Review → Approved by Legal or DPO → Published. Maintains full version history.
- Tracks delivery per principal: records when each notice was served, via which channel, and in which language.
- Triggers re-consent campaigns automatically when a material change is made to a published notice.

5. Campaigns



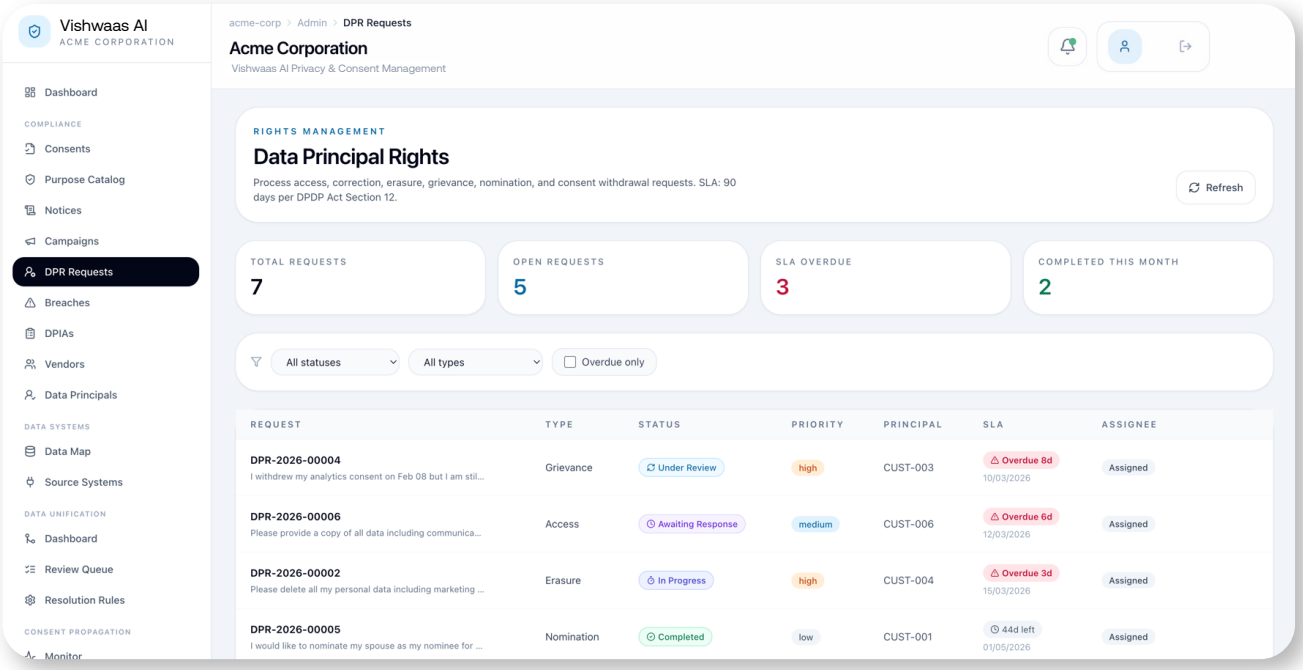
What it is

Campaigns is where the organisation runs structured consent collection drives — the primary mechanism for obtaining DPDP-compliant consent at scale, including retrospective consent for pre-Act data under Rule 3.

What it does

- Lists all campaigns with status (Draft, Pending DPO Approval, Approved, Running, Completed, Cancelled), audience count, channel, and response metrics.
- Allows creating a campaign with: a linked published notice, selected purposes, audience (all principals, those without consent for selected purposes, a custom segment, or an uploaded list), channels (Email, SMS, or both), token expiry period, and an optional schedule.
- Requires DPO approval before dispatch. The DPO can preview the exact notice and purpose cards the recipient will see before approving, in any of the 22 supported languages.
- On execution, generates one unique single-use personalised link per principal and dispatches it. The link opens a branded consent page the principal can act on without logging in.
- Shows live execution progress: tokens generated, dispatched, delivered, opened, and responded. Provides per-campaign analytics: response funnel, per-purpose consent rate, per-channel performance.
- Supports automatic re-send to non-responders after a configurable number of days.

6. DPR Requests



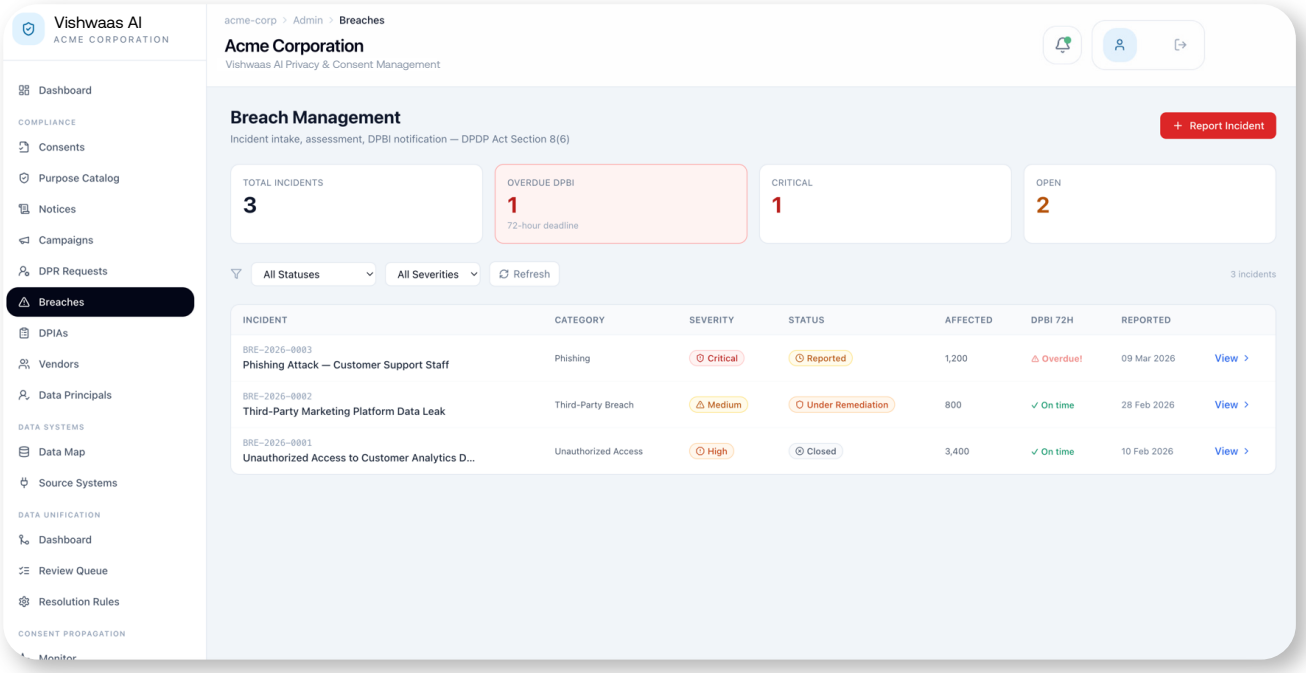
What it is

DPR Requests is the workflow management centre for all Data Principal Rights requests: Access, Correction, Erasure, Nomination, Grievance, and Portability.

What it does

- Lists all requests with reference number (DPR-YYYY-NNNNN), type, principal, submission date, status, assigned staff, and colour-coded SLA deadline indicator.
- Manages each request through a structured workflow: Submitted → Identity Verification → In Progress → Pending Approval → Completed / Rejected / Escalated.
- For erasure requests: runs an automatic Data Footprint Pull (showing every connected system where the principal's data exists) and a Legal Hold Check (identifying what can be erased vs what must be retained by law, citing the specific statute). Staff must acknowledge legal hold findings before erasure jobs are created.
- Creates per-system erasure jobs, dispatches cessation instructions to external processors, and generates an Erasure Certificate PDF on completion.
- For portability requests: packages the principal's data from all connected systems into a structured downloadable file with a time-limited secure link.
- Sends a tokenized 48-hour pre-erasure notification before deletion begins, allowing the principal to choose to keep their data or proceed — without logging in.
- Allows the DPO to escalate unresolved grievances to the Data Protection Board. Sends SLA breach alerts automatically to assigned staff and the DPO.

7. Breaches



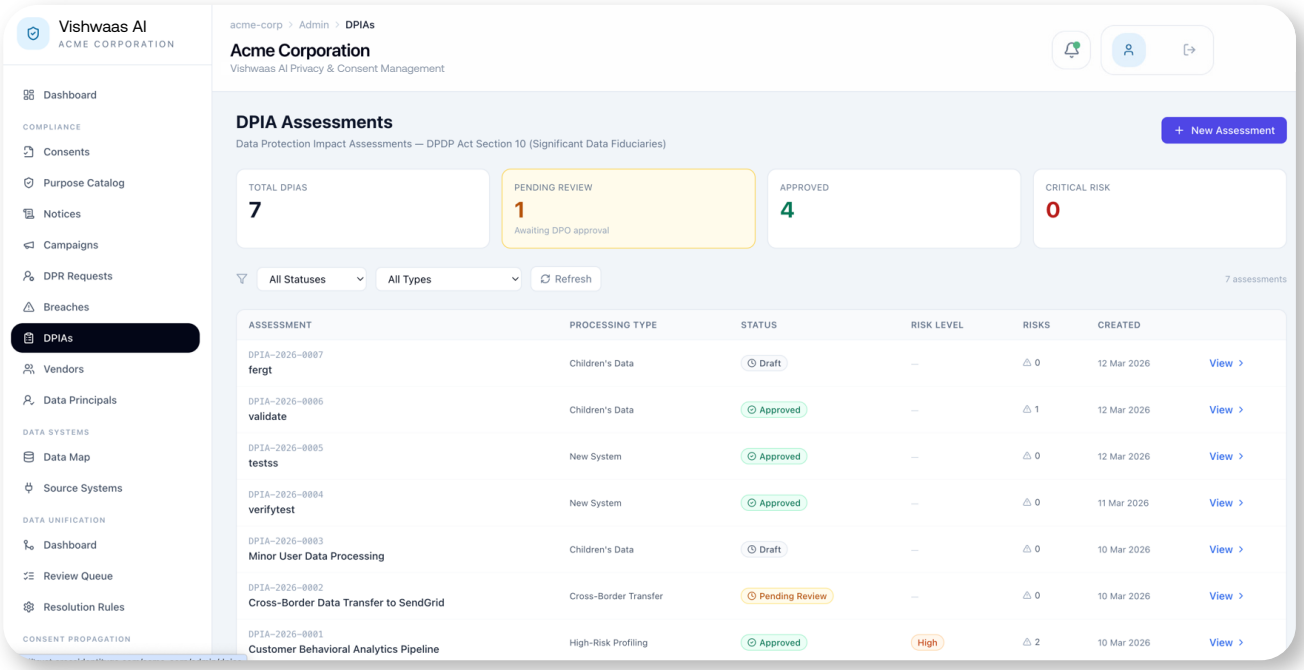
What it is

Breaches is the incident management centre for personal data breaches, covering the full lifecycle from intake to closure.

