VENDOR PACKAGE

AskReplay

Security, privacy, AI data handling, architecture, and procurement details, prepared for vendor review. Last reviewed August 2, 2026.

1. What the service does

AskReplay is a software-as-a-service workspace for sales engineering teams. Customers add their own approved product content and recorded demos. The service turns those into interactive pages that answer buyer questions with citations, and provides internal tools for RFP and security questionnaire responses, competitive material, objection handling, and deal tracking.

Entity: Ask Replay LLC · Missouri, United States · 8 Chandler Court, Saint Charles, MO

Website: https://ask-replay.com

Security contact: contact@ask-replay.com

Hosting and data location: United States

Deployment model: Multi-tenant SaaS, logically isolated per workspace

2. Where your data goes

Customer content is added

Documents, recordings, transcripts, and web pages the customer chooses. Text is extracted, split into passages, and embedded. Passage text and embeddings are stored in the vector store; source records live in the primary database.

Stored or processed by: Supabase (metadata and text), Pinecone (embeddings), AWS S3 (uploaded media, when enabled)

A buyer asks a question

The question is embedded, matched against that workspace's approved passages only, and the matched passages plus the question are sent to the model provider to compose an answer. The answer is returned with citations to those passages.

Stored or processed by: OpenAI (transient processing of the question and matched passages)

Activity is recorded

Views, questions asked, and any viewer email the customer chose to collect are stored so the customer can see engagement. Administrative actions are written to the audit log with actor and IP.

Stored or processed by: Supabase

Deletion

Deleting a source, recording, or workspace removes the database rows, the corresponding vector embeddings, and the stored objects. Deletion is not a soft flag.

Stored or processed by: All of the above

A current subprocessor list, with each provider's purpose and processing location, is published at https://ask-replay.com/subprocessors.

3. Controls in place

Access control and identity

- Sign-in with email and password, Google, or Microsoft. SAML single sign-on is available for workspaces that register their identity provider.
- Two-factor authentication (TOTP authenticator app), enforced server-side on every request rather than only at the sign-in screen. A session that has not cleared its second factor is refused by the API.
- SCIM 2.0 directory sync provisions and deactivates users from the customer's identity provider.
- Role-based access with two roles. Administrators control data export, public publishing, and permanent deletion; members do day-to-day work.
- Session tokens are signed and httpOnly, verified server-side on every request.
- Administrators can end a person's sessions immediately, or remove the account entirely. Both take effect without waiting for token expiry.
- Privileged operations run server-side under scoped service credentials; the browser never holds them.

Data protection

- Encryption in transit using TLS. Encryption at rest is provided by our infrastructure providers.
- Tenant isolation: every record is scoped to a workspace, enforced by database row-level security in addition to application checks.
- Uploaded video is stored privately and served through short-lived signed URLs, never a public object URL.
- Per-recording passwords and optional email gating on buyer-facing pages. Deal rooms are invite-only by email with one-time code verification.
- Deletion is real and complete: removing a workspace, recording, or source purges the database rows, the vector embeddings, and the stored objects.
- Optional content approval, so newly added knowledge cannot answer a buyer until a reviewer approves it.

AI and content handling

- Customer content is not used to train AI models, ours or a provider's. It is sent to the model provider only to generate a response for that request.
- Answers are generated only from content the customer has added and approved, and every buyer-facing answer carries citations to the source it came from.
- The system fails closed. When approved content cannot answer a question, the product says so and logs the gap rather than generating an unsupported answer. This is enforced in code, not by prompt instruction alone.
- Buyer-facing answers never draw on the open web. Web search is used only in internal, seller-facing drafting tools, and those drafts are reviewed by a person before use.
- Model providers are listed as subprocessors. Text sent for embedding and completion is processed under those providers' API terms, which exclude training on API data.
- Administrators control which content is available to answer, and can revoke a source at any time; retrieval reflects the change immediately.

Application security

- Rate limiting on public, authenticated, and AI endpoints, with per-workspace ceilings on model usage.
- Server-side request forgery protections on every feature that fetches a customer-supplied URL: HTTPS only, DNS resolved and checked against private address ranges, no cross-host redirects, and byte and time caps.
- Input validation on API boundaries with schema enforcement.
- Content Security Policy, clickjacking protection, strict transport security, and MIME-sniffing protection set at the edge.
- Secrets are held in the hosting provider's encrypted environment configuration and are never exposed to the browser.
- Continuous integration runs type checking, linting, and an offline grounding evaluation on every change, so a regression in the citation or abstention behavior fails the build.

