Boosting digital adoption of MSME ecosystem

TSI DPDP Consent Management System

Integration Approach

28th May 2025
V1.0

TSI Tech Solutions Cooperative Foundation
A section 8 company

https://tsicoop.org

Table of Contents

Version History

Author(s)	Date	Version	Description
Satish Ayyaswami TSI Tech Solutions Cooperative Foundation	28/05/2025	0.1	Draft

Abbreviations, Terms and Definitions

DPDP Act	Digital Personal Data Protection Act 2023
CMS	Consent Management System
DF	Data Fiduciary
DP	Data Processor
CM & CA	Consent Manager & Consent Aggregator
DPB	Data Protection Board
SDK, API, WCAG	Software Development Kit, Application Programmable Interface, Web Content Accessibility Guidelines
PII	Personally Identifiable Information
MFA, RBAC	Multi factor authentication, Role based Access Control

About Us

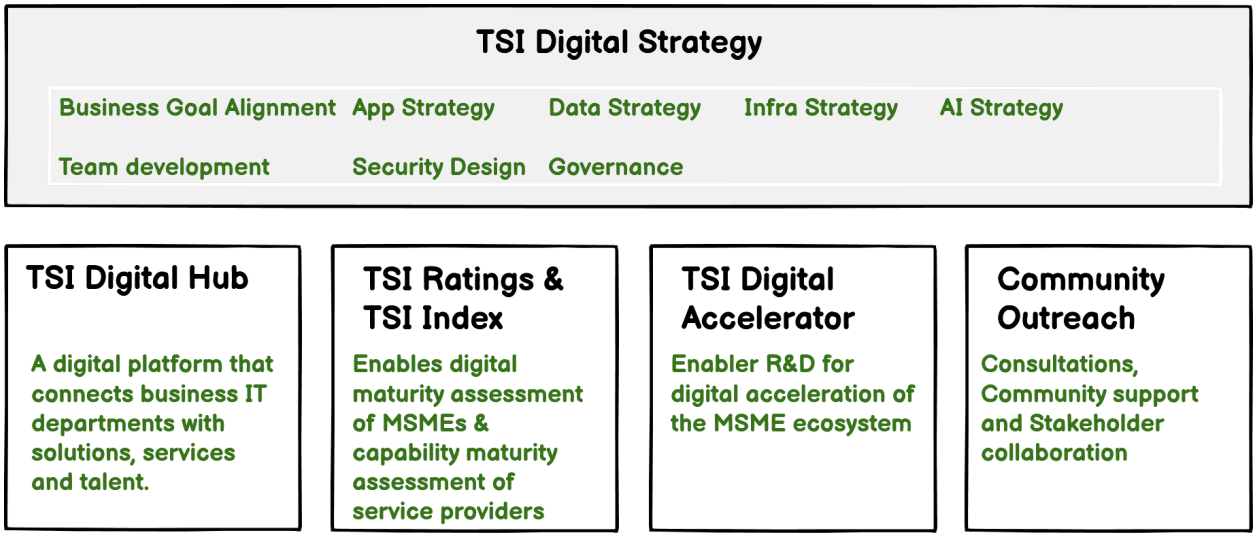
TSI Tech Solutions Cooperative Foundation (TSI Coop) initiative aims to address critical gaps in the MSME digital ecosystem by enabling businesses to implement successful technology strategies with the help of niche providers. Our mission also focuses on creating sustainable pathways for graduates from tier-3 and tier-4 institutions while fostering a more equitable and efficient domestic IT supply chain.

TSI stands for Technology & Social Impact. 'Coop' embodies the spirit of a cooperative economic model, where smaller providers and MSMEs collectively drive digital adoption within the ecosystem, fostering shared growth and opportunity.

While our IT machinery prioritizes foreign markets, GCCs, high profile startups and large enterprises, MSMEs are underserved. We aim to unlock their potential by facilitating the following:

- Discovery of niche providers, products, services and talent. Direct Interactions.
- Continuous digital maturity assessment of MSMEs ecosystem participants, helping stakeholders' identify areas for improvement
- Enabler R&D for digital acceleration of MSME ecosystem
- Community support and stakeholder collaboration

Our offerings for the MSME ecosystem below:



TSI DPDP Consent Management System is a key component of our TSI Digital Accelerator program.