What it does

- Lists all incidents with reference number (BRI-YYYY-NNNNN), type, severity, status, CERT-In notification status, DPB notification status, and date reported.
- The Report a Breach button is available in the top navigation for all admin roles at all times. The intake form captures: discovery timestamp, breach type, affected systems, affected data categories, estimated principals, and immediate containment actions.
- On submission, two regulatory clocks start simultaneously and are displayed as live countdowns: CERT-In clock (6-hour deadline under Rule 7) and DPB clock (72-hour deadline under Section 8(6)). Both change colour as deadlines approach and send escalation alerts at defined thresholds.
- CERT-In and DPB notification workflows are each a multi-step process: auto-generated draft → DPO review and edit → DPO approval → mark as submitted with reference number entry → clock freezes showing submission timestamp.
- Principal notification composer is pre-filled from the impact assessment, requires DPO approval, and dispatches a unique tokenized link per affected principal to a branded breach notification page (no login required).
- Tracks remediation actions with owners, deadlines, and evidence uploads. Incident cannot be closed until all remediations are complete. Generates a Breach Closure Report PDF on closure.

8. DPIAs



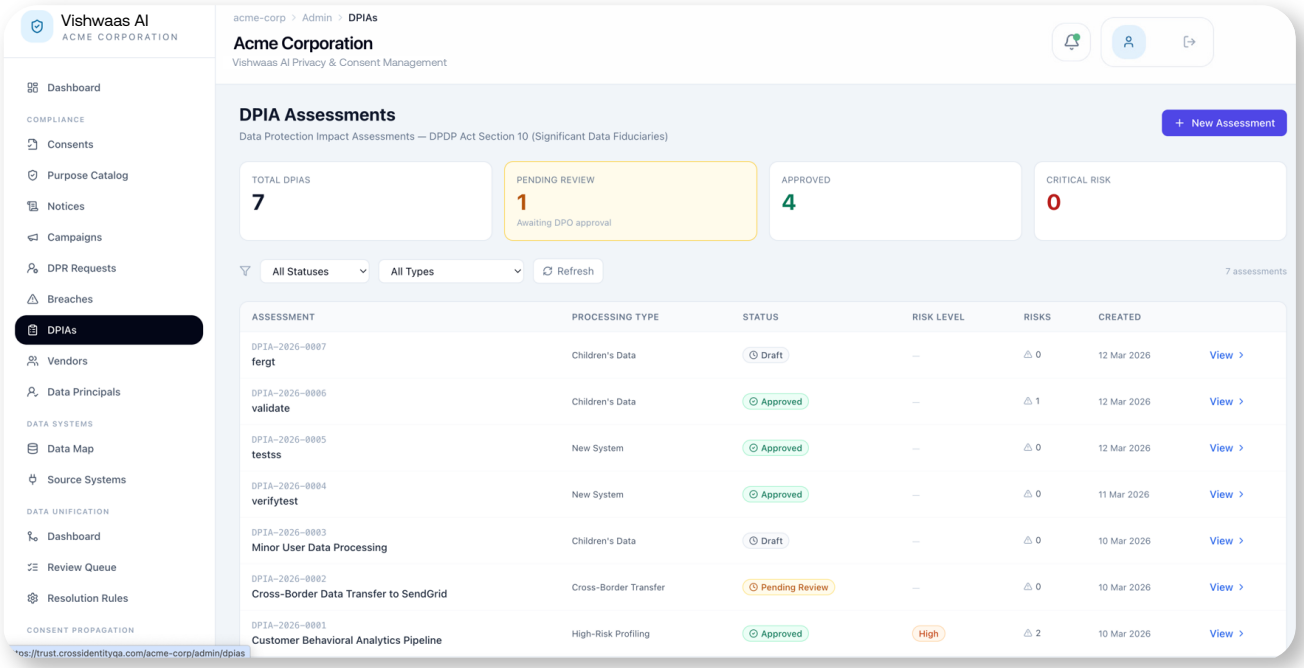
What it is

DPIAs manages Data Protection Impact Assessments — mandatory evaluations before initiating high-risk processing activities, required for Significant Data Fiduciaries.

What it does

- Lists all DPIAs with title, linked processing activity, risk score, risk level (Low/Medium/High/Critical), status, DPO approval status, and next review date.
- Provides a step-by-step guided questionnaire covering processing description, data categories, volume, necessity and proportionality, and risk identification.
- Auto-calculates a risk score 0–100 based on data sensitivity, volume, processing nature, and impact potential.
- Provides a structured risk registry with likelihood, impact, and planned mitigation per identified risk. Tracks mitigation implementation with assigned owners and deadlines.
- Routes completed DPIAs through a DPO approval chain. Displays a radar chart for risk dimensions and generates a printable DPIA Report PDF for Board or auditor submission.

9. Vendors



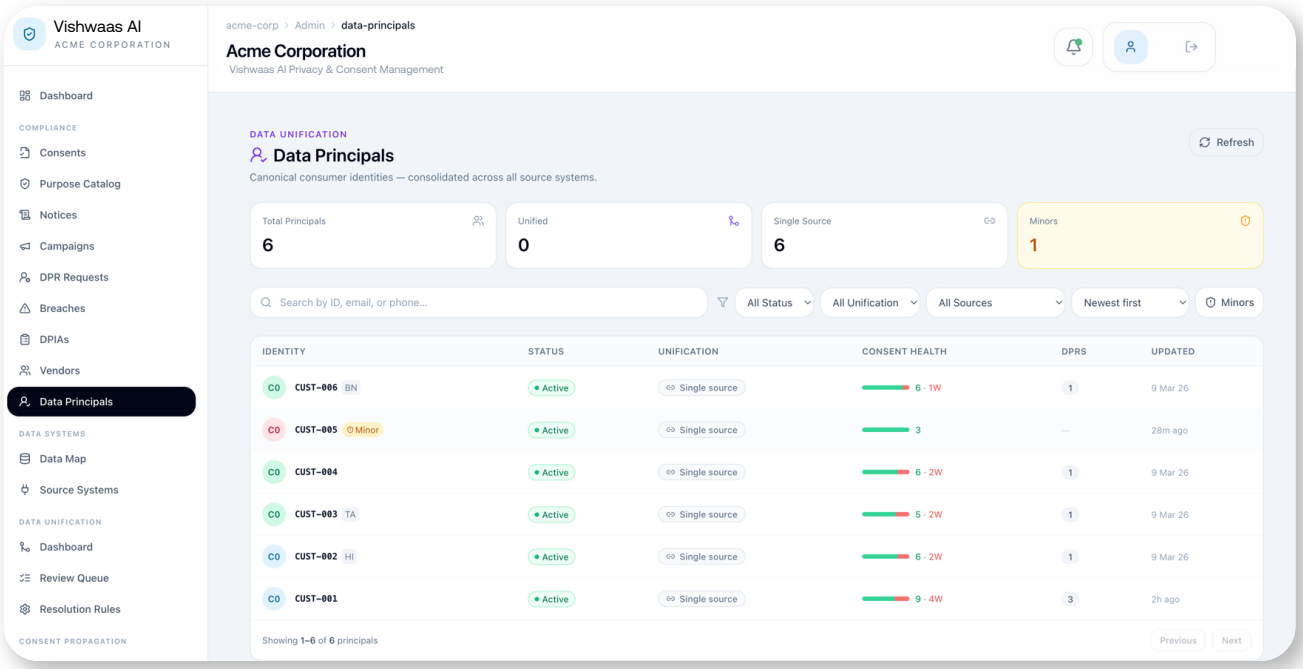
What it is

Vendors is the organisation's data processor registry for onboarding, assessing, and continuously monitoring all third-party vendors who process personal data on the organisation's behalf.

What it does

- Lists all vendors with name, type (Processor/Sub-Processor/Joint Controller), country, risk level, DPA status, DPA expiry date, and lifecycle status.
- Allows generating a DPDP-compliant DPA from a built-in clause library (required clauses locked, optional clauses togglable), previewing the full document, and dispatching for e-signature via Leegality. DPA activates automatically when both parties sign.
- Automatically flags vendors outside India as cross-border transfers and checks the destination country against the government restricted country list.
- Manages cessation instructions: when a principal withdraws consent for a purpose shared with a vendor, a cessation instruction is auto-created, dispatched to the processor liaison, and tracked through acknowledgement and confirmation.
- Sends DPA expiry alerts. Manages vendor lifecycle: Pending Review → Approved → Active → Suspended → Terminated.

