Vishwaas.ai

Implementation Guide

Strategy, Process & Timeline for Going Live with Vishwaas AI

Overview

Vishwaas AI is a self-service platform — the majority of organisations are fully operational within 2–4 weeks without a systems integrator. This guide walks through the recommended implementation strategy: what to do, in what order, who needs to be involved, and what "done" looks like at each stage.

The implementation is structured in **seven phases**. Phases 1–4 cover the compliance core (consent, notices, rights, breach) and are the minimum viable deployment. Phases 5–7 cover the advanced capabilities (identity unification, consent propagation, full operations) and apply to organisations with complex multi-system environments.

Who Needs to Be Involved

Implementation is a cross-functional effort. Assign owners before kick-off:

Role	Responsibility	Time Commitment
DPO / Privacy Officer	Overall project owner; approves purposes, notices, policies	4–6 hrs/week during implementation
IT / Security Admin	Technical setup, source system connectors, webhook configuration	8–12 hrs/week during technical phases
Legal / Compliance	Reviews and approves purpose definitions and notice language	2–4 hrs/week
Marketing	Cookie SDK deployment, consent campaign design	2–4 hrs for cookie setup; 4–6 hrs for campaigns
Source System Owners	Provide API credentials and field mapping for each connected system	1–2 hrs per system
Executive Sponsor	Approves scope and unblocks cross-functional decisions	Kick-off + milestone reviews

Phase 0 — Discovery and Planning

Duration: 3–5 days **Owner**: DPO + IT Admin **No technical work** — this phase is entirely preparation.

0.1 Data and Processing Inventory

Before configuring Vishwaas AI, map what you are actually doing with personal data. Answer:

- **What personal data do we collect?** (email, phone, name, Aadhaar, health data, financial data, behavioural data, device IDs)

- **From whom?** (customers, employees, job applicants, website visitors, app users)
- **For what purposes?** (marketing, service delivery, analytics, credit decisions, HR administration, fraud detection)
- **In which systems?** (CRM, ERP, marketing platform, mobile app, HRIS, support tool)
- **Who do we share it with?** (vendors, analytics platforms, advertising networks, group companies, regulators)
- **Where does it go?** (India only, or cross-border to US/EU-hosted SaaS tools)

This inventory becomes the foundation for your **Purpose Catalogue** and **Vendor Registry** in Vishwaas AI. The more thoroughly it is completed now, the faster configuration proceeds.

0.2 Consent Gap Analysis

Review your existing consent collection mechanisms:

Check	Pass / Fail Criteria
Consent is purpose-specific	Separate consent for each processing purpose — not a single bundled checkbox
Consent is affirmative	No pre-ticked boxes; explicit user action required
Consent is not conditional	Marketing consent not required to receive the service
Consent text is documented	You have a record of what was shown to the user at the time of consent
Withdrawal is easy	User can withdraw any consent without contacting support
Language accessibility	Consent and notices available in the user's language

Purposes where existing consent fails these checks require a **re-consent campaign** after go-live.

0.3 Stakeholder and Approval Workflow Design

Define who approves what inside your organisation:

- Who approves new consent purposes? (typically DPO + Legal)
- Who approves publication of a privacy notice? (typically DPO + Legal)

- Who processes DPR requests? (typically Grievance Officer / DPO)
- Who approves DPIA completion? (typically DPO)
- Who owns breach incident management? (typically DPO + CISO)

Map these to the Vishwaas AI role model (11 pre-built roles including `dpo`, `privacy_manager`, `legal_officer`, `grievance_officer`, `it_admin`).

0.4 Deliverables Before Phase 1

- [ ] Personal data inventory spreadsheet (system, data categories, purpose, sharing)
- [ ] List of all processing purposes (draft names and descriptions)
- [ ] List of all vendors / data processors
- [ ] Consent gap analysis — which purposes need re-consent campaigns
- [ ] Org chart mapped to Vishwaas AI roles
- [ ] Source systems list with IT owners identified

Phase 1 — Foundation Setup

Duration: 2–3 days **Owner**: IT Admin + DPO **Prerequisite**: Phase 0 deliverables complete

1.1 Tenant Provisioning

Your Vishwaas AI tenant is provisioned by the IdentityPlus onboarding team within 24 hours of contract execution. You receive:

- Tenant slug (e.g. `acme-corp`) — your login URL: `https://app.vishwaasai.in/acme-corp/login`
- Super admin credentials for initial setup
- Environment details (API base URL, Swagger docs, MailHog/email capture if QA)