Infrastructure and operations

- Hosted on Vercel (application and edge delivery) with Supabase for authentication and the primary database, both in the United States.
- A health endpoint verifies the database, vector store, model provider, and object storage.
- Application errors carry a stable fingerprint and release identifier, with throttled alerting to the operator.
- An administrative audit log records who performed each privileged action, from which IP address, with CSV export available to workspace administrators.
- Infrastructure is managed by providers who maintain their own compliance programs; we do not operate physical infrastructure.

Privacy and data rights

- A Data Processing Agreement is available and published at /dpa.
- The subprocessor list is public at /subprocessors and is updated when it changes materially.
- Buyer email capture on demos is optional and controlled by the customer.
- Customers can delete their workspace and all associated content at any time; deletion cascades to the database, vector store, and object storage.
- Personal data processed is limited to account holders (workspace users) and any viewer contact details the customer chooses to collect.

Availability and recovery

- The primary database is backed up by the provider on a daily schedule with point-in-time recovery.
- Application code is versioned and deployments are immutable, so a bad release can be rolled back to a previous deployment.
- Object storage and vector data are managed by providers with their own durability guarantees.

4. Security questionnaire responses

Prepared answers to the questions standard questionnaires ask, grouped by the domains they share, so they can be transferred into a CAIQ, SIG, VSA, or a custom format. If you send your own questionnaire we will complete it directly; we aim to return it within two business days.

Company and governance

Describe your company and the service provided.

AskReplay is a software-as-a-service workspace for sales engineering teams. Customers add their own approved product content and recorded demos; the service turns those into interactive pages that answer buyer questions with citations, and provides internal tools for RFP responses, competitive material, and deal tracking.

Do you hold SOC 2, ISO 27001, or equivalent certification?

Not at this time. The underlying controls are implemented and documented in our public trust materials, and we disclose the gap rather than imply certification. We commence a SOC 2 Type II examination when a customer agreement requires the report.

Who is responsible for security at your organization?

Security is owned by the founder, who is also the engineering lead. Security questions and incident reports go to contact@ask-replay.com.

Do you use subcontractors or subprocessors to deliver the service?

Yes. Our subprocessors are published and kept current at https://ask-replay.com/subprocessors, with each provider's purpose and processing location.

Access control

How do users authenticate?

Email and password, Google, or Microsoft sign-in. SAML single sign-on is supported for workspaces that register an identity provider. Sessions use signed, httpOnly tokens verified server-side on every request.

Is multi-factor authentication supported and can it be enforced?

Yes. Time-based one-time password (TOTP) authenticators are supported, and enforcement is server-side: once a user has a verified factor, requests presenting a session that has not satisfied that factor are refused by the API, not only by the interface.

How is user provisioning and deprovisioning handled?

Administrators can invite and remove users directly. SCIM 2.0 directory synchronization provisions and deactivates users automatically from the customer's identity provider. Administrators can also terminate a user's active sessions immediately without removing the account.

Describe your authorization model.

Two roles: administrator and member. Data export, public publishing, permanent deletion, and workspace-wide settings require the administrator role. Records are additionally scoped by ownership and coverage within a workspace.

How do you control internal (vendor) access to customer data?

Privileged operations execute server-side using scoped service credentials. Access to production data is limited to the founder for the purpose of operating and supporting the service, and administrative actions performed in-product are recorded in the customer-visible audit log.

Data protection and encryption

Is data encrypted in transit and at rest?

In transit, yes, using TLS. At rest, encryption is provided by our infrastructure providers (Supabase for the database, AWS S3 for object storage, Pinecone for vector data).

How is customer data segregated from other customers?

Logical multi-tenancy. Every record carries a workspace identifier, enforced by database row-level security policies in addition to application-layer checks. Vector queries are filtered by workspace identifier as a base condition.

What data do you collect about our end users?

Only what the customer chooses to collect. Viewer email capture on shared pages is optional and configured per workspace. Where enabled, we store the email address supplied by the viewer along with their activity on that customer's content.

What is your data retention and deletion policy?

Customer content is retained while the workspace exists. Deleting a source, recording, or workspace performs a real deletion: the database records, the corresponding vector embeddings, and the stored objects are all removed. Deletion is not a reversible soft flag.

Where is data processed and stored?

