Vishwaas.ai

Product FAQs

Questions Customers Ask — and the Answers

Section 1 — About the DPDP Act

Q: The DPDP Act has been passed but the Rules are not yet fully notified. Do we need to start now?

The DPDP Act 2023 is in force. The DPDP Rules 2025 have been published. The Data Protection Board of India (DPBI) is being constituted. Enforcement timelines have not been announced, but the legal obligations exist today — and the DPBI can investigate complaints from the date it is operational. Organisations that wait until enforcement begins to build their consent infrastructure will be starting from zero under pressure. Those who deploy now will have 7-year consent records, trained staff, and operational workflows in place before the first DPBI notices go out.

Q: We already have consent checkboxes on our website. Aren't we compliant?

Almost certainly not under DPDP Act standards. Common gaps in existing implementations:

- A single "I agree to Terms & Conditions" checkbox that bundles service consent with marketing consent — the DPDP Act requires consent to be specific to each purpose
- Pre-ticked checkboxes — the Act requires affirmative action; silence or pre-selection does not constitute consent
- No record of what text the user was shown at the time of consent — without a consent text snapshot, you cannot prove what was agreed
- No timestamp from a trusted authority — a database timestamp can be altered; the DPDP Act's burden-of-proof requirement needs something stronger
- No easy withdrawal mechanism — the Act requires withdrawal to be as easy as giving consent

Vishwaas AI addresses all five gaps out of the box.

Q: We process employee data, not customer data. Does the DPDP Act apply to us?

Yes. The DPDP Act applies to the processing of any digital personal data of Indian citizens — including employees, contractors, job applicants, and vendors. HR data (salary, PAN, Aadhaar, performance records, health insurance) is personal data under the Act. Employee consent, access rights, and data principal rights apply in full.

Q: What is the penalty for non-compliance?

Schedule 1 of the DPDP Act specifies penalties up to ₹250 crore per instance for processing personal data without valid consent, and up to ₹200 crore for failure to notify the DPBI of a data breach within 72 hours. Penalties are assessed per violation — a company with millions of customers processed without valid consent faces cumulative exposure that can exceed these per-instance caps.

Section 2 — About Vishwaas AI

Q: What exactly does Vishwaas AI do?

Vishwaas AI is a multi-tenant SaaS platform that helps organisations comply with India's DPDP Act 2023. It covers five operational areas:

- **Consent management**
  Collect, record, and manage purpose-specific consent; serve a multilingual consumer portal for viewing and withdrawing consent
- **Rights management**
  Receive and process Data Principal Rights (DPR) requests: access, correction, erasure, nomination, grievance
- **Compliance operations**
  Manage Privacy Notices, Data Protection Impact Assessments (DPIAs), vendor contracts, breach incidents, and training
- **Identity unification**
  Resolve fragmented customer identities across CRM, e-commerce, HRIS, and other systems into a single canonical profile
- **Consent propagation**
  Push every consent decision to every downstream system within 5 seconds; provide a real-time consent status API for point-of-use checks

Q: How is Vishwaas AI different from a privacy policy generator or a consent banner tool?

- Consent records are cryptographically signed — each record carries a SHA-256 hash, an RSA-2048 digital signature, and an RFC 3161 Timestamp Authority token
- Records are tamper-proof at the database level — UPDATE and DELETE are revoked at the PostgreSQL role level; not even a system administrator can alter a consent record after it is written
- Consent decisions are propagated in real time to every downstream system via signed webhooks — not just recorded and forgotten
- Identity unification links consent to the correct individual across all your source systems — so a DPR erasure request reaches every system that holds that person's data

No consent banner or privacy policy tool provides any of these capabilities.

Q: We already use OneTrust. Why should we consider switching?