Scope

This document outlines the strategic approach to integrating the TSI Digital Personal Data Protection Solution with external systems and entities. The goal is to establish robust, secure, and compliant data flows that enable Data Fiduciaries to meet their obligations under the DPDP Act, 2023, while minimizing operational friction. Our focus is on providing clear APIs and standard protocols to facilitate seamless interoperability.

This document serves to:

- Define the core principles guiding all integration efforts.
- Detail the various integration scenarios and patterns supported by the DPDP Solution.
- Provide technical guidelines for Data Fiduciaries, Data Processors, and System Integrators to effectively integrate their systems with the DPDP Solution.
- Outline the security considerations for all integration touchpoints.

The DPDP Solution (Consent Management System - CMS) is designed to integrate with:

- **Data Fiduciary's Core Systems:** Websites, Mobile Applications, CRM, ERP, Marketing Automation Platforms.
- **Data Processors' Systems:** Cloud providers, analytics platforms, advertising networks, payment gateways.
- **Regulatory Bodies:** Specifically, the Data Protection Board (DPB) of India.
- **External Identity Providers:** For SSO/MFA.

Integration Principles

All integration efforts will adhere to the following principles:

1. **API-First Design:** All interactions with the DPDP Solution's core functionalities will be exposed via well-documented, RESTful APIs.
2. **Security by Design:** All integration channels will implement strong authentication, authorization, and encryption.
3. **Compliance-Driven:** Integrations will be designed to directly support and enforce DPDP Act requirements (e.g., granular consent, purpose limitation, audit trails).
4. **Standardization:** Preference for industry-standard protocols (HTTPS, JSON, TLS) to ensure broad compatibility.

5. **Transparency & Auditability:** Integration points will support comprehensive logging for auditing purposes.
6. **Scalability & Resilience:** Designed to handle high volumes of concurrent requests and ensure high availability.
7. **Ease of Use:** Provide clear documentation, SDKs (where applicable), and support for integrators.

Key Integration Scenarios & Patterns

The TSI DPDP Solution supports various integration patterns to accommodate diverse operational needs:

Direct API Integration (Push/Pull Model)

Description: Data Fiduciary or Data Processor systems directly call the DPDP Solution's APIs to exchange data or retrieve consent status.
Use Cases:

- **Frontend:** Displaying consent banners, submitting consent choices.
- **Backend:** Validating consent before data processing, retrieving consent history, managing Fiduciary/Processor profiles.
- **Data Processors:** Receiving data purging instructions, confirming data deletion.

Technical Details: RESTful APIs, JSON payloads, HTTPS, API Keys.

SDK/Library Integration

Description: Provide client-side (JavaScript, mobile SDKs) or server-side libraries to abstract API calls and simplify integration for common tasks.
Use Cases:

- **Websites:** Frontend consent collection and dynamic script blocking.
- **Mobile Apps:** Consent management within native applications.

Technical Details: JavaScript SDK for web, Native SDKs (Android/iOS) where applicable.

Service Adapter Webhook for data purge

Description: The DPDP Solution notifies integrated systems in real-time about significant events (e.g., consent withdrawal, policy updates, new privacy requests).
Use Cases:

- Triggering data purging processes in Data Fiduciary's & Data Processor systems upon consent withdrawal.
- Notifying Data Fiduciaries of new Data Principal rights requests.
- Manual Override for handling withdrawals & exceptions

Technical Details: HTTPS POST requests from CMS to registered webhook URLs, requiring the recipient system to verify incoming requests.

Detailed Integration Points

This section details how specific modules of the DPDP Solution integrate with external systems.

Data Fiduciary Onboarding & Management:

External System: Data Fiduciary's IT/DNS Management System.
Interaction: DPDP Solution captures Fiduciary Name, Domain. Data Fiduciary adds a unique DNS TXT record to their domain.
Method: Manual DNS update by Fiduciary, automated DNS lookup by DPDP Solution backend for validation.
Purpose: Securely link the CMS deployment to the Fiduciary's domain for trust and operation.

