Data Security Privacy Plan

> **Source File:** generated-documents\dmbok\data-security-privacy-plan.md
> **Generated:** 30/07/2025 at 06:57:45
> **Generated by:** Requirements Gathering Agent - PDF Converter

Data Security & Privacy Plan

Generated by adpa-enterprise-framework-automation v3.2.0
Category: dmbok
Generated: 2025-07-17T08:33:23.953Z
Description: Defines the policies, procedures, controls, and responsibilities to protect data assets and ensure privacy compliance.

Document ID: DSEC-PLN-001
Version: 1.0
Status: Proposed
Date: 2025-07-17

Data Security & Privacy Plan

Project: adpa-enterprise-framework-automation
Version: 3.2.0

---

1. Introduction

1.1 Purpose

This document establishes the data security and privacy policies, controls, and responsibilities for the “adpa-enterprise-framework-automation” platform—a Node.js/TypeScript, modular, enterprise automation framework for requirements, project, and data management. The plan aims to prevent unauthorized access, use, disclosure, alteration, or destruction of data and ensure compliance with relevant privacy regulations.

1.2 Scope

This plan applies to all environments (development, test, production) and covers all data processed, stored, or transmitted by the framework, including:

- Customer, employee, and end-user data
- Project and requirements documentation
- Financial, operational, and audit data
- Intellectual property, templates, and proprietary logic
- Logs and telemetry

---

2. Security Policies

2.1 Data Classification Policy

- **Policy:** Data is classified as *Public*, *Internal*, *Confidential*, or *Restricted*.
- **Controls:**
  - Data classification is defined at the schema/model level.
  - Access is restricted via role-based access control (RBAC) and enforced in middleware and API layers.
  - Sensitive data (PII, financial) is marked and logged access is monitored.

2.2 Access Control Policy

- **Policy:** Enforce least privilege and RBAC across API, CLI, and integrated services.
- **Controls:**
  - **Authentication:**
    - JWT (JSON Web Tokens) and/or OAuth2 for user/API authentication.
    - Multi-factor authentication (MFA) required for privileged/admin access.
    - API keys are required for service/service and CLI access, rotated on a schedule.
  - **Authorization:**
    - RBAC with granular permissions; enforced via middleware and database queries.
    - Support for enterprise SSO integration (Azure AD, Google Identity, etc.).
  - **Access Reviews:**
    - Quarterly reviews of user, service, and admin access.

2.3 Encryption Policy

- **Policy:** Encryption is mandatory for all sensitive data at rest and in transit.
- **Controls:**
  - **At Rest:**
    - Use AES-256 for all persisted data (databases, object/file storage, secrets).
    - Credential and secret management via environment variables or secure vaults (Azure Key Vault, AWS Secrets Manager).
  - **In Transit:**
    - All API endpoints require HTTPS/TLS 1.3.
    - Internal service communication (microservices, provider APIs) also secured by TLS.
  - **Secrets Management:**

- No credentials or secrets are stored in source code or version control.
- .env files are excluded from repositories and managed per environment.

2.4 Logging & Monitoring Policy

- **Policy:** Security events and access are logged and monitored for anomalies.
- **Controls:**
  - Centralized logging (e.g., via Winston, Azure Monitor) with log rotation and retention.
  - Masking of sensitive data in logs.
  - Real-time monitoring and alerting for suspicious activity (failed logins, privilege escalation).

2.5 Incident Response Policy

- **Policy:** Maintain and regularly test a formal incident response plan.
- **Controls:**
  - Defined incident response team and escalation contacts.
  - Playbooks for common incidents (data breach, malware, DDoS).
  - Forensic logging to facilitate investigation.
  - Root cause analysis and post-incident reporting.
  - Regulatory notification in accordance with GDPR, CCPA, and other applicable laws.

---

3. Privacy Policies

3.1 Data Minimization

- **Policy:** Only data necessary for business and technical requirements is collected and retained.
- **Controls:**

    - Data fields and retention are reviewed during design and periodically thereafter.
    - Temporary files and cache are purged automatically after use.

3.2 Purpose Limitation

- **Policy:** Personal data is used only for specified, legitimate purposes.
- **Controls:**
    - Data usage is documented and limited by API/service design.
    - Use of data for analytics/training is opt-in and anonymized where possible.

3.3 Data Subject Rights

- **Policy:** Framework supports data subject rights (access, rectification, erasure, portability).
- **Controls:**
    - Mechanisms to process data subject requests within regulatory timeframes (e.g., GDPR 30 days).
    - Audit trails for data changes and subject requests.

3.4 Data Retention & Deletion

- **Policy:** Retain data only as long as necessary; securely delete data after retention period or upon request.
- **Controls:**
    - Data lifecycle management for all storage layers.
    - Secure wiping and cryptographic erase for deletions.
    - Automated job for expired data cleanup.

---

4. Roles & Responsibilities

Role	Responsibilities
Chief Information Security Officer (CISO)	Maintains the security program, approves policies, and oversees compliance.
Data Protection Officer (DPO)	Ensures regulatory compliance, manages privacy impact assessments.
IT Security Team	Implements and monitors technical controls, responds to incidents.
Solution/Platform Owners	Ensure application security posture and compliance.
Developers/Operators	Follow secure coding and operational practices.
All Users	Comply with security and privacy policies; report incidents.

5. Compliance

This plan supports compliance with:

- **GDPR** (EU General Data Protection Regulation)
- **CCPA** (California Consumer Privacy Act)
- **ISO/IEC 27001** (Information Security Management)
- **SOC 2** (Trust Services Criteria)
- Other regionally relevant regulations as applicable

6. Secure Development & Third-Party Management

- **Dependency Management:**
  - Regularly update and vulnerability scan all dependencies (npm audit, Snyk, etc.).
  - Use only trusted and well-maintained libraries (see project dependency list).
- **Secure SDLC:**
  - Static code analysis (e.g., SonarQube), code reviews, and security testing.
  - Automated pipeline checks for secrets, sensitive data, and vulnerabilities.
- **Third-Party Integrations:**
  - OAuth2 and API key management for Adobe, Azure, Google, Microsoft Graph, and others.
  - Contractual and technical due diligence for providers' security posture.

---

7. Training & Awareness

- All employees and developers receive annual security/privacy training.
- Targeted training for new features, regulations, and emerging threats.
- Simulated phishing and social engineering tests.

---

8. Plan Review & Maintenance

- **Review Frequency:** Annually, and after major system/regulatory changes.
- **Change Management:**

- All changes to this plan tracked and approved by the CISO and DPO.
- Emergency updates possible in response to incidents or urgent threats.

---

9. Appendix: Technical Controls Reference

- **API Security:**
  - Express.js: Helmet, CORS, rate limiting, input validation (express-validator, joi, zod)
  - JWT & API key authentication (see API-TESTING-COMPREHENSIVE-SUMMARY.MD)
  - Secure file uploads (multer) and document publishing (SharePoint, Confluence)
- **Monitoring:**
  - Logging (winston, morgan), centralized error reporting
  - Health checks (`/api/v1/health`)
- **Cloud Security:**
  - Azure/Cloud provider best practices (resource isolation, identity management)
  - Regular review of API and resource permissions (see AZURE-PORTAL-API-CENTER-SETUP-GUIDE.MD)

This plan is effective immediately upon project activation and must be acknowledged by all project participants.