10. Data Principals



What it is

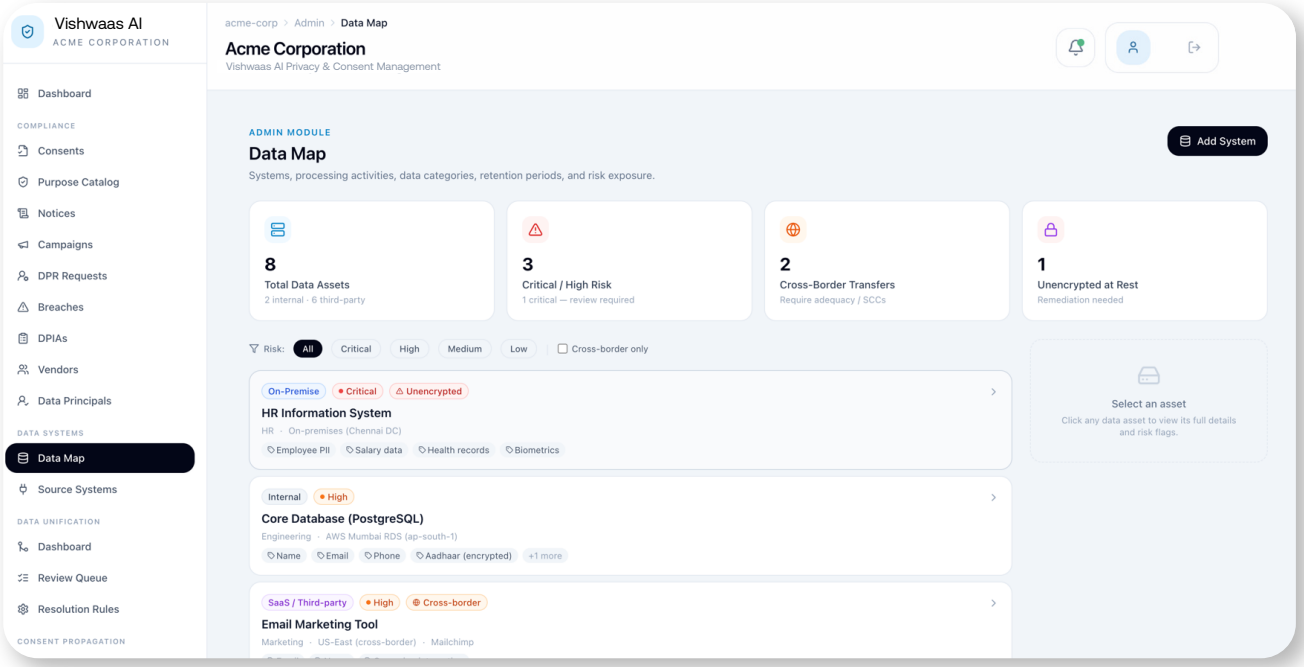
Data Principals is the organisation's unified registry of all individuals whose personal data is held and processed — customers, users, employees, or any other individuals.

What it does

- Lists all principal records with name, email, consent status summary, minor flag, and last activity date.
- Each record shows: full profile, identity graph (external IDs across all connected systems), consent decisions per purpose, rights request history, and complete activity timeline.
- Shows the data footprint: every system holding data for this individual, data categories held per system, and the responsible processor.
- For minor principals: shows the is_minor flag, age verification method, guardian email, and per-purpose guardian consent status. Allows sending a guardian consent request directly from the record.
- Allows staff to submit a rights request on behalf of a principal, manually flag a principal as a minor, and link a guardian.

DATA SYSTEMS

11. Data Map



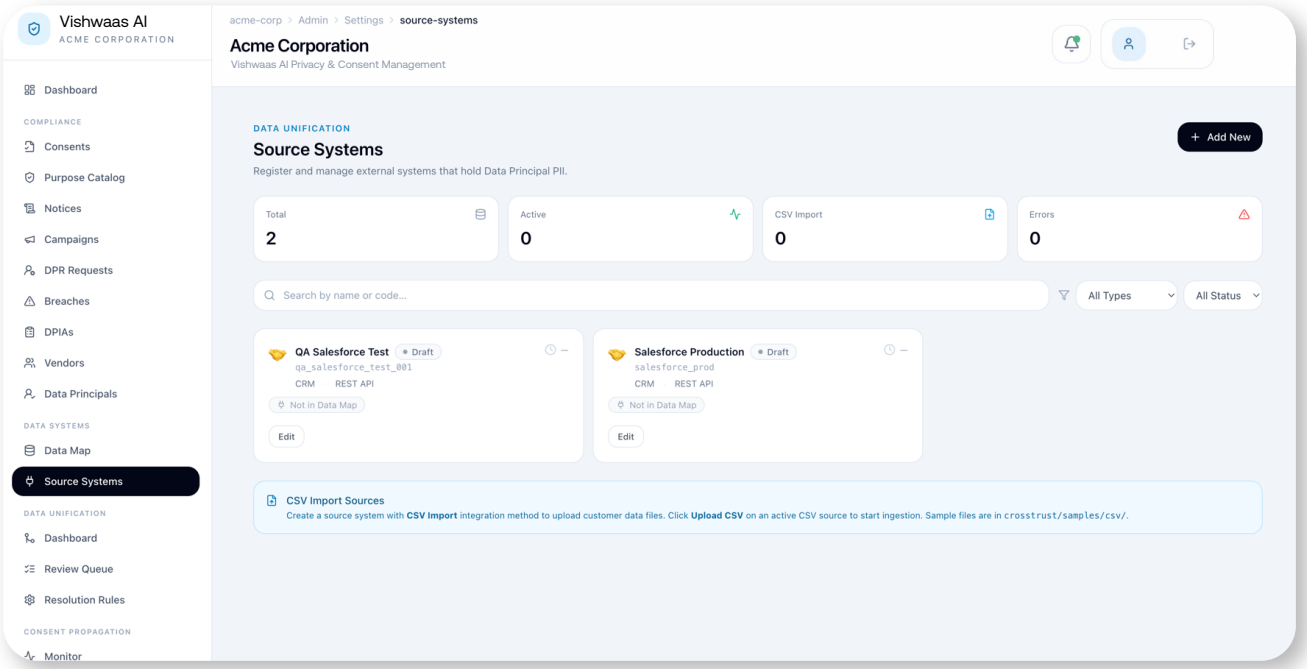
What it is

The Data Map is the organisation's visual Record of Processing Activities (RoPA) — an interactive diagram showing how personal data flows between all internal systems and external processors.

What it does

- Renders an interactive diagram with internal system nodes and processor nodes. Edges show data flows labelled with data categories. Cross-border transfer edges are visually distinct.
- Clicking any node opens a detail panel: name, data categories, DPA status. Clicking any edge shows data categories flowing, transfer mechanism, DPA status, and blacklist check result.
- An Open Gaps panel automatically identifies compliance discrepancies: assets with no processing activity, activities with no lawful basis, processors with no active DPA, unregistered cross-border transfers, purposes with no linked notice, and uncategorised data categories. Each gap has a Resolve button navigating directly to the fix.
- The gap count feeds into the Compliance Score. Allows exporting the full RoPA as PDF, CSV, or JSON.

12. Source Systems



What it is

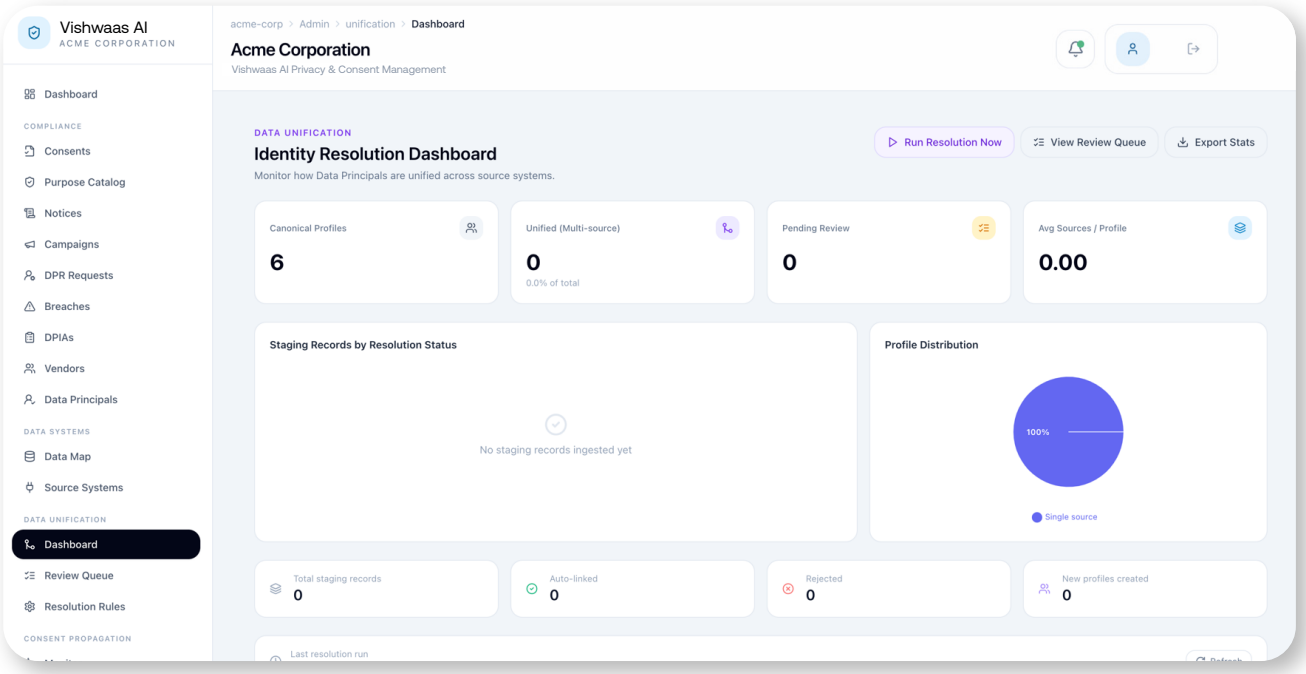
Source Systems is where Vishwaas AI is connected to all external applications and databases holding personal data — the foundation for the identity graph, data discovery, RoPA population, and consent propagation.