1.2 User Accounts and Role Assignment

Create user accounts for all team members identified in Phase 0:

1. Navigate to **Admin → Users → New User**
2. Enter email address and assign role
3. User receives OTP login email (no password — passwordless by design)

4. Verify access by role: DPO sees full compliance dashboard; IT Admin sees settings and integrations; Grievance Officer sees DPR queue only

Role reference:

Vishwaas AI Role	Assign To
tenant_manager	Project owner / senior admin
dpo	Data Protection Officer
privacy_manager	Privacy / compliance team
legal_officer	Legal / compliance counsel
it_admin	IT / Security team
grievance_officer	DPR / customer rights team
training_admin	L&D / HR team
auditor	Internal / external auditors (read-only)

1.3 Tenant Configuration

In **Admin → Settings**:

- **Organisation profile**: legal name, registered address, DPBI registration ID (if obtained), DPO contact details
- **Language defaults**: set the default language and supported languages for your consumer-facing portal
- **Email / SMTP**: configure outgoing email for OTP, DPR notifications, and breach alerts (production: AWS SES; dev/QA: MailHog)
- **Auth policy**: OTP expiry (default: 10 minutes), rate limits (default: 3 OTP requests per 5 minutes)

1.4 Phase 1 Completion Checklist

- [ ] All team users created and can log in
- [ ] Roles verified — each user sees only what their role permits
- [ ] Tenant profile complete
- [ ] SMTP configured and test email delivered successfully
- [ ] Admin dashboard accessible

Phase 2 — Consent and Notice Configuration

Duration: 3–5 days **Owner**: DPO + Legal + Privacy Manager **Prerequisite**: Purpose list from Phase 0

This is the highest-value phase — it directly produces the DPDP Act compliance artefacts.

2.1 Build the Purpose Catalogue

Navigate to **Admin → Consents → Purposes → New Purpose** for each processing purpose identified in Phase 0:

Field	Guidance
Purpose Code	Short machine-readable identifier (e.g. mkt_email, analytics, credit_bureau)
Purpose Name	Multilingual: enter in English + all languages you support
Category	Select: Service Delivery / Marketing / Analytics / Legal Obligation / Research / Other
Lawful Basis	Consent / Legitimate Use / Legal Obligation / Contractual Necessity
Data Categories	Tag which personal data categories this purpose uses
Requires Explicit Opt-In	Enable for all marketing, analytics, and third-party sharing purposes
Retention Period	How many days data is retained after consent withdrawal or account closure

Requires Legal review: Purpose names and descriptions will appear in your Privacy Notice and in the consumer portal. Legal should approve the language before publishing.

2.2 Author and Publish the Privacy Notice

Navigate to **Admin → Notices → New Notice**:

1. Author notice content in the TipTap rich text editor — or paste from an existing draft
2. Add language versions (one tab per language)
3. Link relevant consent purposes to the notice
4. Submit for DPO approval → DPO reviews and approves in the approval workflow
5. Publish — the notice is assigned a version number and a content hash; it is now available at a public URL for embedding in your website, app, and consent flows

The published notice URL is static and versioned — you can safely link to it from your cookie banner, registration form, and mobile app.

2.3 Configure the Cookie Consent Banner

Navigate to **Admin → Settings → Cookies**:

1. Define cookie categories (Strictly Necessary, Analytics, Marketing, Personalisation, Affiliate — or custom)
2. Assign third-party trackers to categories
3. Configure banner appearance (position, colour scheme, button labels)
4. Set language: auto-detect from browser, or fixed language
5. Copy the <script> tag → deploy to your website's <head> (one line of HTML)

After deployment, all non-essential trackers are blocked until the visitor explicitly consents to their category.

2.4 Phase 2 Completion Checklist

- [ ] All processing purposes configured and approved
- [ ] Purpose names and descriptions reviewed by Legal
- [ ] Privacy notice authored, approved by DPO, and published
- [ ] Notice URL embedded in website footer and registration form
- [ ] Cookie SDK deployed and tested — verify trackers are blocked on page load
- [ ] Cookie banner tested in 3+ languages
- [ ] First live consent record visible in **Admin → Consents**

Phase 3 — Consumer Portal and Consent Collection

Duration: 2–4 days **Owner**: IT Admin + Marketing + DPO **Prerequisite**: Phases 1–2 complete

3.1 Configure the Consumer Portal

The data principal portal is live at https://app.vishwaasai.in/{your-slug}/portal as soon as your tenant is provisioned. Configure it in **Admin → Settings**:

- Portal display name and logo
- Supported languages (defaults to all configured languages)
- Default language per region (can be auto-detected from browser locale)
- Contact details shown to data principals (DPO email, grievance officer contact)

3.2 Integrate Consent Collection into Your Flows

Option A — Embedded Consent Form (Cookie SDK) For website and web app flows: the Cookie SDK handles consent collection inline. No additional integration required beyond Phase 2 deployment.

