COMPLETE PACKAGE

# Four pieces. One platform.

Everything your team needs to enforce PII controls across KYC and AI workflows — from the command line to the compliance dashboard.

IN THE BOX

- **CLI + SDK for operators & developers**
- **Control Plane API for runtime enforcement**
- **Encrypted Vault with consent management**
- **Dashboard for audit & compliance teams**

01

## CLI & SDK

Two integration surfaces, one package. The CLI lets operators manage PII from the terminal. The SDK (`@treza/sdk`) lets developers integrate PII controls directly into application code.

- `treza pii submit` / `pii audit` / `pii delete`
- SDK: submit, consent, retrieve, and audit via API
- Works standalone or embedded in existing pipelines
- Node.js, TypeScript — no additional infrastructure

02

## Control Plane

The enforcement layer. Sits between every step in your AI pipeline and strips any PII field a step didn't explicitly declare it needs — automatically, at runtime.

- Per-step field policy declared in config
- Consent verified before every retrieval
- Violations flagged instantly with full context

03

## Vault

Encrypted PII storage backed by AWS KMS. Raw data never persists in plaintext — decryption only happens inside a TEE. Consent is checked on every retrieval request.

- KMS envelope encryption at rest
- TEE-only decryption — plaintext stays in the enclave
- Customer-scoped consent + declared purpose to retrieve

04

## Dashboard

The compliance team's view. Browse PII records (metadata only), manage consent grants, inspect the full audit trail by customer or workflow, and export for regulators.

- Audit log queryable by customer or workflow ID
- Grant and revoke consent without engineering
- 90-day TTL, exportable for GDPR / SOC 2 audits