Actee – AI Security & Architecture Overview

## Summary

Actee integrates AI into the platform through a controlled and secure architecture.

Key principles include:

- AI is accessed only through the Actee platform
- OpenAI GPT Enterprise API is used for AI processing
- users remain responsible for reviewing generated content
- uploaded documents are automatically deleted after game creation
- AI functionality operates within Actee's broader GDPR and security framework

Further details are available at:
https://actee.com/terms-and-gdpr/

## Actee – AI Security & Architecture Overview

This document provides an overview of how artificial intelligence (AI) functionality is integrated into the Actee platform, how data flows through the system, and how security and deletion mechanisms are implemented.

This document complements Actee's broader GDPR and security documentation available at:
https://actee.com/terms-and-gdpr/

Detailed Technical and Organisational Measures (TOMs) are maintained internally and can be shared upon request during procurement or security review processes.

---

## 1. Overview of AI Architecture

AI functionality within the Actee platform is implemented through a controlled backend integration with the **OpenAI GPT Enterprise API**.

The architecture follows a standard enterprise pattern:

User → Actee Platform → Actee Backend → AI Service (API) → Actee Platform → User

Key characteristics:

- AI is accessed only through the Actee platform
- AI services are integrated via secure API calls

- users do not interact directly with external AI systems
- all AI interactions pass through Actee's application layer

This architecture ensures that Actee maintains control over data processing and AI usage.

---

## 2. AI Processing Flow

When AI functionality is used to create a learning game or training scenario, the following process occurs:

1. The user provides instructions or uploads optional documents within the Actee platform.
2. The Actee backend processes the input and extracts relevant context.
3. Selected content is sent to the AI model through the GPT Enterprise API.
4. The AI generates structured output (for example game elements, scenarios, or exercises).
5. The output is returned to the Actee platform and presented to the user for review and editing.

AI output is always reviewed and controlled by the user within the platform.

---

## 3. Handling of Uploaded Documents

Users may upload documents to assist in generating a game or learning simulation.

Examples include:

- training materials
- workshop descriptions
- strategy documents
- internal process descriptions

Document handling follows this process:

- the document is temporarily processed within the platform
- relevant context may be extracted and sent to the AI service
- AI-generated output is returned to the platform

Uploaded documents are used only to generate the requested game or training content.

Once the game has been created, uploaded documents are **automatically deleted from the system** to ensure that documents are not retained longer than necessary.

---

## 4. Data Flow Summary

The simplified data flow for AI processing is:

User Input
→ Actee Platform
→ Actee Backend Processing
→ GPT Enterprise API (AI generation)
→ Actee Platform Output
→ User Review and Editing

This design ensures that:

- Actee controls all interactions with the AI service
- AI requests are mediated through the platform
- AI-generated outputs remain within the Actee system

---

## 5. Security Controls for AI Processing

AI processing is protected by the same security framework applied to the Actee platform.

Security measures include:

- authenticated access to the platform
- secure API communication with the AI provider
- controlled backend integrations
- monitoring and logging of system activity

These controls form part of Actee's broader security framework.

More information is available at:
https://actee.com/terms-and-gdpr/

---

## 6. AI Data Retention

AI processing follows strict data minimisation principles.

Key retention practices include:

- uploaded documents are used only for generating the requested game
- documents are **automatically deleted once the game has been created**
- AI outputs remain within the platform for the user to review and edit

This approach ensures that temporary input data is not retained longer than necessary.

## 7. AI Model Training

AI processing uses the **OpenAI GPT Enterprise API**.

Under this API-based model:

- customer inputs are not used to train OpenAI models
- data is processed only to generate the requested output
- model training remains separate from API interactions

This helps ensure that customer information submitted through the Actee platform is not used to improve or train the underlying AI models.

---

## 8. Compliance and Governance

AI functionality within Actee operates within the platform's broader compliance framework, including:

- GDPR compliance
- Actee Terms and Data Processing Agreement
- internal Technical and Organisational Measures (TOMs)

Further information can be found at:
https://actee.com/terms-and-gdpr/

Detailed security documentation may be provided upon request during enterprise procurement or vendor security assessments.

---