ENTERPRISE TECHNICAL SPECIFICATION | DPDP ACT 2023 VERIFIED | ISO 27001 / SOC 2 ALIGNED

Enterprise Security, Data Provenance & Statutory DPDP Compliance Specification

Architectural Standard for Cryptographic Referral Provenance, Data Fiduciary Shielding, and Enterprise HR Boundary Segregation

Document ID: VCR-SEC-SPEC-2026-V2 **Classification:** Confidential / Enterprise Review **Target Audience:** CISO, Legal Counsel, DPO, TA Leads

1. EXECUTIVE SUMMARY & STATUTORY GOVERNANCE

VOUCHIR operates as an institution-grade referral provenance mesh engineered to automate talent sourcing, structure 50/50 Co-Vouch financial incentives, and enforce cryptographic attribution across distributed enterprise talent networks. In modern high-compliance talent acquisition environments, processing candidate Personally Identifiable Information (PII) presents heightened statutory exposures under India's **Digital Personal Data Protection (DPDP) Act 2023**.

The Statutory Liability Shield: Traditional employee referral workflows (such as employees forwarding unsolicited candidate CVs or sharing unconsented phone numbers) expose enterprises to non-compliance liabilities under DPDP Act Section 33 reaching up to **₹250 Crore per violation**. VOUCHIR operates strictly as an automated, consent-gated Data Processor, capturing verifiable digital consent receipts prior to data ingestion and insulating the enterprise (Data Fiduciary) from statutory exposure.

2. STATUTORY DPDP ACT 2023 ALIGNMENT & PENALTY MITIGATION

Under Section 7(i) of the DPDP Act 2023, data processing must rest upon explicit, verifiable consent for clearly specified legitimate purposes. VOUCHIR operationalizes this statutory requirement through deterministic technical safeguards that directly address each critical provision of the Act:

DPDP ACT SECTION	STATUTORY PENALTY EXPOSURE	VOUCHIR ARCHITECTURAL IMPLEMENTATION	ENTERPRISE INSULATION LEVEL
Section 6(1) Notice & Valid Consent	Up to ₹50 Crore	Pre-ingress candidate consent gate with granular scope itemization and immutable digital consent receipts.	**Complete Statutory Shield**
Section 8(5) Security Safeguards	Up to ₹250 Crore	Field-level AES-256-GCM encryption at rest, TLS 1.3 in transit, and row-level tenant schema isolation.	**Maximum Risk Reduction**
Section 8(7) Retention Limits	Up to ₹50 Crore	Automated 180-day Time-To-Live (TTL) candidate lifecycle with cryptographic purge verification.	**Zero Residual Liability**
Section 9 Obligations on Children	Up to ₹200 Crore	Automated age-verification and mandatory employment eligibility gating at candidate ingress.	**Complete Protection**
Section 11–13 Data Principal Rights	Up to ₹50 Crore	Self-service Data Subject Rights (DSR) portal for immediate access, correction, and programmatic erasure.	**Automated Compliance**

3. ZERO-TRUST CANDIDATE INGRESS & CONSENT LIFECYCLE

VOUCHIR prevents unverified or third-party PII ingestion through an asymmetric 4-stage cryptographic consent protocol. At no point can an employee advocate directly upload a candidate resume into the platform without candidate authorization.

STAGE 01
Tokenized Referral
Advocate generates an encrypted, single-use invite token via Slack or MS Teams. Zero candidate PII collected.

STAGE 02
Candidate Gate
Candidate opens secure link, reviews statutory purpose notice, and grants explicit digital consent.

STAGE 03
Consent Receipt
An immutable JSON-LD consent record is cryptographically signed and anchored to the ledger prior to ATS ingest.

STAGE 04
Automated TTL
If candidate is unhired at day 180, automated cascade deletion scrubs all PII across databases and caches.

```
// Cryptographic Consent Receipt Formulation: Consent_Receipt_Hash = SHA-256( Candidate_ID_Hash + Fiduciary_ID + Scope_Bitmask + UTC_Timestamp + Platform_Signature )
```

4. DATA SEGREGATION & CANDIDATE PRIVACY BOUNDARY

Collaborative referral platforms introduce significant risk of confidentiality leaks regarding candidate performance, interview notes, and compensation discussions. VOUCHIR enforces a rigid technical boundary between enterprise recruiters and employee advocates:

> **The Candidate Privacy Guarantee:** Internal recruiter evaluations, hiring manager scorecards, interview rubrics, compensation bands, and salary negotiation logs are **permanently redacted** from employee advocates. Advocates receive exclusively high-level enum state updates (e.g., *Application Received*, *Interviewing*, *Milestone 1 Reached*).

