

Security & Compliance SOP

The Cognition Factory — HAL-E and AAE

1. Purpose

This document outlines the high-level security and compliance posture for HAL-E (Hyper Accelerated Learning Engine) and AAE (Adaptive Assessment Engine). It is intended for prospective clients, partners, and decision-makers during evaluation and sales discussions.

2. Scope

This overview applies to all enterprise and institutional deployments of HAL-E and AAE. It summarizes key controls and compliance considerations without disclosing detailed technical implementation or internal operational procedures.

3. Compliance Frameworks

GDPR (General Data Protection Regulation)

We process personal data in accordance with GDPR principles. Data processing is limited to what is necessary for service delivery. Users retain rights to access, rectification, erasure, and data portability. Data Processing Agreements (DPAs) are available upon request for enterprise customers.

ISO 27001

Our information security management practices are aligned with ISO 27001 principles. We maintain documented policies covering access control, incident management, risk assessment, and continuous improvement of security controls.

4. Data Handling Principles

We follow these core principles across all deployments:

- Data minimization: Only necessary data is collected and retained.
- Purpose limitation: Data is used solely for the purposes outlined in our agreements.
- Security by design: Security and privacy considerations are embedded into system architecture from the outset.
- Transparency: Customers are informed about what data is processed and why.

5. Security Measures

Key security controls include:

- Encryption of data in transit (TLS 1.2+) and at rest using industry-standard algorithms.
- Strict access controls with role-based permissions and audit logging.
- Regular security assessments and vulnerability management.
- Secure development practices and code review processes.
- Incident response procedures with defined escalation paths.

6. Roles and Responsibilities

Security and compliance responsibilities are shared between The Cognition Factory and the customer. We are responsible for the security of the platform itself. Customers are responsible for configuring access controls appropriately, managing user accounts within their organization, and ensuring their use of the system complies with applicable laws.

7. Subprocessors and Third Parties

We use a limited number of subprocessors to deliver the service (e.g., infrastructure providers). A current list of subprocessors is available to enterprise customers upon request. All subprocessors are contractually bound to appropriate confidentiality and security obligations.

8. Incident Response

We maintain documented incident response procedures. In the event of a confirmed security incident affecting customer data, we will notify affected customers without undue delay, in accordance with applicable legal requirements and our contractual obligations.

9. Documentation Availability

This document provides a high-level overview. Detailed security documentation, including technical controls, risk assessments, and operational procedures, is available to qualified prospects and customers under appropriate confidentiality agreements during the sales and implementation process.

10. Version History

Version 1.0 — July 2026 — Initial release