amazee.ai

Drupal AI Provider Whitepaper

Technical White Paper

Version: 1.0 | **Date:** December 2025

Contact: ai.support@amazee.io

Trust Center: trust.amazee.io

1 | Regional Hosting & Deployment Flexibility

amazee.ai Drupal AI Provider supports full deployment flexibility through its cloud-native architecture:

Customer-Controlled Regional Selection

Infrastructure is deployed in the region of choice by the customer, including:

 Switzerland

 Germany

 United Kingdom

 United States

 Australia

Additional regions available upon request.

Supported Environments

- Public Cloud (AWS or alternatives like Azure, GCP)
- Private Cloud (via customer tenancy)
- On-Premises deployments (via Kubernetes)

Local & Regional Compliance

Hosting respects data residency preferences with full sovereignty over location and infrastructure.

Drupal Integration

The Drupal AI Provider module integrates directly with your existing Drupal hosting, with no migration required. AI infrastructure operates independently while your Drupal site remains with your current hosting provider.

2 | Data Encryption

amazee.ai applies encryption consistently across transit and storage layers:

At Rest: All hosted data, including vector embeddings of your indexed Drupal content, is encrypted using provider-managed encryption keys (e.g., AWS, Azure, GCP).

In Transit: TLS 1.2+ is enforced across all endpoints; all APIs are HTTPS-secured.

End-to-end/Secure Enclave for in-use encryption is available in private region deployments upon request.

---

3 | Access Control & Identity Assurance

Domain Verification: Only valid emails can be used for account creation, ensuring organizational control over who can create API keys for your organization.

Administrative Access Control:

- **No Access to User Conversations:** amazee.ai does not access input/output data under any circumstance by default.
- **No Query or Response Logging:** User queries to the AI and LLM responses are never logged or retained (see Section 4).

- **Restricted Support Access:** In edge cases (e.g., service restoration), authorized personnel may access available logs or data only with explicit, documented consent from the user.

API Key Management:

- Multiple API keys can be created under a single team account
- Environment-specific keys enable separation between development, staging, and production
- Rate limits and storage quotas are enforced per key for isolated resource management

---

4 | Data Logging & Observability

No Input/Output Logging: User queries and model responses are never logged or retained.

Metadata Logging Only:

- API key usage
- IP addresses (for security monitoring)
- API version
- Model ID and region
- User email address and request headers

These logs support fraud detection, incident response, and audit traceability without capturing sensitive content.

5 | Data Isolation & Storage Control

Dedicated AI Instances: Each customer interacts with isolated model instances (e.g., via AWS Bedrock) to prevent data leakage between customers.

Dedicated Vector Database: Each Drupal AI subscription includes a dedicated vector database instance:

- Vector embeddings of your indexed Drupal content are stored in your isolated database
- Storage limits are per database (1 database for Pro plan, up to 6 databases for Growth plan)
- Data is never shared across customers
- amazee.ai personnel have no access to vector database contents

Content Indexing: Only the Drupal content explicitly indexed through the Search API integration is converted to vector embeddings and stored. This gives you complete control over what data enters the AI system.

Environment Separation: Using environment-specific API keys and Search API collections enables clean separation between development, staging, and production data within your organization.

6 | Key Management

amazee.ai provides Private API Keys that work with OpenAI-compatible endpoints, managed securely through Drupal's Key module.

Simple Setup:

1. Navigate to /admin/config/ai/settings in your Drupal site
2. Select "amazee.io" as your AI provider
3. Enter your email address
4. Verify via email code
5. Keys are automatically provisioned and stored securely

Bring Your Own Key (BYOK) is not required, but the infrastructure is technically compatible with BYOK scenarios through standard integrations.

---

7 | Compliance & Certifications

amazee.ai adheres to internationally recognized security standards and provides verified compliance documentation:

GDPR Compliance: Architected to meet all core requirements of the General Data Protection Regulation (EU 2016/679).
ISO 27001 Certified: Verified compliance available via our Trust Center.
SOC 2 Type II: Available for review on request via NDA.

PA Contracts: Available to all enterprise customers on request.

Data Sovereignty: Regional deployment options ensure your data remains within your chosen jurisdiction, supporting compliance with local data protection regulations.

---

8 | Security Audits & Penetration Testing

amazee.ai maintains a proactive stance on infrastructure testing and vulnerability management:

Regular Security Testing:

- Annual third-party penetration testing is conducted as part of our ISO 27001 and SOC 2 compliance processes
- Tests are executed by certified external security specialists simulating real-world attack scenarios
- Detailed results and mitigation reports are made available upon request or via our Trust Center

Customer-Initiated Penetration Testing: amazee.ai supports customer-led penetration testing under controlled conditions:

Advance coordination is required to avoid operational disruptions and false alarms.

Customers must define:

- Scope (which systems, environments)
- Methods/tools used
- Timing and duration

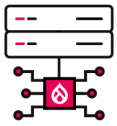
For high-impact testing (e.g., DDoS simulations), we may provision dedicated infrastructure to isolate the test environment.

These arrangements are typically made with enterprise clients who have formal security audit requirements.

---

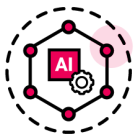
9 | Drupal AI Provider Architecture

The amazee.ai Drupal AI Provider module serves as a bridge between Drupal's AI module ecosystem and amazee.ai's sovereign AI infrastructure:



Integration Layer: The provider module integrates with your existing Drupal installation without requiring migration or hosting changes.

Search API Integration: Content indexing is managed through Drupal's Search API, giving you granular control over which content is vectorized.



Multiple LLM Access: Automatic access to multiple language models through a single API key, enabling flexibility in model selection for different use cases.

Open Source Foundation: Built on Drupal's open source AI module ecosystem, avoiding vendor lock-in and enabling community-driven innovation.

10 | Use Cases & Data Flow

Typical Drupal AI Workflows:

1 Content Indexing:

- You configure Search API to index specific Drupal content
- Content is sent to amazee.ai for vectorization
- Vector embeddings are stored in your dedicated vector database

2 AI-Powered Features:

- User queries (e.g., chatbot interactions, content recommendations) are sent to amazee.ai
- Queries are processed using your regional LLM instance
- Relevant context is retrieved from your vector database
- Responses are generated and returned to your Drupal site
- No queries or responses are logged by amazee.ai

3 Administrative Operations:

- API key management through Drupal's Key module
- Usage monitoring (in development)
- Collection management for environment separation

Data Retention: Only vector embeddings of your indexed content are retained in your dedicated database. All query and response data is ephemeral and never logged.

Conclusion

The amazee.ai Drupal AI Provider is designed to give Drupal organizations complete control over their data, hosting, and security posture while enabling powerful AI capabilities. By enforcing strong isolation principles, regional deployment options, and modern encryption practices, amazee.ai offers a foundation of trustworthy AI infrastructure purpose-built for the Drupal ecosystem.

The combination of:

- Dedicated vector database instances per customer
- Isolated LLM processing per customer
- No logging of queries or responses
- Regional data sovereignty
- Integration with existing Drupal hosting
- Enterprise-grade compliance certifications

...ensures that organizations can confidently deploy AI capabilities while meeting the most demanding security, privacy, and compliance requirements.

For additional technical documentation or compliance information, please contact: ai.support@amazee.io

Additional Resources:

Drupal AI Provider Module: https://www.drupal.org/project/ai_provider_amazeeio

Trust Center: trust.amazee.io