OneTrust was built for GDPR at a time when the DPDP Act did not exist. Key gaps for Indian organisations:

Dimension	OneTrust	Vishwaas AI
Design basis	GDPR-first; DPDP added as a module	DPDP Act 2023 — built ground-up
Cryptographic non-repudiation	Database logs only	SHA-256 chain + RSA + RFC 3161 TSA
Indian languages	Limited	22 Eighth Schedule languages + English
Consent propagation SLA	No defined SLA	< 5 seconds, dead-letter queue
Identity unification	Not available	Deterministic + probabilistic matching
India data residency	Optional / premium	Default — AWS Mumbai (ap-south-1)
Pricing for Indian market	₹25–50L+ USD-denominated	Starter tier in INR, SMB-accessible
Time to deploy	3–6 months, SI-led	Days to weeks, self-service

Section 3 — Technical and Security

Q: Where is our data stored? Does it leave India?

All data processed through Vishwaas AI is stored exclusively in AWS Mumbai (ap-south-1). There is no cross-region replication of personal data. This satisfies the DPDP Act's data localisation expectations and RBI's directive on storage of payment system data.

Q: How secure is the platform? Can your team access our customer data?

Access controls are designed to prevent it:

- All PII (email, phone, name, Aadhaar) is stored **encrypted** (AES-256-GCM). The encryption key is held in AWS Secrets Manager or AWS KMS — not accessible to application support staff
- Aadhaar is **never stored in plaintext** — only as a SHA-256 hash, including in staging records
- The consent ledger is **append-only at the database level** — UPDATE and DELETE are revoked at the PostgreSQL role level; no support engineer, DBA, or administrator can alter a consent record
- Every action taken by any user — including IdentityPlus staff in support contexts — creates an immutable entry in the hash-chained audit log
- Tenant data is isolated via PostgreSQL Row-Level Security — a query executed in one tenant's context cannot return another tenant's data, even if the application layer is bypassed

Q: How does the cryptographic proof actually work? Can we verify it independently?

Yes — and this independence is the point. Each consent record carries:

- **record_hash —** SHA-256 of the deterministic JSON of the record content. If any field is changed after creation, the hash no longer matches.
- **chain_hash —** SHA-256 of record_hash + previous_chain_hash. Changing any record in the sequence breaks every subsequent chain hash.
- **digital_signature —** RSA-2048 signature over the record hash using your tenant's private key (held in AWS KMS). Proves the record was created by your authorised system.

- **tsa_token** — RFC 3161 Timestamp Authority token issued by DigiCert or GlobalSign. This token is verifiable by any party — including the DPBI, a court, or your auditor — using only the TSA's public certificate. It does not require Vishwaas AI to be online or to cooperate.

The TSA token is the critical element for legal defensibility: it is a signed attestation from a globally trusted third party that a specific data structure existed at a specific moment in time.

Q: What happens if Vishwaas AI goes offline? Can we still access our consent records?

Consent records can be exported at any time as a signed PDF or structured JSON with the full cryptographic chain intact. The RFC 3161 TSA tokens embedded in each record are verifiable independently — offline, without any Vishwaas AI infrastructure. For enterprise customers, scheduled automated exports to customer-controlled AWS S3 buckets are available, ensuring a continuously updated offline copy of the consent ledger.

Q: We have data in on-premise systems. Can Vishwaas AI connect to them?

Yes, via the **Self-Hosted Agent** deployment model. A lightweight connector agent is deployed inside your private network or VPC. It pulls data from on-premise core banking systems, mainframes, or air-gapped systems using your existing network policies, and syncs to Vishwaas AI over an outbound-only encrypted channel. No inbound firewall rules are required.

Section 4 — Implementation and Operations

Q: How long does deployment take?

For a standard SaaS deployment:

Milestone	Typical Timeline
Account provisioning and environment setup	Day 1
Cookie SDK deployed on website	Day 1–2
First consent purposes configured	Day 2–3
Privacy notice authored and published	Day 3–5
First source system connector live	Day 3–7
Consumer portal accessible to data principals	Day 5–7
First DPR request workflow operational	Day 7–10
Full stack (all modules) operational	2–4 weeks

Enterprise deployments with multiple source systems, custom field mappings, and change management typically take 4–8 weeks.