Consent Collection & Enforcement (Website/App Integration):

External System: Data Fiduciary's Website/Mobile Application (Frontend & Backend).
DPDP CMS Solution Module: Policy Service, Consent Record Service, Dynamic Rendering.
API/SDK:

- GET /api/personal-data-policies/active?fiduciaryId={fId}&jurisdiction={j}&lang={l} (Policy Retrieval).
- POST /api/consent (Record new/update consent).
- GET /api/consent/{userId}/active (Validate current consent for processing).

Method: Frontend JavaScript SDK/direct API calls from Fiduciary's application.

Purpose: Displaying consent UI, capturing user choices, and enforcing consent for data processing.

Data Processor Configuration & Interaction:

External System: Data Fiduciary's internal systems, Data Processor's systems.
DPDP CMS Solution Module: Fiduciary & Processor Service, Data Retention/Purge Service.
API/Method:

- **Fiduciary to CMS:** POST /api/webhook to register/update Data Processor profiles.
- **CMS to Processor:** Webhook for instructing data purges/anonymization requests initiated by Data Retention Policy or Data Principal Right to Erasure.
- **Processor to CMS:** Confirmation API calls from Processor when purge/anonymization is completed POST /api/purgestatus.

Purpose: Define processor scope, automate data lifecycle management based on Fiduciary instructions.

Notification Integration

External System:

Email Gateway (External SaaS**):** (e.g., Zoho Zepto, Mailgun, Sendgrid, Azure Communication Services Email)

- A reliable third-party service specializing in bulk and transactional email delivery.
- Provides APIs for sending emails.
- Handles email deliverability, bounce management, sender reputation.

SMS Gateway (External SaaS)**:** (e.g., Kaleyra, Gupshup, Azure Communication Services SMS)

- A reliable third-party service for sending SMS messages within India.
- Provides APIs for sending SMS.

DPDP CMS Solution Module: Notification Service

- Acts as the central orchestrator for all notifications.
- Receives events/triggers from other CMS microservices.
- Selects appropriate templates, resolves recipients, personalizes content.

- Dispatches messages to Email Gateway and SMS Gateway.
- Handles carrier routing, delivery receipts.

Purpose: Send out timely notifications to Data Principals and other stakeholders.

Regulatory Reporting (DPB Integration):

External System: Data Protection Board's (DPB) official API/Portal.
DPDP Solution Module: Regulatory (DPB) Service.
API/Method:

- POST /dpb/register (CMS registration with DPB).
- POST /dpb/reports/{type} (Breach notifications, compliance reports).

Security: Mandatory Two-Way SSL (Mutual TLS) for authenticated and encrypted communication.
Purpose: Fulfill mandatory reporting obligations and establish secure communication with the regulator.

Security Considerations for Integration

All integration points are designed with robust security measures:

- **API Authentication:** Strong authentication for all API endpoints (API Keys, OAuth 2.0 Bearer Tokens, Mutual TLS where highest security is required).
- **Authorization (RBAC):** API endpoints enforce role-based access control, ensuring only authorized systems/users can perform specific actions.
- **Encryption:** All data in transit across integration channels (APIs, webhooks, file transfers) must use TLS 1.2/1.3. Sensitive data should be encrypted at rest on receiving systems.
- **Input Validation:** Strict validation of all incoming payloads to prevent injection attacks and ensure data integrity.
- **Rate Limiting & Throttling:** Protect APIs from abuse and denial-of-service attacks.
- **Secure Webhooks:** Require HMAC signatures for webhook payloads to verify sender authenticity.
- **Audit Logging:** Comprehensive logging of all API calls, data exchanges, and access attempts across integration points for forensic analysis.
- **Error Handling:** Implement clear, non-verbose error messages to prevent information leakage.

- **Data Processing Agreements (DPAs):** Mandate legally binding DPAs with all Data Processors, outlining data protection responsibilities and security obligations.

Support & Maintenance

API Documentation: Comprehensive, up-to-date API documentation (e.g., OpenAPI/Swagger) for all integration points.
SDKs & Samples: Provide SDKs and code samples in popular languages to accelerate integration.
Version Management: Clearly version APIs to ensure backward compatibility and smooth upgrades.
Dedicated Support: Establish a dedicated support channel for integrators during onboarding and ongoing operations.