WHITE PAPER: PERSONAL DATA VECTORS

Status	Published
Categories	Guidelines
Tag	

PRIVACY BY DESIGN, MINIMALISM, AND INBOUND PAYLOAD SANITIZATION

Executive Summary

This document defines how Synaptic Integrations handles Personal Data Vectors (such as user profiles, session logs, and access credentials). We apply a strict **Privacy by Design** methodology, actively stripping out sensitive identifiers at the perimeter to minimize risk exposure before data is committed to our system logs.

1. The Sanitization Pipeline

When a user interacts with the platform, all input data passes through an automated sanitization process before it reaches our backend storage:

```
[ RAW INPUT PAYLOAD ] ──> [ REGEX FILTER ARRAY ] ──> [ ANONYMIZED STRUCT ] ──> [ AUDIT LO
G ]
  (Contains PII/Names)      (Strips PII & Tokens)       (Safe Telemetry)         (Complia
nt)
```

- **Token-Stripping Filters:** Outbound and inbound payloads run through pattern-matching filters to catch and remove personally identifiable information (PII), such as phone numbers, credit card strings, or addresses.
- **Cryptographic Hashing:** Static identifying metrics (like user IDs or IP addresses) are instantly transformed into irreversible hashes using a unique

system key. This preserves data structure and system utility without storing readable personal records.

2. User Authentication Integrity

User access control is handled through an enterprise-grade Identity Provider framework utilizing secure JSON Web Tokens (JWT).

- **No Password Storage:** We do not store raw or un-salted passwords within our environment. Identity validation is managed through advanced cryptographic handshakes.
- **Multi-Factor Enforcement (MFA):** All platform access requires multi-factor confirmation, blocking brute-force attacks and credential reuse vectors.

3. Compliance Framework Mapping

Our personal data processing pipelines align directly with international privacy statutes:

- **Texas Data Privacy and Security Act (TDPSA):** Enforces consumer rights, data minimization mandates, and strict purpose-limitation bounds.
- **GDPR / CCPA Alignment:** Features clear, automated tools for data portability, complete access verification, and irreversible account deletion upon authorized request.