Q: Do we need technical staff to operate Vishwaas AI?

No. Day-to-day compliance operations — managing consent purposes, publishing notices, processing DPR requests, reviewing identity matches, monitoring propagation — are handled through the admin console without any technical involvement. A DPO or Privacy Manager can operate the platform independently.

Technical involvement is needed only for: initial source system connector setup (one-time), Cookie SDK deployment (one script tag), and webhook endpoint configuration on downstream systems (one-time per system).

Q: We have existing customer consent data in our CRM. Can we migrate it?

Yes, via CSV import. Your historical consent records can be uploaded with the existing consent date, purpose, and channel. These are imported into the Vishwaas AI consent ledger with a channel: import flag and a note that the record represents a migrated legacy consent. Forward-going consent events from the import date onward carry the full cryptographic chain. We recommend a consent re-collection campaign for customers where the original consent evidence is insufficient for DPDP Act standards.

Q: How does the multilingual support work? Do we need to translate our privacy notices?

The platform provides the infrastructure; your team provides the content. The notice authoring tool (TipTap rich text editor) lets you author notice content in multiple languages simultaneously, with a side-by-side view. For consent text, you author the text in each language and the platform serves the correct language based on the data principal's stated preference.

For organisations that need translation assistance, we partner with certified legal translation services who are familiar with DPDP Act terminology. Ask your account team for details.

Section 5 — Specific Feature Questions

Q: What is the "dead-letter queue" in consent propagation?

When Vishwaas AI dispatches a consent change webhook to a downstream system and that system is unavailable, the platform retries automatically (immediately, then +1s, +5s, +30s). If all three retries fail, the delivery attempt is moved to the **dead-letter queue** — a visible, auditable list of failed deliveries.

The dead-letter queue shows the full webhook payload, the HTTP error received at each attempt, and the timestamp. Operations staff can manually Retry (re-attempts delivery) or Dismiss (acknowledges the failure with an audit log entry, typically used when the downstream system has been decommissioned). Nothing is silently lost.

Q: A data principal has submitted an erasure request. What exactly happens?

- The DPR request is received and logged with a unique reference number (e.g. DPR-2026-00042) and a 30-day SLA deadline
- Identity verification is performed (OTP to registered email/phone, or stronger method if configured)
- The Vishwaas AI identity graph is queried — every source system holding this individual's data is listed
- The DPO or Grievance Officer reviews the request; for each data category, the system flags whether a statutory retention obligation applies
- For data not under retention hold, erasure jobs are dispatched to each linked source system
- Completion is tracked per system; the data principal is notified when erasure is confirmed across all systems
- If any system fails to confirm erasure, it is escalated for manual follow-up
- A complete audit trail of every step is retained in the append-only audit ledger

Q: Can a data principal see their own consent records?

Yes. The **Data Principal Portal** (accessible at /{your-organisation}/portal) gives every data principal a self-service view of: - All purposes for which consent has been collected, with the exact text they agreed to - The date and channel of each consent grant or withdrawal - Active consent toggles — they can withdraw any consent with a single click - All DPR requests they have submitted and their current status - Privacy notices delivered to them

The portal is available in all 22 Indian Eighth Schedule languages plus English, served based on the user's stated language preference.

Q: How does Vishwaas AI handle minors?

The platform supports the DPDP Act Section 9 requirements for child data:

- A is_minor flag on the Data Principal record triggers the guardian consent workflow
- Guardian consent is linked to the minor's profile with a separate consent record
- Purposes categorised as behavioural_tracking or targeted_advertising are blocked from minor profiles at the data model level — they cannot be activated regardless of banner interaction
- DigiLocker and Aadhaar OTP eKYC for verifiable guardian consent are on the near-term roadmap (see Product Roadmap, document 1.13)

Contact us

+1 888 208 5076
+91 901 926 6824

sales@crossidentity.com

www.crossidentity.com