AIVO Assist security and data flow brief

UK and US supplier review | Version 1.0 | 25 November 2026

Prepared for information security, procurement and privacy teams. This brief describes how AIVO Assist is deployed on a client website, what data it handles, and the security and privacy commitments AIVO, Inc. publishes. The order form and the AIVO Assist Data Processing Addendum (DPA) set out the deployment-specific details for each client.

1. Service and deployment scope

AIVO Assist helps human buyers and their AI agents resolve product or service suitability questions against information the client has approved. It runs from a client-approved knowledge repository and one or more question routes on the client's website. Any connection to other client systems is scoped and agreed separately in writing.

Service	Website footprint
Free store test	Conducted externally against public product pages. No installation and no access to client systems.
Assist Answer	One visible link on the client's site routes submitted questions to a private client dashboard, where the client approves and publishes answers. The link is not a visitor-tracking script.
Assist Expert	Managed live product expert that answers from the client-approved knowledge repository. Routes are agreed for each deployment and can include an expert page and form on the client's domain, a WebMCP tool, Ask-by-URL links, an MCP server and a REST API.

Standard access boundary

Standard scope uses only client-approved product or business facts and the questions buyers submit. AIVO, Inc. does not require corporate VPN access, internal network credentials, CRM, ERP or customer database access, payment processing, or checkout write permissions. Any optional integration requires a separate written scope and permission review.

Each deployment has a spend cap. When the cap is reached, answers stop, the client is alerted, and the client can restart the service.

2. Architecture and information flows

Stage	Data and destination
1 Inquiry	A buyer or AI agent submits a product-fit question through a client-approved route.
2 AIVO, Inc. service	The question and technical request data (IP address, user agent and, if declared, the agent's name) reach the AIVO-hosted Assist service over HTTPS/TLS.
3 Approved evidence	Assist Expert consults the client-approved knowledge repository. With Assist Answer, the client reviews and approves each answer in its dashboard.

Stage	Data and destination
4 Model processing	Assist Expert calls a commercial AI model API from AIVO-hosted services to compose the answer from approved facts. Providers are used only on terms that exclude training on client data. AIVO, Inc. does not train or fine-tune models.
5 Response	A verdict (Fits, Fits if, No suitable option, or Need a little more information), the deciding facts and sources, and a random answer reference return to the buyer or agent.
6 Reporting	Consultation records and answer references feed the client dashboard. If the client connects its own records, order or booking references and values support outcome attribution.

3. Data inventory and retention

Data category	Retention
Consultation log (request text, route, time, answer reference)	13 months, then deleted or kept only as counts.
Technical request data (IP address, user agent, declared agent name)	30 days, for security and abuse management.
Charge records	7 years.
Linked commercial outcomes (optional)	Life of the contract.
Approved knowledge repository	Life of the contract; returned and deleted within 30 days after termination.

AIVO Assist does not ask for names, email addresses, phone numbers, account numbers, payment details or exact location, and buyers are told to leave personal details out. If personal details appear in a free-text request anyway, they are kept only in that request's log entry, and health, religion and sexual orientation details are deleted once found. Outcome data may be personal data, depending on what the client connects.

4. Security controls

Control area	Current position
Hosting and storage	The application database and backups, including consultation logs, are hosted in the United States. Static front-ends are served through a global delivery network.
Encryption	HTTPS/TLS for browser and AI-provider connections. The database and backups are encrypted at rest.
Access control	Role-based access, with client access logically segregated. AIVO, Inc. staff access is limited to authorized personnel using multi-factor authentication, and every access is logged. SSO is not currently supported.
Model training	Client and consultation data are never used to train AI models.

Control area	Current position
Subprocessors	Hosting and AI model providers. The current list, with processing locations, comes with each order form and is available on request. Clients receive 30 days' notice before a new subprocessor is added.
Deletion and export	Clients own their consultation and outcome data and can request deletion of any record at any time. At contract end, clients can request an export within 30 days; AIVO, Inc. then deletes the data within a further 30 days unless the law requires keeping it. Production deletion and backup expiry are separate, documented steps.

5. Privacy and contract

Topic	Position
Roles	For consultations on a client's website, the client is the controller and AIVO, Inc. is the processor under the client agreement and the AIVO Assist DPA. AIVO, Inc. is the controller only for its own website, aivocorp.com.
International transfers	Data is held in the United States. Transfers from the UK, EU, EEA or Switzerland rely on the EU Standard Contractual Clauses and the UK Addendum. Terms for US engagements are set in the client agreement.
Individual rights	Requests from individuals about a client's website go to the client. AIVO, Inc. helps the client respond within 10 business days.
Breach notification	Notification terms are set out in the AIVO Assist DPA.

6. Assurance position

AIVO, Inc. does not hold ISO 27001 certification or a SOC 2 report, and an independent penetration test of its services has not yet been completed. Certifications held by infrastructure providers apply to those providers' own services. AIVO, Inc. will complete the client's security questionnaire and document the scoped deployment for the client's own risk assessment.

Reference documents

AIVO Assist service description · https://aivocorp.com/assist
AIVO, Inc. procurement information · https://aivocorp.com/procurement
AIVO, Inc. privacy notice · https://aivocorp.com/privacy

Supplier

Renu Earth, Inc. dba AIVO, Inc. · Delaware C Corporation, USA
131 Continental Dr, Suite 305, Newark, DE 19713, USA
Security and procurement contact: Tim de Rosen · tim@aivocorp.com
AIVO, Inc. is not affiliated with Aivo, the conversational AI company acquired by Engageware in 2023.