What it does

- Lists all connected systems with type, connection status, last sync timestamp, and principal record count.
- Supports pre-built connectors for: Salesforce, HubSpot, Shopify, CleverTap, Freshdesk, Darwinbox, PostgreSQL/MySQL/MongoDB, AWS S3/Azure Blob/GCS, and a generic REST/GraphQL connector for any custom API.
- On connection, triggers an automated PII Discovery Scan identifying all personal data fields and categorising them by type.
- Maintains continuous real-time or scheduled sync after initial connection. Allows configuring connector-specific actions — the native system commands triggered on consent changes (e.g. DoNotEmail flag in CRM, unsubscribe in email marketing platform).

DATA UNIFICATION

13. Dashboard (Data Unification)



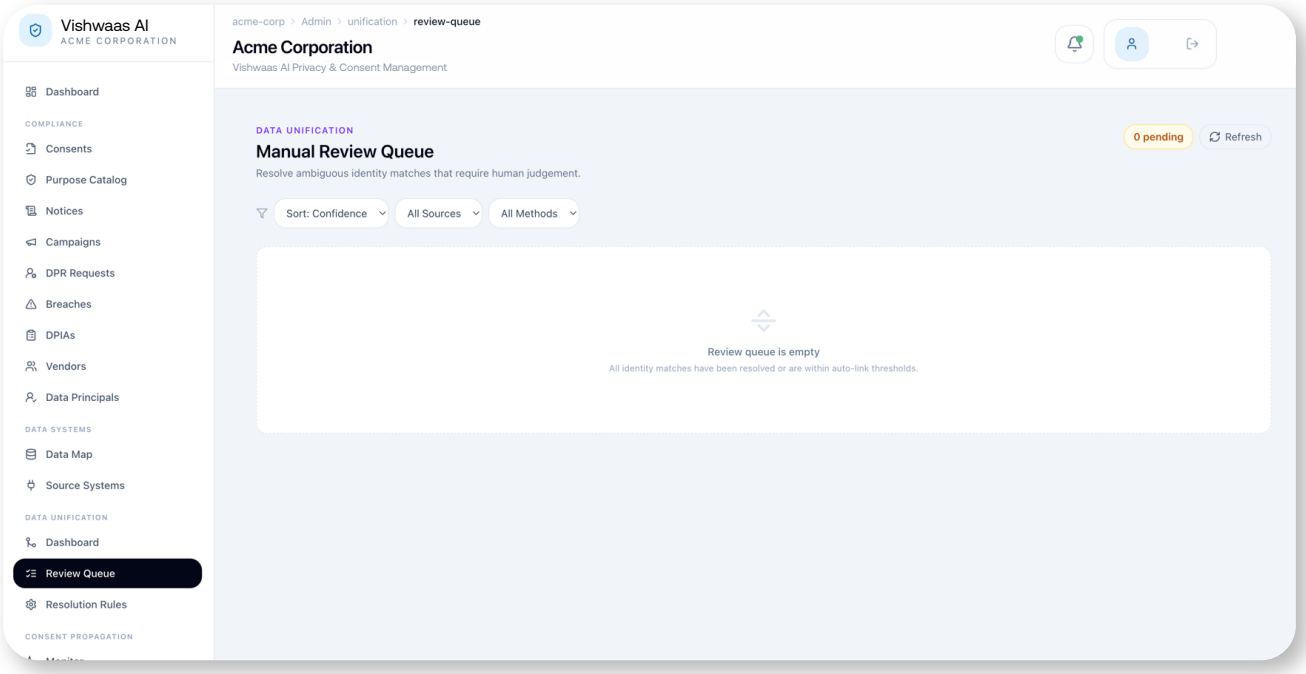
What it is

The Data Unification Dashboard provides an overview of the identity resolution process — how Vishwaas AI matches and merges records about the same individual from multiple connected systems into a single unified Data Principal profile.

What it does

- Displays summary metrics: total principals identified, matches confirmed, matches pending manual review, and duplicates flagged.
- Shows trends in match rates and resolution queue volume over time, with a breakdown by match type: deterministic (exact match on email, phone, Aadhaar hash, PAN, customer ID) versus probabilistic (fuzzy Jaro-Winkler name and address matching).

14. Review Queue



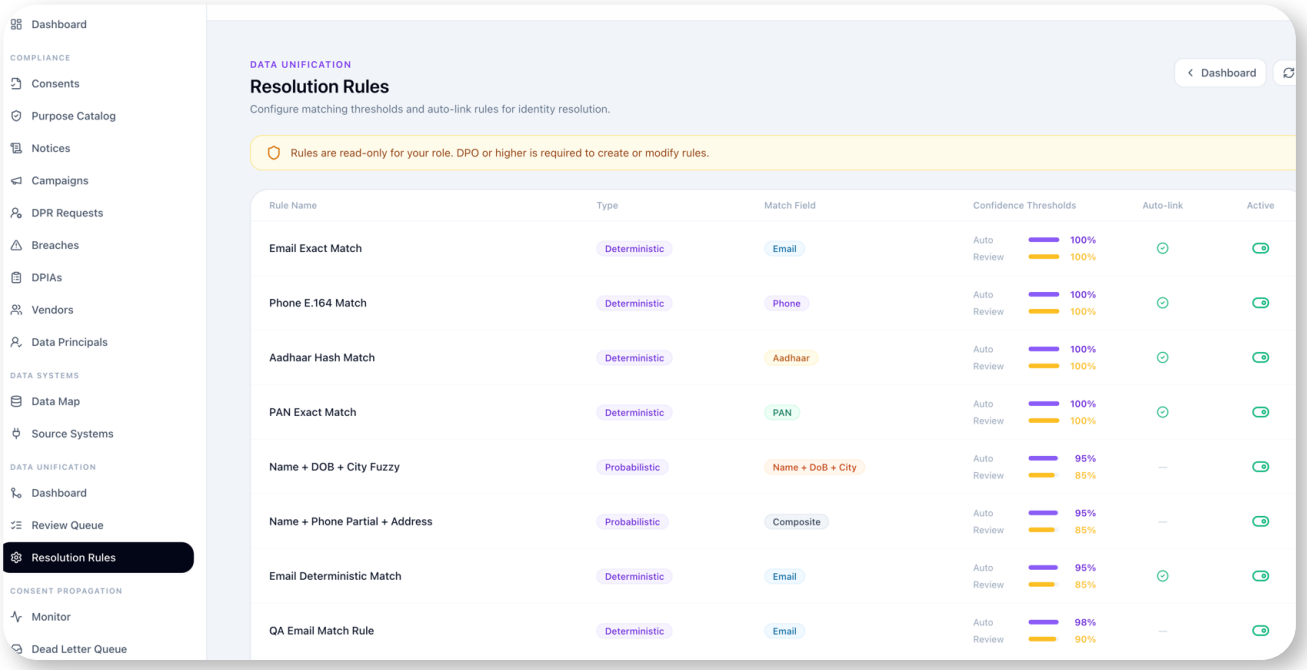
What it is

The Review Queue is where Privacy Managers act on probabilistic identity matches the system could not confirm automatically — cases where two records are likely the same person but require human judgement.

What it does

- Lists all pending matches with: the two records being compared, confidence score, matching fields (name, DOB, address fragments), and source systems.
- For each match, shows both records side by side. The reviewer can Confirm (merging into one unified profile) or Reject (keeping as separate individuals, preventing future matching of this pair).
- Every decision is written to an immutable merge audit trail with: reviewer identity, timestamp, records involved, and confidence score. Allows bulk assignment of items to staff members.

15. Resolution Rules



What it is

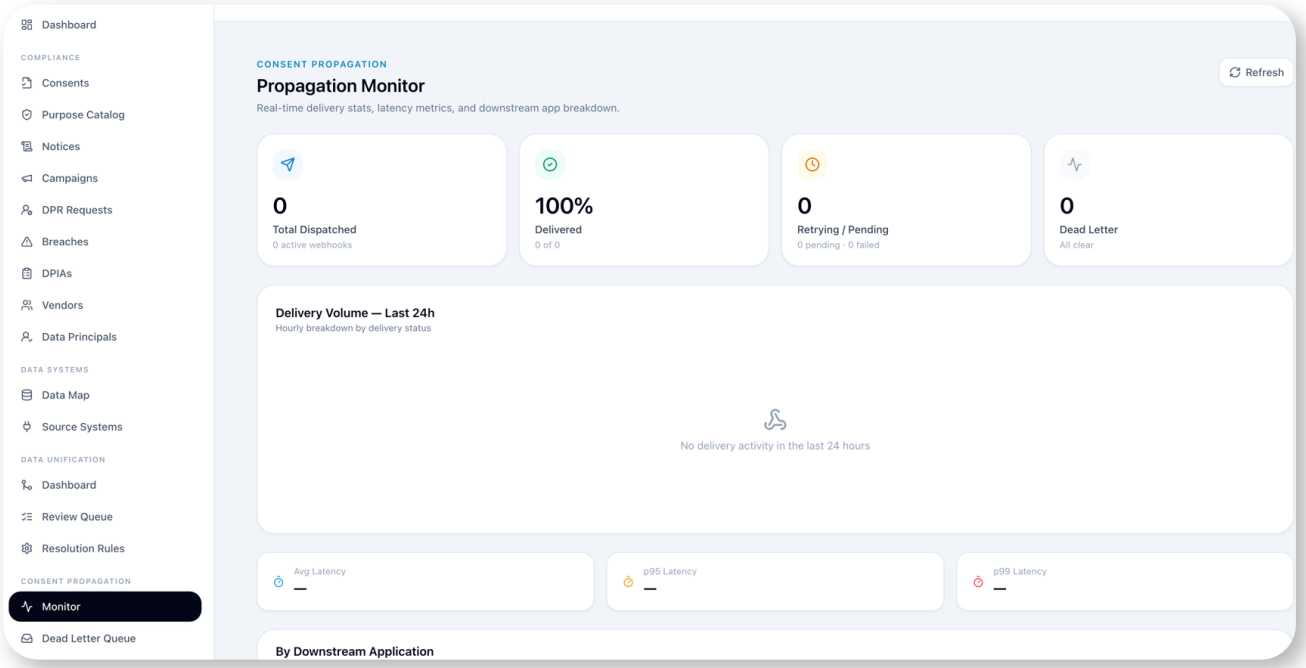
Resolution Rules is where administrators configure how the identity resolution engine behaves — which fields are used for matching, what confidence thresholds trigger automatic vs manual review, and how cross-system data conflicts are resolved.