DATA VECTOR / ATTRIBUTE	PERMITTED VISIBILITY SCOPE	TECHNICAL ISOLATION MECHANISM
Job Requisitions	All authenticated employees	Read-only cached tenant catalog via Redis cluster.
Referral Stage Enum	Advocate & Candidate (Co-Vouch View)	Sanitized high-level status only; rubrics and reviewer notes stripped.
HR Evaluation Scorecards	Hiring Managers & TA Leads only	Quarantined in enterprise ATS; never synced to VOUCHIR datastores.
Compensation & CTC Bands	HR Admins & Payroll Approvers	Restricted by Row-Level Security (RLS) and scoped RBAC policies.
Cryptographic Provenance	Compliance Officers & System Auditors	Append-only SHA-256 ledger transactions with HMAC tamper evidence.

5. CRYPTOGRAPHIC ATTRIBUTION LEDGER & 50/50 SETTLEMENT

VOUCHIR replaces fragile browser cookies with an immutable SHA-256 block hash-chained ledger. Every lifecycle transition generates an auditable record linked to the previous block digest:

```
Block_N = SHA-256( Block_N-1.Hash || Tenant_UUID || Advocate_ID || Candidate_Email_Hash || Stage_Enum || UTC_Microtime )
```

Referral Collision & Double-Brokerage Elimination: Multi-advocate attribution disputes are eliminated at the PostgreSQL schema layer via composite uniqueness constraints on `(tenant_id, candidate_email_hash, job_requisition_id)`. The first verified cryptographic registration locks attribution, rejecting duplicate submissions with millisecond-level audit proof.

MILESTONE EVENT	TRIGGER CONDITION	FINANCIAL SETTLEMENT LOGIC
Milestone 1: Offer Joining	Candidate onboarded (Verified ATS status: *Joined*).	50% reward balance unlocked for advocate and candidate celebration.
Milestone 2: 90-Day Retention	Candidate clears 90 calendar days of active employment.	Remaining 50% reward disbursed automatically via UPI / Voucher API.
Early Departure Exception	Candidate leaves prior to day 90.	Milestone 2 balance voided, protecting enterprise talent budget.

6. INFRASTRUCTURE SECURITY CONTROLS & 99.9% AVAILABILITY SLA

CONTROL DOMAIN	IMPLEMENTED SECURITY ARCHITECTURE	ASSURANCE VERIFICATION
Data Encryption	AES-256-GCM for sensitive fields at rest; TLS 1.3 in transit with HSTS Preload.	KMS envelope encryption with 90-day automated key rotation.
Identity & Provisioning	SAML 2.0 / OIDC SSO with Okta, Azure AD, and Google Workspace; SCIM provisioning.	MFA enforced across all recruiter and administrative sessions.
Webhook Ingestion	Greenhouse, Lever, and Workday webhooks authenticated via HMAC-SHA256 signatures.	Fast-ack queueing (<150ms) with replay protection (300s window).
Contractual SLA	Contractually backed 99.9% System Availability SLA with multi-AZ failover.	Tiered service credits backed by real-time status telemetry.
Subprocessor Governance	Infrastructure localized to AWS Mumbai (ap-south-1) and GCP Delhi.	SOC 2 Type II, ISO 27001, and PCI-DSS certified cloud partners.

7. INFRASTRUCTURE SUBPROCESSOR REGISTER & CLOUD DEPLOYMENT OPTIONS

SUBPROCESSOR ENTITY	SERVICE SCOPE	PRIMARY HOSTING REGION	COMPLIANCE STANDARD
Amazon Web Services (AWS)	Cloud Compute, Managed DB & Cloud HSM	Asia-Pacific (Mumbai, India)	SOC 1/2/3, ISO 27001, PCI-DSS
Google Cloud Platform (GCP)	Secondary Analytics & Warm Disaster Recovery	Asia-South1 (Delhi, India)	SOC 1/2/3, ISO 27001
Cloudflare, Inc.	Edge WAF, DDoS Mitigation & DNSSEC	Global Edge Network (Anycast)	SOC 2 Type II, ISO 27001
Cashfree Payments / RazorpayX	Automated Voucher & UPI Reward Disbursement	India (Local Banking Rails)	RBI Authorized, PCI-DSS Level 1

Deployment Topologies: Enterprise clients can select between *Multi-Tenant Logical Isolation* (isolated by PostgreSQL Row-Level Security with tenant KMS keys) or a *Dedicated Enterprise VPC Connector* (isolated cloud infrastructure with Customer-Managed Keys and VPN interconnects).

8. DOCUMENT CONTROL, REVISION HISTORY & EXECUTIVE SIGN-OFF

REVIEWING AUTHORITY	DESIGNATION / ORGANIZATION	REVIEW STATUS	VERIFICATION DATE
Shubham Pandey	Technology Lead & Founder, VOUCHIR	**APPROVED**	November 9, 2026
Enterprise CISO / InfoSec Lead	Client Security Review Board	Pending Review	[Date]
Data Protection Officer (DPO)	Enterprise Legal & Governance	Pending Review	[Date]

Document Version: 4.2.0-ENTERPRISE-SPEC **Status:** Active Production Architecture **Classification:** Confidential — Enterprise Distribution Only