IdentityPulse

SECURITY POSITION PAPER

Security Overview

Architecture, Encryption & Data Handling

IdentityPulse / August 2026 / v3.1

IdentityPulse Pty Ltd · ABN 88 678 817 902 · 48 Chandos Street, St Leonards NSW 2065 · identitypulse.ai

01 Overview

IdentityPulse is an API-only identity verification and pre-fill enrichment platform. It provides real-time identity matching against over 4 billion reference records across 43 countries, returning match signals and confidence tiers to clients via a single API endpoint.

This document describes the security architecture, encryption controls, and data handling practices of the IdentityPulse platform. It is intended for procurement, compliance, and information security teams evaluating IdentityPulse as a vendor.

IdentityPulse operates under the Information Security Management System (ISMS) of Marketsoft Pty Ltd, which provides technology and operational services under a Perpetual Commercial Services Agreement. Marketsoft has over 35 years of enterprise data services experience, with long-standing engagements including American Express, 3M, and Adobe.

02 Data Architecture

IdentityPulse handles two distinct categories of data. Understanding the distinction is critical to evaluating the platform's security posture, because each category has a fundamentally different risk profile.

2.1 Reference Data (Stored)

Reference data is the identity dataset against which client queries are matched. It consists of over 4 billion records across 43 countries, sourced through licensed partnerships with primary-source data providers and standardised by specialist processing partners before being loaded into encrypted indexes.

Reference data is encrypted at rest using AES-256 and stored within designated Azure regions. IdentityPulse holds this data under licence for matching purposes only. It does not originate the underlying identity data, does not share it with clients in raw form, and does not act as a data broker.

2.2 Client Verification Payloads (Transient)

Client verification payloads are the identity attributes submitted by clients for verification (for example, a name, date of birth, and address). These payloads are processed in-memory, matched against reference data, and disposed of immediately after the response is returned. They are not written to disk, database, log, backup, or cache.

This transient processing model is the foundation of IdentityPulse's security posture. Because client-submitted PII is never persisted, the platform structurally eliminates data breach risk for client verification data. In a storage breach scenario, an attacker would encounter encrypted reference data only, with no record of which individuals have been verified, by whom, or when.

03 Verification Data Flow

IdentityPulse supports two response types. Both follow the same matching process but return different levels of data. The distinction is contractual and is governed by the Permitted Use terms in each client's Master Services Agreement.

3.1 Standard Verification

The client submits an API request containing identity attributes. The payload is received encrypted in transit via TLS 1.2/1.3. Matching is performed using privacy-preserving encryption techniques. Matching is deterministic and rule-based, not probabilistic or AI-driven. A match signal and one of three confidence tiers (Confirmed, High, Possible) is returned. No PII is included in the response. The transient verification payload is disposed of immediately.

3.2 Pre-fill Enrichment

Where pre-fill enrichment is enabled for a client, the matching process is identical to standard verification. However, on a confirmed match, verified identity fields (such as name, address, and date of birth) are returned alongside the match signal. This allows clients to auto-populate onboarding forms using verified data.

Pre-fill enrichment is not enabled by default. It is activated per client under specific contractual terms that define the permitted use, retention, and handling of the returned data. Clients without pre-fill enabled receive match signals and confidence tiers only.

04 Encryption & Data Protection

The following encryption and data protection controls are confirmed and in production:

Encryption in Transit	TLS 1.2/1.3 enforced on all API communication. No unencrypted channels are available.
Encryption at Rest	AES-256 encryption applied to all reference data at rest.
Key Management	Centralised secrets management via Azure Key Vault. API authentication credentials are rotated automatically on a monthly cycle.
Privacy-Preserving Matching	Privacy-preserving techniques are applied throughout the matching process. Full technical documentation of the matching architecture, including cryptographic implementation details, is available under NDA upon request.
Transient Payload Disposal	Client verification payloads are processed in-memory and disposed of immediately after the response is returned. They are not persisted to any storage medium.
Regional Data Residency	Reference data is processed and stored within designated Azure regions. Data for each country is isolated within its assigned region.

05 Authentication & Access Control

5.1 Client API Authentication

Client API access is authenticated using a dual-key model: an API key (passed as a request header) and a function code (passed as a query parameter). Both are required on every request. Keys carry usage tracking, verification limits, and expiry dates, and can be rotated or revoked per client without affecting other clients.

API keys are managed centrally via Azure Key Vault, with automated monthly credential rotation. OAuth 2.0 Client Credentials flow is on the platform roadmap.

5.2 Internal Access Control

Internal platform access is managed via Auth0 with multi-factor authentication (MFA), role-based access controls (RBAC), and JWT token management. All internal sessions are authenticated and scoped to the minimum privilege required.

