

October 2026

Beacon AI Security Overview.

How Unimarket protects customer data when AI features are used

Summary.

Beacon AI is Unimarket's AI assistant for procurement. It gives buyers plain language guidance based on their organization's own procurement policy documents and, for Nova customers, lets users ask questions about the procurement data held in their Nova modules. Unimarket also uses AI to extract data from emailed invoices and contract documents. AI features are off by default and sit within Unimarket's independently audited security program.

- Unimarket holds SOC 2 Type 2 and is independently audited every year.
- Customer data is not used to train large language models.
- AI features can only access data that the signed in user is already permitted to see.
- Customers decide whether AI features are enabled, and which users can use them.

Security assurance and certifications.

Framework	What it demonstrates	Independent assessment
SOC 2 Type 2	Controls operate effectively over time	Audited annually
HIPAA	Safeguards for protected health information	Assessed alongside SOC 2
PCI DSS 4.0.1	Security standard for payment card data	Assessed annually

AI features and processing locations.

Feature	What it does	Where data is processed
Beacon AI	Answers procurement and policy questions in plain language, using the customer's own policy documents. Nova customers can also ask about data held in their Nova modules.	US customers: in the United States. Australian and New Zealand customers: currently outside Australia, including the United States. An opt in setting to process requests in Australia is under development.
Document extraction	Extracts data from emailed invoices and contract documents. Users do not enter free text.	US customers: in the United States. Australian and New Zealand customers: in Australia.

Data storage and encryption.

- Data, backups and disaster recovery are held in the customer's hosting region. Australian and New Zealand customers are hosted in Australia, and US customers are hosted in the United States. Disaster recovery is tested every six months.
- Beacon AI conversation history is stored within the application, in the customer's hosting region, for the life of the customer's contract, regardless of where Beacon AI requests are processed. It is then deleted in line with the Data Management Policy in the Unimarket Trust Center.
- Data at rest is encrypted with AES 256 bit. Data in transit uses TLS 1.2 or higher, with strong ciphers. Web certificates use RSA (2048 bit minimum) or ECC (256 bit minimum) with SHA2 or greater.

Large language models and training.

- Beacon AI uses large language models provided through commercial enterprise AI services, not public consumer AI products, so data is handled under strict contractual terms.
- Unimarket does not use customer data to train large language models. Its agreements with AI providers contractually prohibit them from retaining customer data or using it to train their models.

Full detail is in the AI Data and Privacy Policy: <https://www.unimarket.com/privacy-and-security/ai-data-privacy-policy/>

Data isolation and access control.

- Customer data is segregated between customers.
- AI features only access data that the signed in user is already permitted to see. They follow the roles and permissions the customer has configured, and are never given broader access than the user has. Beacon AI can draw on the customer's policy documents and, for Nova customers, any Nova data and tools the user is permitted to access.
- AI actions are logged and auditable. Customers can request access to audit logs through Unimarket support.
- Safeguards include prompt injection prevention, output checking before the system acts on a response, and rate limiting on AI endpoints.

Secure development and operations.

- AI features are built within the Unimarket platform codebase and follow a secure software development lifecycle, incorporating OWASP guidance for web applications, APIs and large language models. Every change requires peer and secure code review, and automated checks must pass before a change reaches production.
- Access to source code and production environments follows least privilege. Privileged access requires MFA and named accounts, is reviewed at least quarterly, and is logged.
- Vulnerability scanning is continuous. Critical and high vulnerabilities are remediated within 30 days, and penetration testing is performed annually.

AI governance and incident response.

- Unimarket's AI governance framework aligns with ISO/IEC 42001 principles and covers both Unimarket managed AI and approved third party AI services. Unimarket is not currently ISO/IEC 42001 certified.
- All staff are trained on the responsible use of AI, and incidents involving AI are handled under Unimarket's Incident Response Plan.
- Unimarket notifies affected customers of a security breach involving their data within 72 hours of becoming aware of it.

- AI responses can contain errors. Users should review responses before relying on them, and a person stays in the loop for destructive or financial actions.

Customer controls.

Control	What the customer can do
Opt in	AI features are off by default. Unimarket activates them on request, and customer administrators can then enable or disable them within the system.
Role based access	Customers choose which users can use AI features through user roles.
Audit logs	Customers can request access to audit logs through Unimarket support.
Regional processing	For Australian and New Zealand customers, a setting to process Beacon AI requests in Australia is under development and is not yet available. Requests from US customers are always processed in the United States.

Subprocessors.

Unimarket uses a variety of subprocessors to deliver the platform and its AI features, including Google Cloud (platform hosting and AI services) and Microsoft Azure (hosting for some Source to Contract modules). Before engaging any subprocessor, Unimarket carefully vets its privacy, security and confidentiality practices and signs agreements that carry the applicable data protection obligations. AI service providers are contractually prohibited from retaining customer data or using it to train their models. The current list of subprocessors, including any changes, is published at <https://www.unimarket.com/privacy-and-security/sub-processors-list/>

Further information.

AI Data and Privacy Policy: <https://www.unimarket.com/privacy-and-security/ai-data-privacy-policy/>

The Unimarket Trust Center at <https://trust.unimarket.com/> holds Unimarket's security policies, including the Data Management Policy and the Third Party Management Policy.

Security questions can be sent to security@unimarket.com