United States. Application hosting, database, vector storage, model processing, object storage, and payment processing providers are all US-based; see the subprocessor list for each.

Artificial intelligence and machine learning

Is our data used to train AI models?

No. Customer content is not used to train models, ours or a provider's. Content is transmitted to the model provider only to generate a response to a specific request, under API terms that exclude training on submitted data.

What prevents the AI from stating something inaccurate to our customers?

Buyer-facing answers are generated only from passages retrieved from content the customer has approved, and citations are bound in code to the passages actually retrieved, so a citation cannot be invented. When no approved content supports an answer, the system declines and records a content gap rather than generating an unsupported response.

Does the AI have access to the open internet when answering our buyers?

No. Buyer-facing answering has no web access. Web search is used only in internal, seller-facing drafting tools (for example competitive research), where output is explicitly a draft for human review before any use.

Which AI providers do you use, and can we review them?

OpenAI for text embedding and completion, and Pinecone for vector storage. Both are listed as subprocessors with their purpose and location.

Can we control what content the AI is permitted to use?

Yes. Content approval can be enabled so newly added knowledge cannot answer buyers until a reviewer approves it, and any source can be restricted or removed at any time, taking effect immediately.

Application and infrastructure security

Describe your secure development practices.

Changes are version controlled and deployed through an automated pipeline. Continuous integration enforces static type checking, linting, and an offline evaluation of the grounding behavior (citation and abstention), so a regression in the safety-relevant behavior fails the build before release. Deployments are immutable and can be rolled back.

How do you protect against common web vulnerabilities?

Schema validation at API boundaries, parameterized database access, Content Security Policy, strict transport security, clickjacking and MIME-sniffing protections, rate limiting on public and AI endpoints, and explicit server-side request forgery protections (HTTPS-only, DNS resolution checked against private ranges, no cross-host redirects, byte and time caps) on every feature that fetches a customer-supplied URL.

Do you perform penetration testing?

Not at this time. We disclose this rather than imply otherwise, and a test can be commissioned as a condition of a customer agreement.

How are secrets and credentials managed?

In the hosting provider’s encrypted environment configuration, scoped to the server runtime. Credentials are never delivered to the browser, and privileged database access uses a service credential available only server-side.

Do you maintain audit logs?

Yes. Privileged administrative actions are recorded with the acting user, timestamp, target, and originating IP address. Workspace administrators can view and export the log as CSV.

Incident response and continuity

Do you have an incident response process?

Yes. Application errors are captured with a stable fingerprint and release identifier and alert the operator. On confirming an incident affecting customer data or availability, we contain the issue, assess scope using application and provider logs, notify affected workspace administrators by email, and follow up with a written summary of cause and remediation.

What is your breach notification commitment?

We notify affected customers without undue delay and, where the Data Processing Agreement applies, within the timeframe it specifies, with the information available at the time of notice.

Describe your backup and recovery capability.

The primary database is backed up daily by the provider with point-in-time recovery. Application deployments are immutable and reversible. We have not yet rehearsed a full restore, so we do not publish a recovery time objective; we would rather state that precisely than publish an untested number.

What is your uptime commitment?

We do not currently offer a contractual uptime service level agreement. The service runs on managed infrastructure whose providers publish their own availability targets.

Privacy and legal

Will you sign a Data Processing Agreement?

Yes. Our DPA is published at https://ask-replay.com/dpa and is available for execution.

How do you support data subject rights requests?

Customer administrators can delete individual records, sources, and viewer data directly in the product, and can delete the entire workspace. For requests requiring our assistance, contact contact@ask-replay.com.

Do you sell personal data?

No.

How will you notify us of changes to subprocessors?

The subprocessor list is public and updated when it changes materially. Customers can request notification of changes by contacting us.

5. Commercial and procurement

- Ordering: self-serve checkout with an itemized invoice suitable for expense reporting, or an annual invoice on request.
- Payment: major credit cards through our payment processor. Annual invoicing is available.
- Contract: click-through terms of service and, where required, our Data Processing Agreement. We can review a customer paper agreement, with the understanding that turnaround depends on scope.
- Tax documentation: a completed W-9 is furnished on request.
- Renewal: annual plans renew at the end of the term; cancellation before renewal is available in the billing settings.
- Security contact: contact@ask-replay.com. We aim to return completed security questionnaires within two business days.

Questions, or a document not covered here? Contact contact@ask-replay.com. The current version of this package is always at https://ask-replay.com/trust.