aijency.

Security White Paper

How Aijency protects the data its AI agent handles on your website. Written for security reviewers, procurement teams and anyone completing a vendor assessment.

VERSION
1.0

PUBLISHED
7 August 2026

CLASSIFICATION
Public

ABN
27 129 394 163

Document control

Document owner	Aijency, security@aijency.ai
Version	1.0, published 7 August 2026
Next scheduled review	7 February 2027, or on any material change to our controls
Classification	Public. May be shared freely.
Supersedes	No previous version. This is the first issue.

Contents

1. What Aijent is 3
2. What data we collect 3
3. Where data lives 3
4. Encryption 3
5. Tenant isolation 3
6. AI processing 3
7. Payments 4
8. Application and infrastructure security 4
9. Sub-processors 4
10. Retention and deletion 5
11. Incident response 5
12. Privacy frameworks 6
13. Certification status 6
14. Contact 6

A note on how this document is written. Where a control has a limit, this document states the limit rather than the headline. Several statements below are deliberately narrower than the version a reader might expect, because the narrower one is the one that is true.

1. What Aijent is

Aijent is an AI agent that runs on your website. It answers visitor questions from the knowledge you give it, qualifies enquiries, and depending on your product either books a meeting into your calendar and writes the result to your CRM, or captures the enquiry and hands it to a person. It is embedded with a single script tag and requires no access to your systems beyond the integrations you explicitly connect.

2. What data we collect

Aijent collects only what a visitor voluntarily provides in conversation: typically their name, email address, company, phone number, the needs they describe, and the transcript of the conversation itself.

Two pieces of context arrive automatically. The visitor's time zone, from their browser, so meeting times are offered in local time. And the address of the page the widget is on, so the correct Aijent answers.

What we do not collect. No browsing history, no device fingerprinting and no passive tracking. We do not store IP addresses, user agents or referrers. The widget keeps three values in the visitor's browser: a random identifier for session continuity, a copy of it set by the embed script, and a timestamp of the last engagement so the same person is not prompted repeatedly. None is used for cross-site tracking.

3. Where data lives

Customer and visitor data is stored in **Sydney, Australia**, on managed PostgreSQL in the ap-southeast-2 region, encrypted at rest. Application compute is pinned to the same Sydney region.

Some sub-processors in section 9 process data in the United States, and section 9 states exactly which data reaches each one. Australian data residency describes where your data is *stored*. It does not mean no data ever leaves the country in transit to a named sub-processor.

4. Encryption

In transit. TLS on all connections, with HTTPS enforced.

At rest. AES-256 on the managed database.

Integration credentials. OAuth tokens for your CRM, calendar and video providers are encrypted separately with AES-256-GCM before being written, and decrypted server-side only at the point of use. They are never exposed to the browser.

Key management. The data-encryption key and all application secrets are held in a dedicated, access-controlled secrets manager, kept out of source control and governed by a documented key-management policy.

5. Tenant isolation

Every table carries a tenant identifier, and isolation is enforced by row-level security in the database itself rather than by application code remembering to filter. A query issued on behalf of one customer cannot return another customer's rows even if the application layer above it is wrong.

6. AI processing

Aijent's replies are generated by Anthropic's Claude API. Three things are true about that relationship, stated precisely because this is the area reviewers probe hardest.

No model training. Anthropic does not use API inputs or outputs to train models. This is a contractual obligation under their Commercial Terms and Data Processing Addendum, not a setting.

Retention is governed by their published terms, not by a zero-data-retention arrangement. We do not claim Anthropic retains nothing, because that is not the arrangement in place.

Prompt caching is used deliberately. Your Aijent's instructions and relevant knowledge base content are cached for up to one hour to make replies faster and cheaper. A design decision, disclosed here rather than omitted.

Anthropic independently holds SOC 2 Type II, ISO/IEC 27001:2022 and ISO/IEC 42001:2023, verifiable at trust.anthropic.com. Those are Anthropic's certifications, not Aijency's.

7. Payments

Card payments are handled entirely by Stripe. Checkout and billing management run on Stripe-hosted pages, and there is no card field, card element or card-handling code anywhere in the Aijency application. No card number, expiry or security code is ever stored, transmitted or logged by us. Stripe is certified as a PCI DSS Level 1 service provider.

