PROJECT AEGIS FUNCTIONAL SPECIFICATION

Document: Aegis_Functional_Specification_v4.1.pdf

Status: Approved | Version 4.1 | Effective Date: October 15, 2023

Owner: Head of Digital Operations

Audience: Development, QA, Compliance, and Operations teams.

1.0 PRIMARY OBJECTIVE

This document defines the complete set of business rules, decision logic, and audit requirements for the Project Aegis Real-Time Compliance Orchestration Engine. It serves as the single source of truth for what the system must accomplish. Any discrepancy between system behavior and this specification constitutes a defect.

2.0 CORE COMPLIANCE FRAMEWORKS

The system shall evaluate all inbound digital transactions against three regulatory frameworks:

GDPR (General Data Protection Regulation): Focus on lawful basis, purpose limitation, and data subject rights (Articles 6, 17, 20).

CCPA/CPRA (California Consumer Privacy Act): Focus on consumer opt-out rights, data sales, and disclosure requirements.

APAC Data Framework (v2.3): Focus on cross-border data transfer restrictions and local storage mandates.

3.0 DECISION LOGIC & SCORING MODEL

A transaction's final status is determined by a weighted Compliance Score (0-100%).

APPROVED (Score ≥ 95%): Transaction is automatically routed to the downstream processing channel. No human intervention is required.

REVIEW REQUIRED (Score < 95%): Transaction is automatically queued in the Human Review Dashboard for analyst inspection and manual verdict. This includes all scores in the 90-94.9% "Grey Zone," which may indicate a rule matrix misconfiguration.

BLOCKED (Hard Failures): Transactions that violate immutable rules (e.g., invalid jurisdiction, missing mandatory consent flag) receive a score of 0% and are blocked without review.

4.0 AUDIT & NON-REPUDIATION REQUIREMENTS

For every transaction processed, the system must create an immutable audit record containing:

The original payload hash (SHA-256).

The complete event trail (ingestion, enrichment, rule execution steps).

The final compliance score and individual rule outcomes.

A timestamp and service identifier for each processing step.

This audit log is legally retained for 7 years and is the definitive record for all regulatory inquiries.

5.0 CHANGE CONTROL

Any modification to the logic defined herein requires a formal change request, review by Compliance and Legal stakeholders, and an update to this document version before implementation. This spec is implemented via the configurable Rule_Precedence_Matrix.xlsx and executed by the system architecture defined in the companion documentation.