Endpoint protection is provided by ESET PROTECT across all workstations and servers, with automated alerting for definition status, patch compliance, and detected threats. Data loss prevention (DLP) is enforced via Safetica. Device policies are managed through Microsoft Entra, including 15-minute inactivity screen lock and conditional access policies.

06 Infrastructure

6.1 Cloud Infrastructure

IdentityPulse runs entirely on Microsoft Azure. All API traffic is routed through Azure Front Door, which provides DDoS protection, geographic filtering, and web application firewall (WAF) rules at the edge before requests reach the application layer. Compute is provided by Azure App Service and Azure Functions. Data storage uses Azure SQL Database and Elasticsearch with encryption at rest.

6.2 Physical Security

All reference data is processed and stored within Microsoft Azure data centres, which maintain comprehensive physical security controls validated through SOC 2 Type II and ISO 27001 certifications, including 24/7 security personnel, biometric access, CCTV, and environmental controls.

The Marketsoft operational facility at 48 Chandos Street, St Leonards NSW 2065 maintains electronic PIN-controlled building access, CCTV surveillance, visitor registration with supervised access, after-hours physical locks and alarm systems, and segregated access to server and network infrastructure.

6.3 Vulnerability Management

Infrastructure vulnerability scanning is conducted quarterly using automated scanning tools. Azure Security Center provides continuous cloud infrastructure security posture assessment. Endpoint vulnerability monitoring is performed in real-time via ESET PROTECT. Identified vulnerabilities are assessed, prioritised by severity, tracked to closure, and reported to the Information Security and Compliance Committee under defined remediation timelines (critical: 48 hours, high: 15 days, medium: 30 days, low: 60 days).

Independent penetration testing is conducted annually by third-party specialists, covering OWASP Top 10, infrastructure testing, and SSL/TLS assessment.

07 Data Processing Model

IdentityPulse operates as a data processor, not a data controller. Reference data is sourced under licence through primary-source data partnerships, standardised by specialist processing partners, and loaded into encrypted indexes for matching. IdentityPulse does not originate the underlying identity data.

Client verification payloads are transient by design. IdentityPulse does not retain, log, or share client-submitted PII beyond the immediate verification response. Operational logs contain non-PII metadata only (timestamps, response codes, usage counters) and are retained under the Marketsoft ISMS retention policy.

EXPLICITLY ABSENT FROM THE ARCHITECTURE

Flat file transfer	No flat file transfer of reference data or verification results.
Raw PII in standard responses	Standard verification responses return match signals and confidence tiers only. Pre-fill responses return verified fields under MSA-governed Permitted Use terms.
Payload persistence	No persistent storage of client-submitted verification payloads.
Bulk data access	No bulk data access endpoints or batch extraction capabilities.
Credit reporting	IdentityPulse does not perform credit reporting or furnish data to credit bureaus.
Restricted geographies	No data processing from or storage in restricted geographies.

08 Compliance & Certifications

ISO 27001	Aligned. Formal certification in progress via the Marketsoft ISMS.
ISO 9001	Aligned via the Marketsoft quality management framework.
Azure SOC 2 Type II	IdentityPulse runs entirely on Azure infrastructure, which is independently SOC 2 Type II certified. Azure publishes its compliance reports publicly via the Microsoft Service Trust Portal.
AU ISM	Aligned to the Australian Government Information Security Manual.
GDPR	Architecture designed for data minimisation compliance. Processor-only model. Regional data residency. Transient payload disposal eliminates client PII retention.
eIDAS 2.0	Privacy-preserving architecture designed with consideration for emerging EU Digital Identity Wallet requirements.

09 Governance

IdentityPulse's information security governance is managed by Marketsoft Pty Ltd under a formal ISMS framework aligned to ISO 27001:2022. Marketsoft maintains a documented suite of security policies covering information classification, data handling, data retention and erasure, vulnerability management, data breach response, and business continuity.

Key governance parameters include a target uptime of 99.95%, Recovery Point Objective (RPO) of 15 minutes, Recovery Time Objective (RTO) of 4 hours, and defined incident response and escalation procedures.

Detailed technical documentation, penetration test summaries, and sub-processor information are available under NDA upon request. For security-related enquiries, contact **support@identitypulse.ai**.

SUMMARY

The most effective defence against a data breach is not having data worth stealing.

Client verification payloads are processed in-memory and disposed of immediately — they are never written to disk, database, log, or cache. Reference data is encrypted at rest and in transit. Matching is performed using privacy-preserving encryption techniques. Standard verification responses contain no PII. Where pre-fill enrichment is enabled, verified fields are returned under explicit contractual terms. Even in a storage breach scenario, an attacker would encounter encrypted reference data only, with no record of who has been verified.