Option B — Redirect to Portal Link your registration or login flow to the portal's consent section:

https://app.vishwaasai.in/{slug}/portal/consents

The portal handles authentication (OTP), consent display, and records the result.

Option C — API Integration For mobile apps or custom flows, call the Consent API directly:

```
POST /api/v1/consent/collect
{
 "data_principal_id": "...",
 "purpose_code": "mkt_email",
 "action": "granted",
 "channel": "mobile_app",
 "ip_address": "...",
 "consent_text_snapshot": "..."  // the exact text shown to the user
}
```

This creates a hash-chained, signed consent record immediately.

3.3 Re-Consent Campaign for Existing Customers

For customers whose existing consent does not meet DPDP Act standards (identified in Phase 0 gap analysis):

1. Navigate to **Admin → Campaigns → New Campaign**
2. Target: select purposes needing re-consent
3. Audience: upload CSV of affected customer IDs / emails, or select by existing consent status
4. Message: configure the consent request email/SMS in all supported languages
5. Schedule: set launch date and follow-up reminder timing
6. Launch → campaign sends consent requests; responses are recorded in real time

3.4 Phase 3 Completion Checklist

- [ ] Consumer portal accessible and tested across supported languages
- [ ] At least one consent collection path integrated (SDK / portal redirect / API)
- [ ] Test consumer can log in to portal, see their purposes, and toggle consent
- [ ] Re-consent campaign configured for all legacy consent gaps
- [ ] First re-consent campaign sent; response rate visible in campaign dashboard

Phase 4 — Rights, Breach, and Compliance Modules

Duration: 3–5 days **Owner**: DPO + Grievance Officer + Privacy Manager **Prerequisite**: Phase 3 complete

4.1 DPR (Data Principal Rights) Module

Configure the rights request workflow:

1. **Request types**: enable the request types applicable to your organisation (Access, Correction, Erasure, Nomination, Grievance)

2. **SLA configuration**: the DPDP Act mandates 30 days for most requests and 48 hours for pre-erasure notification; defaults are pre-set
3. **Assignment rules**: configure which team members receive new DPR requests by type
4. **Identity verification**: configure the verification method for DPR requests (email OTP by default; stronger options available)
5. **DPBI escalation**: configure DPBI contact details for escalation of unresolved grievances

Test the end-to-end flow: submit a test DPR request via the consumer portal → verify it appears in **Admin → Rights** → process it through to completion → confirm the notification email is received.

4.2 Breach Management Module

Configure the incident response workflow:

1. **DPBI details**: enter the DPBI notification email/portal URL (for post-constitution notification)
2. **Notification templates**: review and customise the 72-hour DPBI notification template and the data principal notification template
3. **Severity levels**: configure which severity levels trigger automatic escalation to the DPO
4. **Response team**: assign breach response roles (incident owner, DPO approver, legal reviewer)

Tabletop test: log a test breach incident → verify the 72-hour countdown starts → walk through the notification steps → confirm audit trail is complete.

4.3 Vendor Management Module

Register all third-party data processors identified in Phase 0:

1. **Admin → Vendors → New Vendor** for each processor
2. Enter: vendor name, category (marketing / analytics / logistics / cloud / other), data categories shared, DPA status, cross-border transfer flag
3. Upload signed DPA document where available

4. Set vendor risk tier and review schedule

4.4 Phase 4 Completion Checklist

- [ ] DPR request types enabled and SLAs configured
- [ ] Assignment rules set — new requests route to correct team members
- [ ] End-to-end DPR test completed (submit → process → notify)
- [ ] Breach module configured — 72-hour countdown tested
- [ ] All vendors registered with DPA status recorded
- [ ] Compliance dashboard shows accurate posture across all active modules

Phase 5 — Identity Unification (Multi-System Environments)

Duration: 1–2 weeks (depends on number of source systems) **Owner**: IT Admin + Source System Owners **Prerequisite**: Phase 4 complete **Applies to**: organisations with personal data in 2+ disconnected systems

5.1 Connect Source Systems

For each source system in the inventory:

1. Navigate to **Admin → Settings → Source Systems → New Source System**
2. Complete the 5-step connector wizard:
    - **Basic info**: system name, type (CRM / e-commerce / HRIS / support / marketing / other)
    - **Connection**: integration method, base URL, authentication credentials
    - **Test connection**: verify connectivity; review sample field list
    - **Field mapping**: map source fields to Vishwaas AI canonical fields (email, phone, name, PAN, Aadhaar, DOB, city)
    - **Sync settings**: schedule (real-time / hourly / daily / manual)
3. Run initial discovery sync — all records are ingested into the staging area

Estimated time per system: 30–90 minutes depending on API complexity.