What it does

- Configures deterministic matching fields: which fields across connected systems are treated as definitive identifiers.
- Sets probabilistic matching thresholds: the confidence percentage above which a fuzzy match is auto-confirmed, and the range that routes to the manual Review Queue.
- Defines conflict resolution priority: when connected systems have conflicting values for the same field, which system is the source of truth.

CONSENT PROPAGATION

16. Monitor



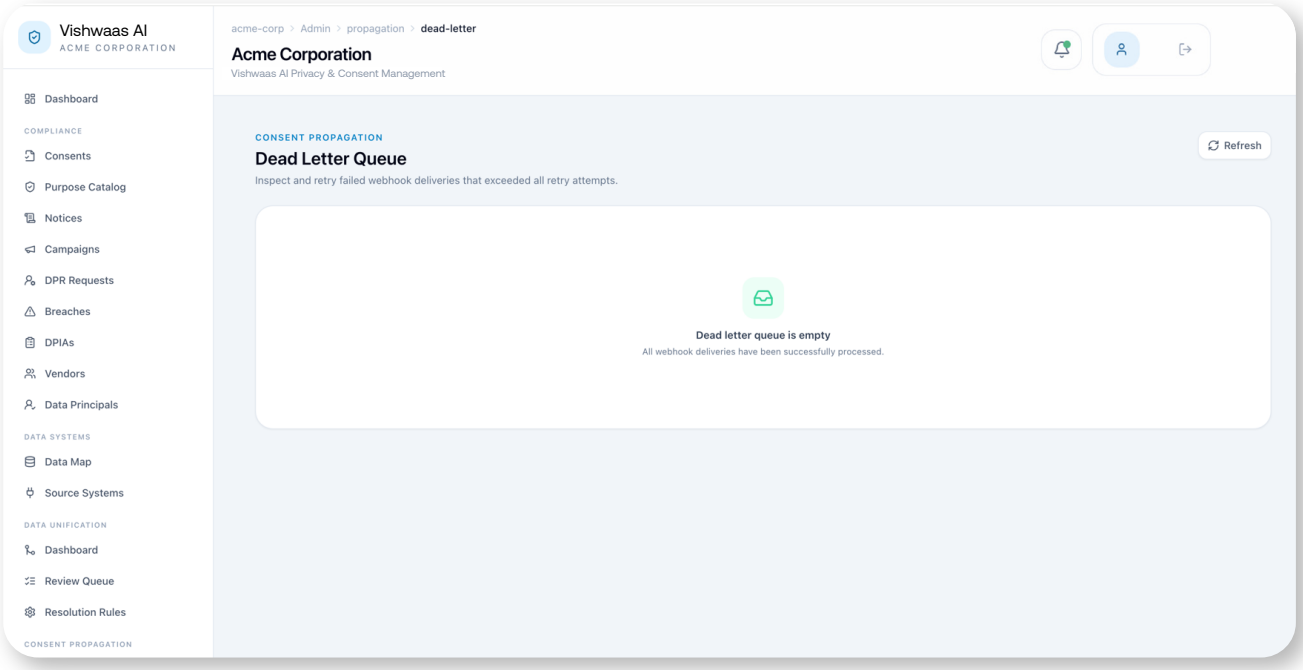
What it is

The Monitor is the real-time view of consent propagation — the process by which consent decisions are automatically communicated to all downstream connected systems. When a principal grants or withdraws consent, Vishwaas AI instructs every connected system to act on it.

What it does

- Displays a live feed of all propagation events: principal, purpose, event type (grant/withdrawal), target system, delivery status (delivered/pending/failed), and timestamp.
- Shows aggregated metrics: total events in a period, delivery success rate, and failed deliveries. Allows filtering by system, event type, status, and date range.
- Allows manual retry of failed events. Provides a drill-down showing the full payload sent and the response received from the target system.

17. Dead Letter Queue



What it is

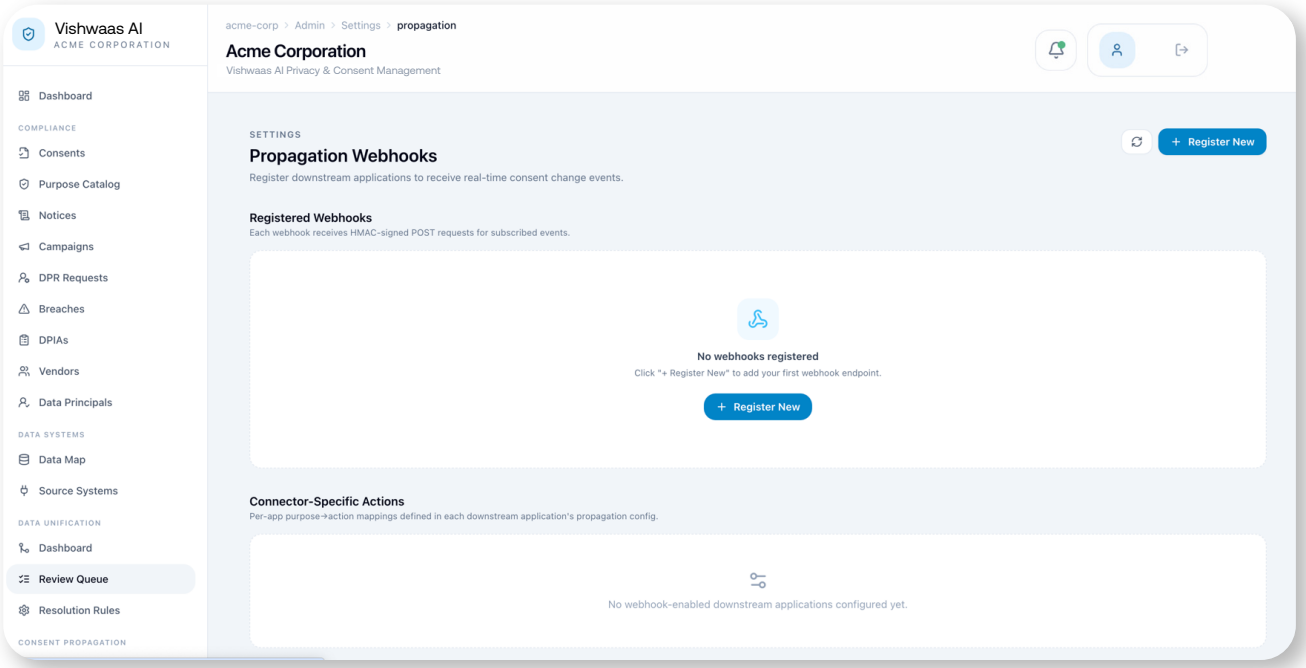
The Dead Letter Queue holds consent propagation events and webhook deliveries that have persistently failed after all automatic retry attempts (three retries with exponential backoff).

What it does

- Lists all failed events with: event type, target system or webhook endpoint, number of retries, last error message, and original timestamp.
- Allows reviewing the full payload and error history per event. Supports manual retry of individual events or bulk retry after resolving the underlying issue.
- Allows permanently dismissing an event with a recorded reason when delivery is no longer required or possible.

SETTINGS

18. Propagation Webhooks



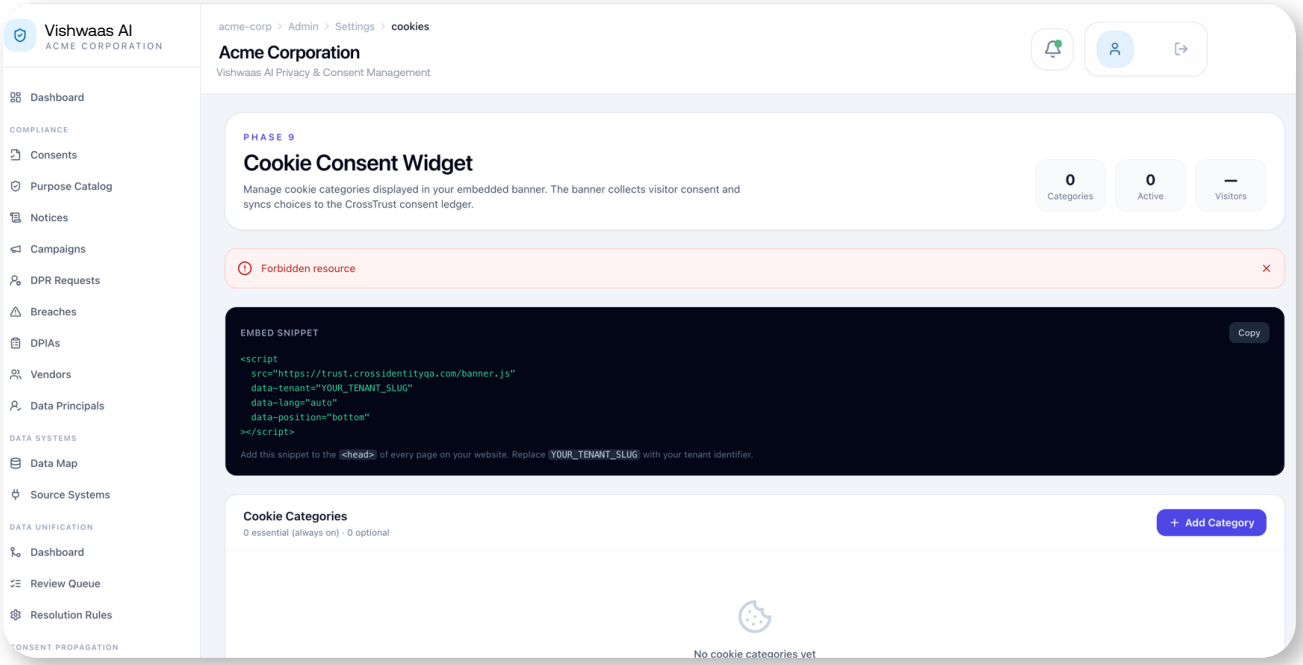
What it is

Propagation Webhooks is where the organisation registers external HTTP endpoints to receive real-time notifications when compliance events occur in Vishwaas AI, enabling connected systems to stay in sync without polling.

