



Privacy AI White Paper

Version: 1.1

Date: September 2025

Contact: ai.support@amazee.io

Trust Center: trust.amazee.io

1. Regional Hosting & Deployment Flexibility

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

Customer-Controlled Hosting: Infrastructure can be deployed in the customer's preferred region, including Switzerland, Germany, Australia, the U.S., or any Kubernetes-compatible environment.

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.

2. Data Encryption

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

- At Rest: All hosted data 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 available in private region deployments upon request.

3. Access Control & Identity Assurance

- Domain Verification: Only verified domains can be used for account creation, ensuring organizational control.
- Administrative Access Control:
 - No Access to User Conversations: amazee.ai does not access input/output data under any circumstance by default.
 - Restricted Support Access: In edge cases (e.g., service restoration), authorized personnel may access logs or data only with explicit, documented user consent.

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.

5. Data Isolation & Storage Control

- Dedicated AI Instances: Each customer interacts with isolated model instances (e.g. via AWS Bedrock) to prevent data leakage.
- Vector Storage Isolation:
 - Chat history and embedding data are stored within the customer's private container.
 - Data is never shared across tenants, and amaze.ai personnel have no access to internal vector databases.
- Multi-Agent Defense: Inputs are processed by multiple AI agents to mitigate prompt injection risks via Resource Poisoning from context sources.

6. Key Management

amaze.ai provides a Private API Key working with OpenAI-compatible endpoints.

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 I/II: Available for review on request via NDA.
- DPA Contracts: Available to all enterprise customers on request.

8. Security Audits & Penetration Testing

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

- Annual third-party penetration testing is conducted as part of our ISO 27001 and SOC 2 compliance processes.
- These tests are executed by certified external security specialists simulating real-world attack scenarios to surface and mitigate vulnerabilities.
- Detailed results and mitigation reports are made available upon request or via our Trust Center, fulfilling enterprise and government procurement standards.

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.

Conclusion

amazee.ai's infrastructure is designed to give customers full control over their data, hosting, and security posture. By enforcing strong isolation principles, regional deployment options, and modern encryption practices, amazee.ai offers a foundation of trustworthy AI infrastructure.

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