Vendor Security, DPA & Data Retention Overview

Prepared for Chief Information Security Officers (CISOs), Compliance Committees, Legal Counsel, and Third-Party Risk Management (TPRM) teams evaluating AlphaTech's official-source Mexican KYC, KYB, and Anti-Fraud API platform.

1. Cloud Certifications & Control Framework Posture

> **Transparent Audit Posture:** AlphaTech operates 100% on Amazon Web Services (AWS regions `us-east-1` and `mx-central-1`), leveraging AWS physical and cloud infrastructure certified under **SOC 1/2/3, ISO/IEC 27001, ISO 27017, ISO 27018, and PCI-DSS Level 1**. AlphaTech's internal application and operational controls are mapped to the **SOC 2 Trust Services Criteria (Security, Confidentiality, Availability)** and **ISO/IEC 27001:2022 Annex A**. While corporate standalone SOC 2 Type II / ISO 27001 certification is on our formal audit roadmap, we provide full SIG Lite / CAIQ questionnaire responses, architecture walkthroughs, and dedicated VPC / On-Premise deployment options for regulated institutions.

2. Data Processing Addendum (DPA) — Executive Summary

All commercial agreements (available in English and Spanish) include our standard Data Processing Addendum aligned with Mexico's Federal Law on Protection of Personal Data Held by Private Parties (**LFPDPPP**) and international cross-border vendor standards:

- **Controller / Processor Roles:** The Customer acts as Data Controller (*Responsable*) and confirms lawful basis / holder authorization; AlphaTech acts strictly as Data Processor (*Encargado*) executing only Customer-instructed API queries.
- **Purpose Limitation & Zero Secondary Use:** AlphaTech never sells, brokers, profiles, or cross-pollinates Customer query inputs or results across tenants.
- **Approved Sub-processors:** Restricted to Amazon Web Services, Inc. (compute, KMS/Secrets Manager, encrypted ephemeral storage) and Cloudflare, Inc. (TLS/WAF edge protection).
- **Incident Notification SLA:** Mandatory written notification within **24 hours** of confirming any unauthorized access affecting Customer credentials or data.
- **Cross-Border Contracting:** Supports direct contracting with US, Canadian, UK/EU, and LATAM parent entities under English MSA + DPA, with USD (ACH/Wire) or MXN (CFDI 4.0) invoicing.

3. Data Retention, Stateless Processing & Cryptographic Disposal

Artifact Category	Encryption & Storage	Retention Window	Disposal Mechanism
REST API Payloads (Sync & Async JSON)	Ephemeral `AES-256-GCM` + Customer `RSA-4096-OAEP` public key.	**0 days cleartext** at rest (stateless in-memory).	Ciphertext readable solely by Customer private key; auto-expired after retrieval.

Artifact Category	Encryption & Storage	Retention Window	Disposal Mechanism
Batch CSV Inputs & Consolidated Outputs	TLS 1.3 upload + client public-key encrypted output archive in S3.	**1 hour** post-completion (or instant manual purge).	Automated S3 object + input file deletion upon window expiry or one-click Portal purge.
Billing & Audit Metadata	Pseudonymized `HMAC-SHA256` hashes; zero cleartext PII in logs.	Contractual audit term.	Cryptographic key destruction & tenant purge within 15 business days of termination.
Enterprise Strict Zero-Retention / On-Premise	Customer-managed VPC or local Kubernetes/Docker perimeter.	**0 bytes** outside Customer network.	100% governed by Customer's internal KMS and retention policies.

4. Cryptographic Architecture & Security Testing Summary

AlphaTech enforces defense-in-depth controls validated against the **OWASP API Security Top 10 (2023)**:

Security Domain	Implemented Technical Control
Transport & Edge Security	Mandatory TLS 1.3 / TLS 1.2 strong ciphers, HSTS, Cloudflare WAF, DDoS mitigation, and optional static CIDR IP allowlisting per tenant.
End-to-End Payload Confidentiality	Hybrid asymmetric encryption (`AES-256-GCM` content encryption key wrapped via `RSA-4096-OAEP-SHA256`). AlphaTech servers never possess the Customer's private decryption key.
Request Integrity & Anti-Replay	`X-API-KEY` + `X-TIMESTAMP` + cryptographic `RSA-PSS` signature verification on protected endpoints; webhooks signed with tenant-specific `HMAC-SHA256` secrets.
Network & Credential Isolation	Private AWS VPC subnets, RDS Proxy over mandatory TLS, least-privilege IAM roles per microservice, and automated zero-downtime database credential rotation via AWS Secrets Manager.
Vulnerability & Penetration Testing	Continuous automated dependency/SAST scanning, container image hardening, and periodic API security assessments covering authentication bypass, BOLA/IDOR, injection, and replay vectors (**0 open Critical or High findings**).
Portal Access & Governance	Role-Based Access Control (RBAC), TOTP Multi-Factor Authentication (MFA), per-user monthly consumption caps, and immutable administrative audit logs.

5. Procurement & Custom Due Diligence Contact

Need a countersigned NDA, full English/Spanish MSA + DPA templates, or completion of your institution's vendor risk questionnaire (SIG Lite, CAIQ, or custom bank security review)?

- **Security & Architecture Desk:** info@alphatechsis.com (Subject: *Vendor Security Review*)
- **Web Security Center:** https://alphatechsis.com/seguridad/
- **WCAG 2.1 AA Digital Accessibility:** Public portal & documentation verified for keyboard navigation and ≥ 4.5:1 contrast ratios.

© 2026 Alphatech Software Innovation Solutions S. de R.L. de C.V.