What it does

- Lists registered endpoints with URL, subscribed event types, status, and delivery success rate.
- Supports 9 event types: consent.granted, consent.withdrawn, consent.expired, dpr.request.created, dpr.request.completed, breach.reported, breach.dpbi_notified, notice.published, and vendor.status_changed.
- Signs every outgoing payload with X-Vishwaas AI-Signature (HMAC-SHA256) for authenticity verification. Retries with exponential backoff; persistent failures go to the Dead Letter Queue.
- Provides a Test Endpoint function to verify connection and signature verification before going live.

19. Cookie Banner



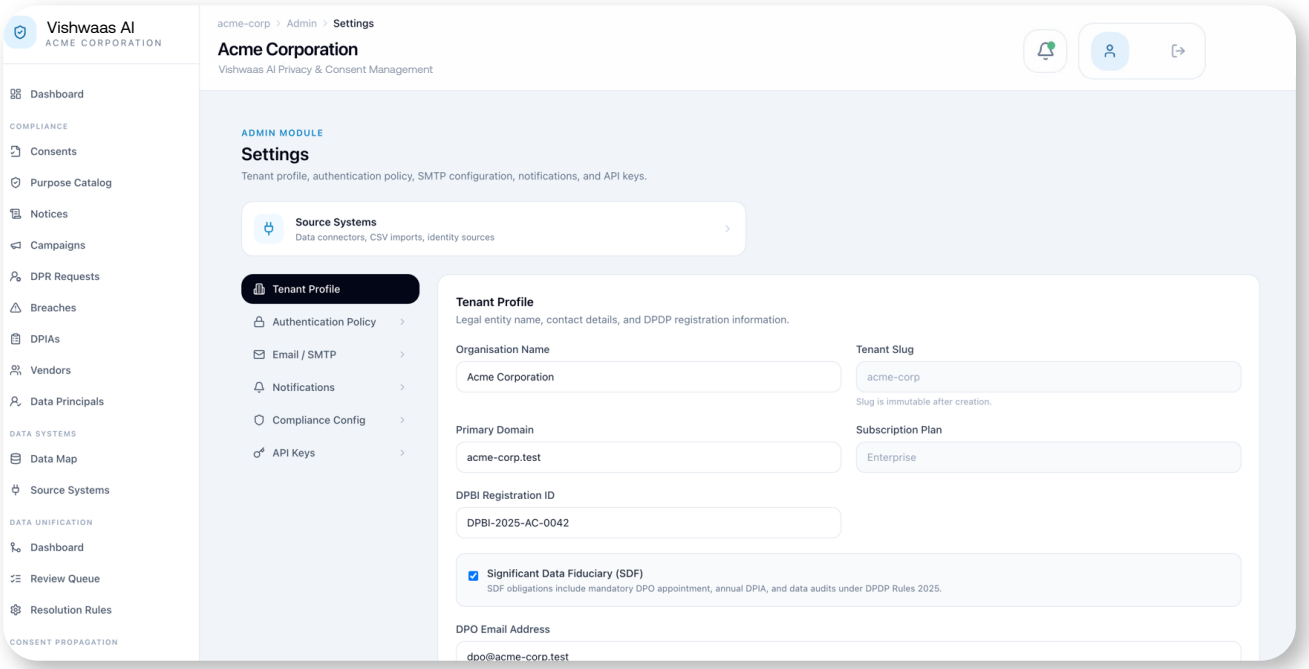
What it is

Cookie Banner is where the organisation configures the embeddable JavaScript cookie consent widget for their website. All cookie consent decisions are recorded in the Vishwaas AI consent ledger.

What it does

- Configures the banner appearance: position (bottom bar, top bar, or modal), branding (logo, colour), and language behaviour.
- Provides a Cookie Scanner that discovers and categorises all cookies on the website, mapping them to four categories: Essential (always on), Functional, Analytics, and Marketing.
- Maps each cookie category to a consent purpose in the Purpose Catalog. Supports all 22 Indian languages and English with browser language auto-detection.
- Generates the embed code (a single script tag) for the organisation's website. Configures the three DPDP-required action buttons: Accept All, Accept Selected, and Reject All. Provides a Preference Centre reopener for returning visitors.

20. General



What it is

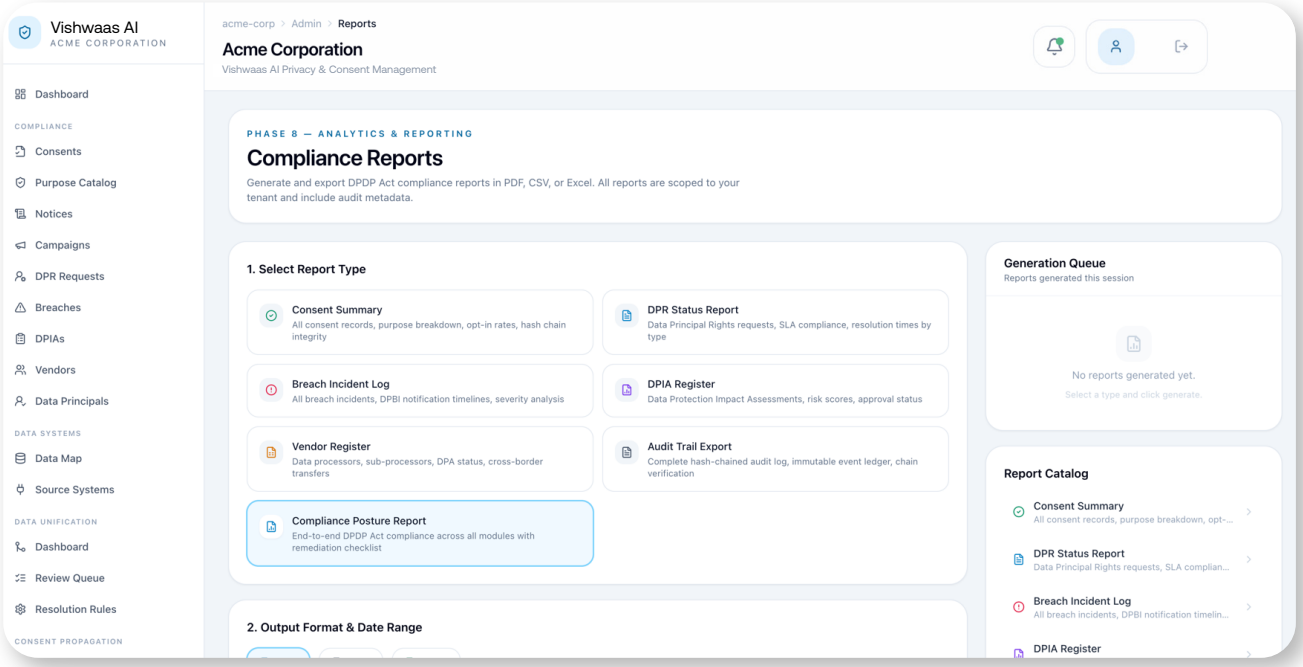
General Settings is the central configuration area for the organisation's Vishwaas AI tenant, covering the organisation profile, portal branding, user management, and API access.

What it does

- Organisation Profile: legal name, DPBI registration ID, SDF flag, industry, default language, timezone.
- DPO and Grievance Officer: name, email, and contact details, displayed in the portal and in all regulatory notifications.
- Portal Branding: logo, brand colours, custom domain for the Data Principal Portal, with live preview.
- User Management: create, update, and deactivate internal users. Assign from 11 system roles. View login history per user.
- API Keys: create, view, and revoke scoped API keys for system-to-system integration.
- Embed Codes: generate consent widget and DSAR submission form embed codes for the organisation's website.