5.2 Run Identity Resolution

After all source systems are synced:

1. Navigate to **Admin → Unification → Dashboard → Run Resolution Now**
2. The engine processes all staged records:
    - Exact email / phone / PAN / Aadhaar matches → auto-linked
    - Probabilistic matches (name + DOB + city ≥ 85%) → queued for review
3. Monitor progress in the Resolution Dashboard

5.3 Process the Review Queue

Navigate to **Admin → Unification → Review Queue**:

- Review each candidate pair side-by-side
- **Approve** to link the staged record to the existing canonical profile
- **Reject** to keep them as separate individuals
- **Defer** to hold for later (e.g. awaiting additional data from the source system)

Typical queue size: 5–15% of total records, depending on data quality across source systems.

5.4 Phase 5 Completion Checklist

- [ ] All source systems connected and initial sync completed
- [ ] Identity resolution run completed — auto-link rate visible in dashboard
- [ ] Review queue processed to < 50 pending items
- [ ] Spot-check: unified profiles for 5–10 known customers look correct
- [ ] Data asset map populated — each canonical profile shows which systems hold their data

Phase 6 — Consent Propagation

Duration: 3–7 days **Owner**: IT Admin + downstream system owners **Prerequisite**: Phase 5 complete (or Phase 4 if identity unification is out of scope)

6.1 Register Downstream Applications

For each downstream system that needs to receive consent signals:

1. Navigate to **Admin → Settings → Propagation → Register New Webhook**
2. Select the downstream application
3. Enter the webhook endpoint URL (the receiving system must expose an HTTPS endpoint)
4. Select event types: consent.granted, consent.withdrawn, consent.expired, consent.renewed
5. Save → copy the **webhook secret** (shown once; store in the downstream system's secrets manager)

Test the connection: use the **[Test]** button to send a test event → verify the downstream system received it and responded with 200 OK.

6.2 Configure Connector Actions

For each downstream application, configure what action it should take per consent event:

- Salesforce: mkt_email withdrawn → set Contact.DoNotEmail = true
- CleverTap: mkt_email withdrawn → remove from all campaign segments
- SendGrid: mkt_email withdrawn → move to suppression list

This configuration lives in **Settings → Propagation → [Application] → Edit Actions**.

6.3 Implement Webhook Receiver (Downstream Systems)

Each downstream system needs a webhook endpoint that:

1. Receives the POST from Vishwaas AI
2. Verifies the X-VishwaasAI-Signature header (HMAC-SHA256)
3. Reads the event_type, purpose_code, and data_principal.external_ids
4. Executes the appropriate action (suppress, remove from segment, update flag)
5. Returns 200 OK

Sample verification (Node.js):

```
const crypto = require('crypto');

function verifySignature(rawBody, secret, signatureHeader) {
 const expected = 'sha256=' + crypto
  .createHmac('sha256', secret)
  .update(rawBody)
  .digest('hex');
 return crypto.timingSafeEqual(
  Buffer.from(expected),
  Buffer.from(signatureHeader)
 );
}
```

6.4 Configure the Consent Status Pull API

For systems that poll consent rather than receive webhooks:

1. Navigate to **Admin → Settings → API Keys → New API Key**
2. Name the key (e.g. salesforce-consent-check), scope: consent:read
3. Copy the key → configure in the downstream system

Downstream system calls:

```
GET /api/v1/consent/status/{dpId}/{purposeCode}
Authorization: Bearer <api_key>
```

6.5 Phase 6 Completion Checklist

- [ ] All downstream systems registered with webhook endpoints
- [ ] Test event delivered and confirmed for each system
- [ ] Signature verification implemented on all receiving systems
- [ ] Connector actions configured per application per purpose
- [ ] End-to-end test: withdraw consent in the portal → confirm all downstream systems updated within 5 seconds
- [ ] Propagation monitor showing > 99% delivery rate in first 24 hours