8. Application and infrastructure security

Static analysis and secret scanning run automatically on everything merged to our main branch, plus a scheduled weekly sweep. These are detective controls reviewed by us; they do not block a build.

OAuth 2.0 with PKCE wherever the provider supports it. Some do not. Slack is one, and its integration uses OAuth 2.0 with a state-nonce CSRF guard instead.

We never hold your provider passwords. Every integration is authorised by you inside that provider, and we hold only a revocable token.

Two-factor authentication protects account login.

Append-only audit logging of security-relevant events. Records cannot be modified or deleted through the application. They are removed when a customer's account is deleted.

Continuous error monitoring across all environments, plus uptime monitoring with alerting and a public status page.

9. Sub-processors

The companies below process personal data on Aijency's behalf. Each entry states what actually reaches that company, because a register that says "processes data on our behalf" tells a reviewer nothing. This table and the published register at aijency.ai/legal/sub-processors render from one source, so they cannot disagree. We review a sub-processor before engaging it.

SUB-PROCESSOR	PURPOSE	LOCATION	PERSONAL DATA IT RECEIVES
Anthropic	Generates your Aijent's replies	United States	The conversation so far, your knowledge base content, and the free meeting times read from your calendar
Voyage AI	Finds the right passage of your knowledge base to answer a question	United States	The visitor's question, on every turn where knowledge is used, and your knowledge base content when it is first indexed

SUB-PROCESSOR	PURPOSE	LOCATION	PERSONAL DATA IT RECEIVES
Kickbox	Checks an email address is real before a booking is made	United States	The visitor's email address
Firecrawl	Reads your website so your Aijent can answer from it	United States	Whatever is published on the pages of your website we read
Supabase	Stores your data	Australia, ap-southeast-2 Sydney	All lead details and full conversation transcripts
Vercel	Runs the application	Australia, ap-southeast-2 Sydney for compute	Handled in passing while a request runs, never stored here
Stripe	Takes subscription payments	United States	Your billing details. No website visitor data ever reaches Stripe
Resend	Sends email	United States	Recipient addresses, and the full conversation transcript attached to an escalation email
Sentry	Reports application errors so we can fix them	United States	Diagnostic data only. Personal data is stripped before sending and session recording is off
PostHog	Product analytics for the customer dashboard	United States	The identity of signed-in customer staff. Website visitors are never sent to PostHog
OpenAI	Standby only for Aijent replies	United States	Nothing today. If ever switched on it would receive what Anthropic receives

10. Retention and deletion

> **Customer data is retained for 30 days after an account is deleted, then removed.**

The 30 day window exists so an accidental deletion can be recovered. After it, the data is gone, including the audit records described in section 8.

Conversation history visible in the product is subject to your plan’s analytics retention period. That is a separate matter from the deletion policy above and is stated on our pricing page.

11. Incident response

> **We will notify affected customers within 72 hours of becoming aware of a personal data breach.**

Notification describes what happened, what data was involved, what we have done, and what you may need to do. This is a commitment. It aligns with the notification window in the GDPR and with the Notifiable Data Breaches scheme under the Australian Privacy Act.

Vulnerabilities can be reported to security@aijency.ai. We acknowledge every report, keep the reporter updated while we investigate, and will not pursue action against anyone who reports a genuine issue in good faith. Our contact record is published at aijency.ai/.well-known/security.txt per RFC 9116.

12. Privacy frameworks

Australian Privacy Act 1988. Our primary governing framework.

GDPR (EU and UK). Standard Contractual Clauses are in place through our providers, including a Data Processing Addendum with Anthropic that incorporates SCCs.

PDPA (Singapore). Supported through our contractual chain.

13. Certification status

Aijency does not currently hold a SOC 2 report. Our SOC 2 Type I audit is underway with Ken & Co, with the Type II audit expected approximately three months after Type I completes. Each report will be published when it is issued.

We display no certification badge we have not been awarded, and we do not present a provider's certification as our own. Where a certification belongs to a company we rely on, this document names that company.

14. Contact

Security questions, procurement questionnaires and Data Processing Agreements: **info@aijency.ai**

Vulnerability reports: **security@aijency.ai**

Arch Aijency, ABN 27 129 394 163. This document is version 1.0, published 7 August 2026. Next scheduled review 7 February 2027.