ANALYTICS

21. Reports



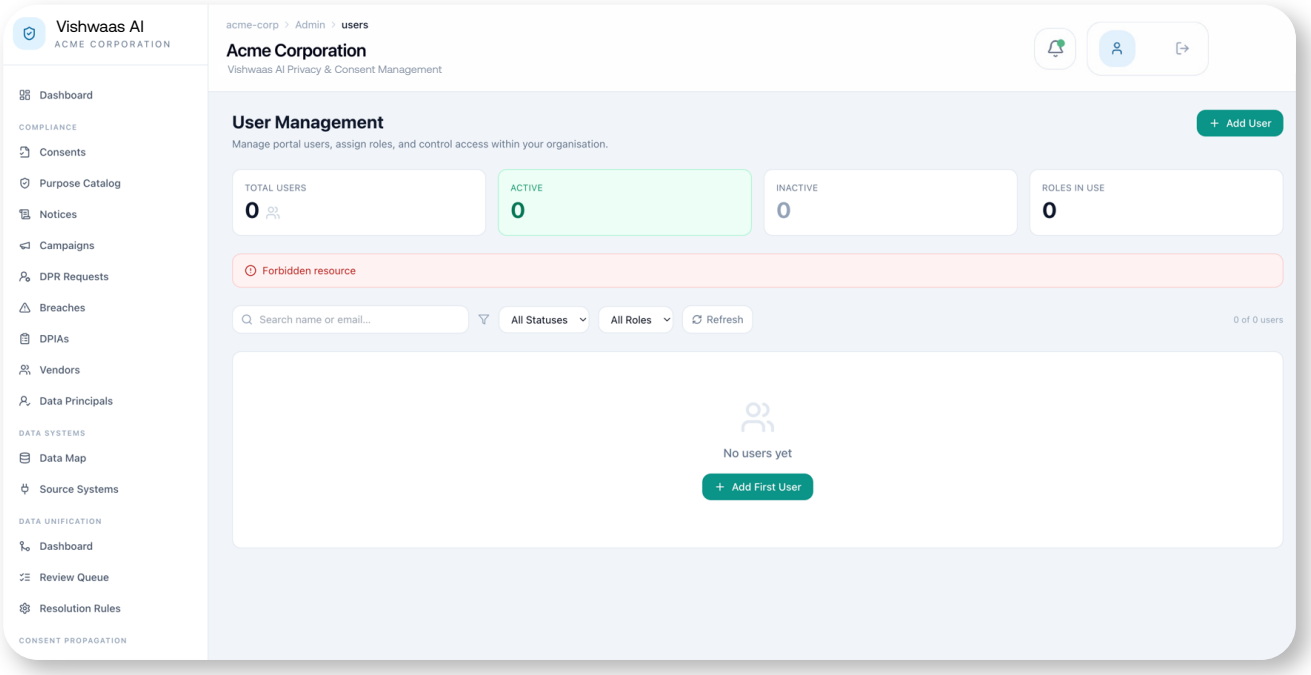
What it is

Reports provides on-demand and scheduled compliance reporting for internal governance, Board submission, regulatory inspection, and legal defence.

What it does

- Generates on-demand reports in PDF and Excel: Compliance Summary, Consent Audit, DPR Summary, Breach Report, Vendor Compliance, and Training Completion. All reports are filterable by date range.
- Schedules automated weekly or monthly report delivery by email to configured recipients.
- Generates a Board of Directors Report for SDF tenants, formatted for executive audiences.
- Generates a DPB Investigation Pack: a formal, bookmarked, multi-section PDF evidence bundle structured by DPDP Act section, assembling evidence from all modules into a single indexed document with a cryptographic audit chain verification result. Used when the organisation is under DPB investigation.
- All generated documents are watermarked, date-stamped, and attributed to the generating user.

22. Users



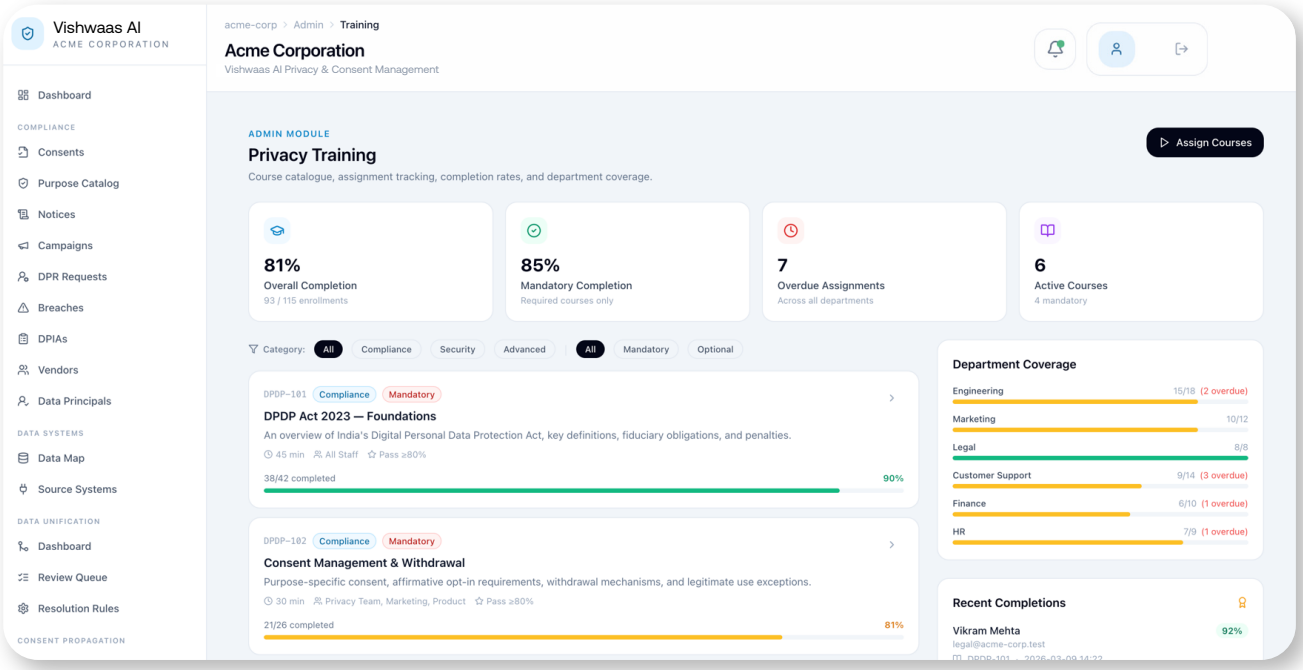
What it is

Users provides a view of all admin users active in the tenant, their roles, account status, and activity history.

What it does

- Lists all admin users with name, email, assigned role(s), account status, last login, and MFA status.
- Allows creating new users by entering name, email, and assigning one or more of the 11 system roles. Allows editing roles and deactivating accounts. Deactivated users cannot log in; their historical actions remain in the audit trail.
- Displays the login audit trail for any user: every login attempt with IP address, device, and timestamp. Shows a summary of recent activity per user.

23. Training



What it is

Training is the privacy awareness e-learning platform for internal staff, covering course assignment, completion tracking, certification, and policy acknowledgement.

What it does

- Provides a library of pre-built privacy courses covering: the DPDP Act, consent handling, breach response, data rights, and children's data protection. Supports role-specific tracks for IT, HR, Marketing, Legal, and Leadership.
- Allows creating custom courses with text modules, video, and resources. Each course has a configurable MCQ assessment, passing score threshold, and certificate validity period (default 12 months).
- Assigns courses to individual users, departments, or roles with a due date. Staff take courses module by module, complete the assessment, and receive a downloadable certificate PDF automatically on passing.
- Displays a completion dashboard by course, department, and user for audit submission. Sends reminders for overdue assignments. Handles certificate expiry and re-assignment for mandatory courses.
- Policy Acknowledgement workflow: publish a policy, assign to staff, staff acknowledge by clicking confirmation. Creates a non-repudiated record with user identity, policy version, timestamp, and IP address.

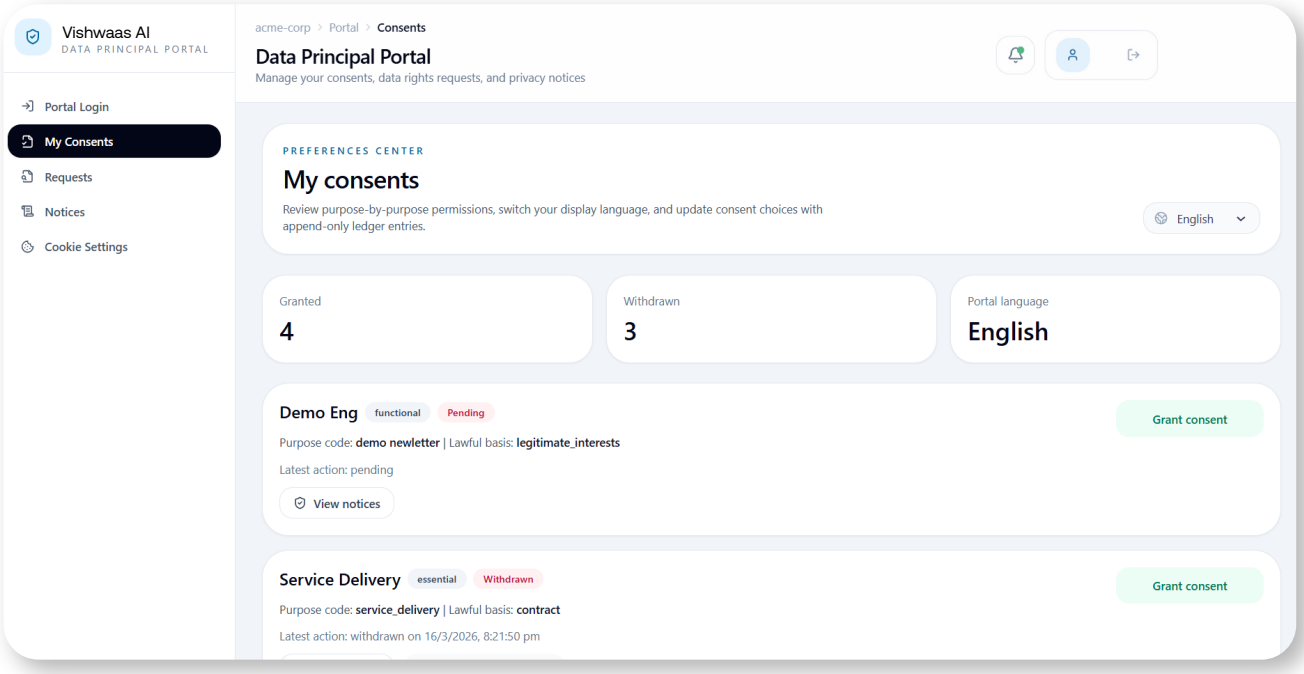
Part 2 — Data Principal Portal

The Data Principal Portal is the self-service interface for individuals to manage their privacy preferences with the organisation. It is fully white-labelled with the organisation's branding, available in all 22 Indian languages and English, fully mobile-responsive, and accessible at the organisation's configured portal domain.