Phase 7 — Full Operations and Handover

Duration: 3–5 days **Owner**: DPO + all module owners

7.1 Staff Training

Vishwaas AI includes a built-in training module (**Admin → Training**) with DPDP Act courses. Beyond platform training, ensure:

Audience	Training Required
DPO / Privacy Manager	Full platform walkthrough; DPBI response procedures; chain verification
Grievance Officer	DPR request processing workflow; escalation paths
IT Admin	Connector management; webhook monitoring; incident response
Marketing	Consent campaign management; what not to send to non-consenting users
All staff with data access	DPDP Act awareness; data principal rights overview

7.2 Establish Operational Rhythms

Cadence	Activity	Owner
Daily	Review DPR request queue; check propagation monitor for dead-letter items	Grievance Officer / IT Admin
Weekly	Review consent dashboard — withdrawal trends, campaign response rates	Privacy Manager
Monthly	Vendor DPA review; DPIA risk register review; consent expiry schedule	DPO

Cadence	Activity	Owner
Quarterly	Full audit chain verification (Admin → Audit → Verify Chain)	DPO / Auditor
On incident	Breach intake → 72-hour DPBI clock started immediately	DPO + CISO
On DPBI inquiry	Export DPBI Evidence Package from relevant module	DPO

7.3 Go-Live Announcement

Before announcing DPDP compliance to customers and regulators:

- [ ] Consumer portal link published on website (footer, privacy policy page)
- [ ] DPR request submission path communicated in Privacy Notice
- [ ] Grievance Officer contact details published (required by DPDP Act §13)
- [ ] DPBI registration (if your organisation qualifies as a Significant Data Fiduciary)
- [ ] Internal communication to all staff: new data handling obligations are in effect

7.4 Phase 7 Completion Checklist

- [ ] All staff trained on their role-specific responsibilities
- [ ] Operational runbook documented (who does what, when)
- [ ] Go-live communication sent internally and externally
- [ ] Compliance dashboard showing green across all active modules
- [ ] First audit chain verification completed and result recorded

Timeline Summary

Starter / SMB (1–2 source systems, < 500K data principals)

Week	Phases
Week 1	Phase 0 (Discovery) + Phase 1 (Foundation) + Phase 2 (Consent & Notices)
Week 2	Phase 3 (Consumer Portal) + Phase 4 (Rights & Breach)
Week 3	Phase 7 (Operations & Handover) — unification and propagation optional
Go-live: ~3 weeks	

Professional / Mid-Market (3–6 source systems, 500K–5M data principals)

Week	Phases
Week 1	Phase 0 (Discovery) + Phase 1 (Foundation)
Week 2	Phase 2 (Consent & Notices) + Phase 3 (Consumer Portal)
Week 3	Phase 4 (Rights & Breach + Vendor)
Weeks 4–5	Phase 5 (Identity Unification — connect systems + resolve)
Week 6	Phase 6 (Consent Propagation) + Phase 7 (Operations)
Go-live: ~6 weeks	

Enterprise (7+ source systems, 5M+ data principals, multiple business units)

Weeks	Phases
Weeks 1–2	Phase 0 (Discovery — extended; multiple BU workshops) + Phase 1
Weeks 3–4	Phase 2 (Consent & Notices — multiple product lines / brands)
Weeks 4–5	Phase 3 (Consumer Portal — multiple portals by brand / region) + Phase 4
Weeks 5–8	Phase 5 (Identity Unification — 7+ connectors, extended review queue)
Weeks 8–10	Phase 6 (Consent Propagation — multiple downstream systems)
Weeks 10–12	Phase 7 (Training at scale, operational handover, BU rollout)
Go-live: ~12 weeks	

Common Implementation Pitfalls

Pitfall	Prevention
Starting without a complete purpose inventory	Phase 0 is non-negotiable — incomplete purpose lists require rework in every later phase
Deploying consent collection before notice is published	The DPDP Act requires notice *before* consent is sought — publish the notice first
Configuring all purposes as "requires_explicit_opt_in"	Service delivery and contractual purposes may use legitimate use — over-requiring consent adds friction without legal necessity
Skipping the re-consent campaign	Legacy consents that fail DPDP Act standards remain a liability until re-consent is obtained
Webhook receiver not verifying the HMAC signature	An unverified webhook receiver can be spoofed — signature check is mandatory, not optional
Going live without training the Grievance Officer	The first DPR request may arrive within hours of go-live — someone must be ready to process it
Treating implementation as a one-time project	DPDP compliance is an ongoing operational function; new purposes, new vendors, new systems all require updates