24. Portal Login

The Portal Login screen displays the organisation's branding (not Vishwaas AI branding). The data principal enters their email address and receives a 6-digit OTP. No password is required or stored. On successful verification, the principal is directed to their My Consents dashboard. After 5 failed OTP attempts, the account is temporarily locked.

25. My Consents



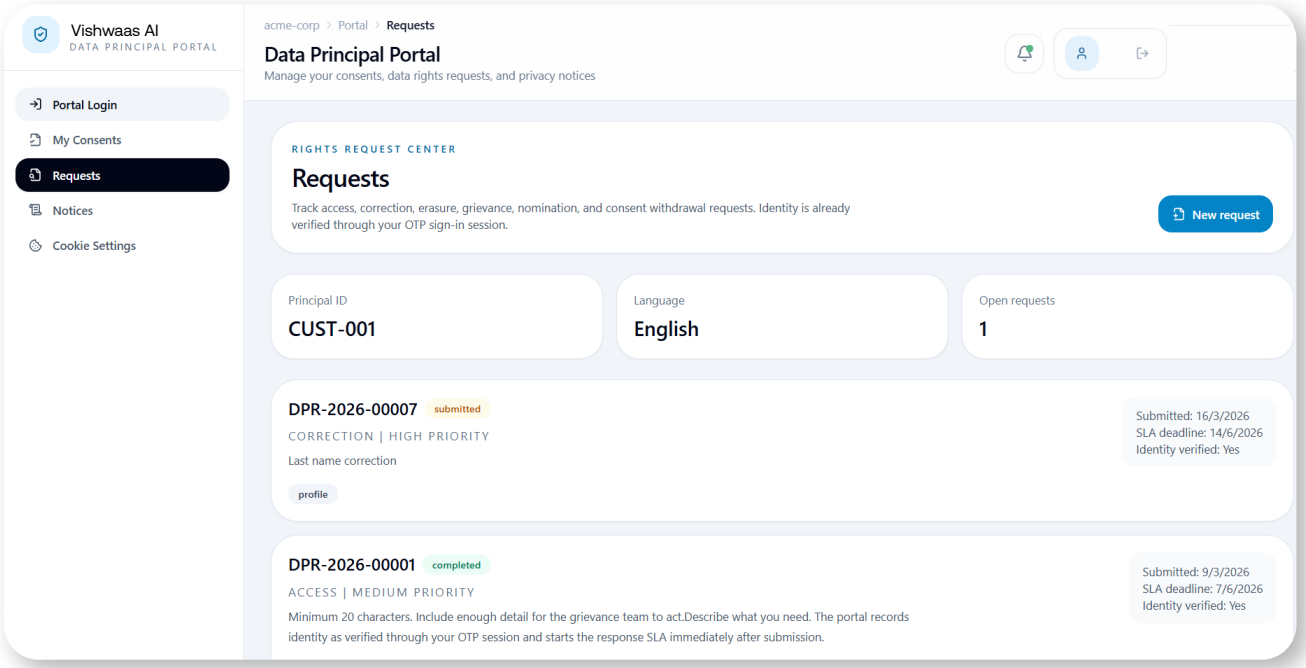
What it is

My Consents is the primary screen of the Data Principal Portal. It gives the principal a complete view of all consent purposes and allows them to manage each one individually.

What it does

- Displays one card per consent purpose: purpose name in the principal's selected language, a plain-language description, data categories involved, retention period, and current status with an ON/OFF toggle.
- Each toggle change takes effect immediately and is recorded in the consent ledger with a cryptographic hash. Each card links to the exact notice version shown at the time consent was originally given.
- Provides a Withdraw All Consents action with a confirmation dialog.
- For minor principals: all non-Essential toggles are disabled and labelled "Consent managed by your guardian."
- Shows a notification when any consent is approaching expiry, with a Renew option.

26. Requests



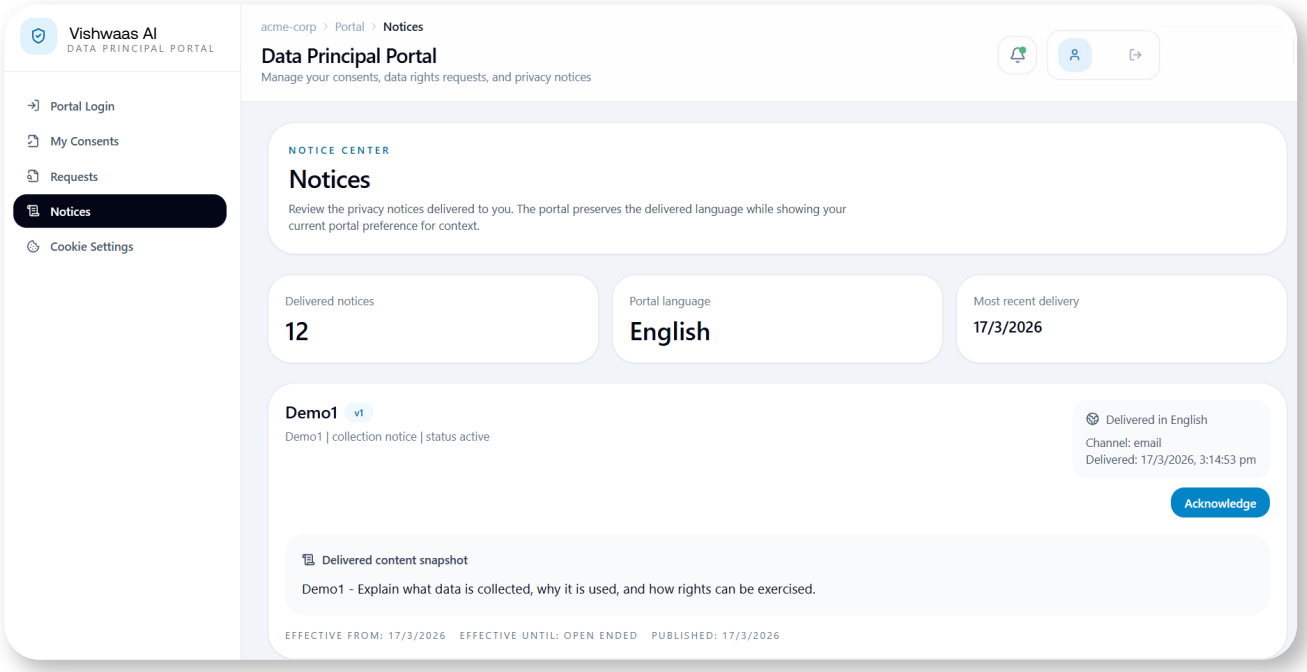
What it is

Requests is where data principals submit and track their formal rights requests: Access, Correction, Erasure, Portability, Grievance, and Nomination.

What it does

- Lists all previously submitted requests with reference number, type, submission date, current status, and SLA deadline.
- Allows submitting a new request by selecting the type and providing a description. A reference number is generated and displayed immediately.
- Request detail view shows the full status timeline, any messages from the assigned staff member, and downloadable documents (erasure certificate, portability data package).
- Shows the Grievance Officer's name and contact details prominently in the Grievance request flow.

27. Notices



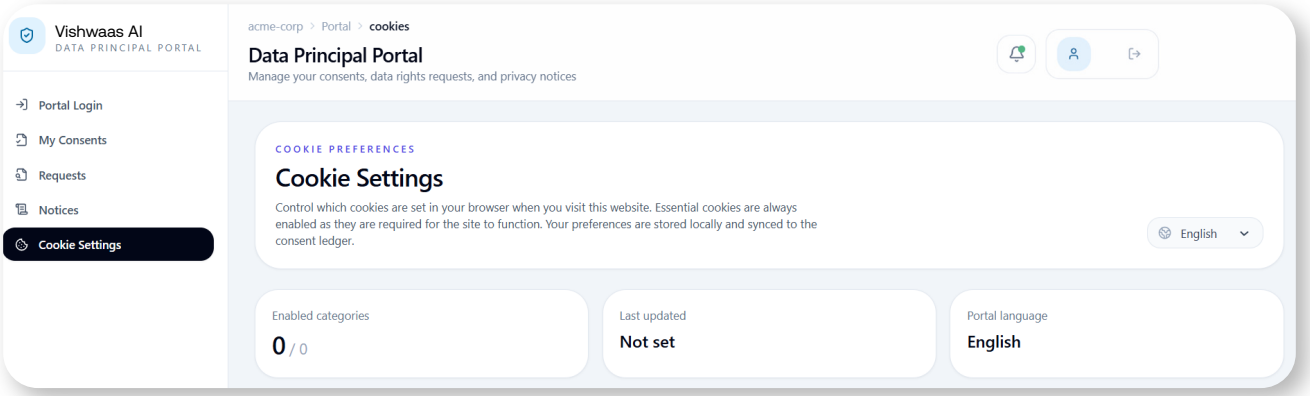
What it is

Notices is the principal's personal library of all privacy notices the organisation has delivered to them.

What it does

- Lists all notices delivered to this principal: notice name, delivery date, channel, and language.
- Allows reading the full text of any notice in the preferred language via the language selector. Shows version history for each notice.
- Breach notification communications are accessible here after their tokenized link has expired, allowing the principal to refer back to breach notifications at any time.

28. Cookie Settings



What it is

Cookie Settings allows the principal to manage their cookie preferences from within the portal at any time, without needing to revisit the organisation's website.

What it does

- Displays the four cookie categories: Essential (always on, non-togglable), Functional, Analytics, and Marketing, each with a description.
- Allows toggling Functional, Analytics, and Marketing categories individually, with Accept All and Reject All shortcuts.
- Changes synchronise with the consent ledger and propagate to connected systems. Shows the current preference state and when it was last updated.

Contact Us

+1 888 208 5076 / +91 901 926 6824

sales@crossidentity.com

www.crossidentity.com

Release Date - 19/03/2026 Version 1.0