nonimo

SECURITY WHITE PAPER

Nonimo Gateway security: a white paper for privacy officers

The answers an Australian privacy officer needs before AI tools touch client or patient information: where the text goes, who can read it, what is kept and what evidence stays with you.

Nonimo team

November 2026

nonimo.com.au

SECURITY WHITE PAPER

Nonimo Gateway security: a white paper for privacy officers

The answers an Australian privacy officer needs before AI tools touch client or patient information: where the text goes, who can read it, what is kept and what evidence stays with you.

Nonimo team · November 2026 · 15-minute read

What's inside

- A one-page summary built around the questions a privacy officer asks first
- The path a request takes, from your application to your AI provider and back
- Your own isolated environment in Sydney, and the guarantees that come with it
- What is stored, where, and the four moments it is deleted
- Who is who: your organisation, Nonimo, Microsoft Azure, your AI provider
- How the Gateway lines up with APP 6, APP 8, s 16C, APP 11 and the NDB scheme
- Twelve questions your privacy officer can put to us, with short answers

In short

- Your Gateway runs in an isolated environment in Microsoft Azure's Australia East region (Sydney), dedicated to your organisation.
- Personal information the Gateway detects is replaced with labels before a request reaches your AI provider, and the reply comes back with the real details.
- Nonimo receives figures only: request counts, counts of redacted items and licence renewal. The text makes its trip and moves on.
- A signed monthly report and a per-request log give your privacy officer evidence for APP 1, APP 11 and privacy impact assessments, with no personal information inside.

In many Australian firms and health providers, whether staff use AI is no longer the privacy officer's call. The partners or the board have often settled that. What lands on the privacy officer's desk is narrower and harder: when our software sends client or participant information to an AI provider, what exactly leaves the building, who can read it on the way, and how do we show we took reasonable steps?

This paper answers those questions for Nonimo Gateway, hosted in Sydney. It covers what the Gateway does and what we guarantee around it. It is written so you can lift sections straight into a privacy impact assessment or an AI use policy.

01

The one-page summary for your privacy officer

The table below is the short version. Each row is a question a privacy officer working under the Privacy Act 1988 (Cth) [1] tends to ask first, with the answer and the principle it speaks to.

The question	The answer	Where it matters
Where is the text handled?	In Sydney, in an isolated environment in Microsoft Azure's Australia East region, dedicated to your organisation	APP 8, APP 11
Who can read it there?	Your Gateway, while it works. What it processes is not read by Nonimo or Microsoft staff	APP 11
What does the AI provider get?	The request, with labels such as `[PERSON_1]` standing in for the personal information found	APP 6, APP 8, s 16C
What does Nonimo receive?	Figures only: totals of requests and of redacted items, plus licence renewal	APP 6
What is stored?	Three things: your settings, the key to your AI provider account and any terms you add, all kept in Australia East	APP 11
When is it deleted?	During the trial, after three idle days in a row (we warn you the day before); when a trial finishes with no plan chosen; when a subscription finishes; or on request	APP 11
What evidence do we keep?	A signed monthly report and a per-request log, both made of counts and metadata	APP 1, PIAs
What paperwork is available?	The data processing terms, on request at support@nonimo.ai	APP 1

The rest of the paper explains each row.

02

The path a request takes

The Gateway sits between your organisation's applications and the AI provider you have chosen. Your developers swap the provider's address in the application for your Gateway's, and use your Gateway's access key. Everything else in the code stays as it is: the official SDK, the models, the messages, the logic. The Gateway speaks the APIs your applications already use, those of OpenAI (chat completions and responses) and Anthropic (messages). It works with the AI provider you choose, for example OpenAI or Claude.

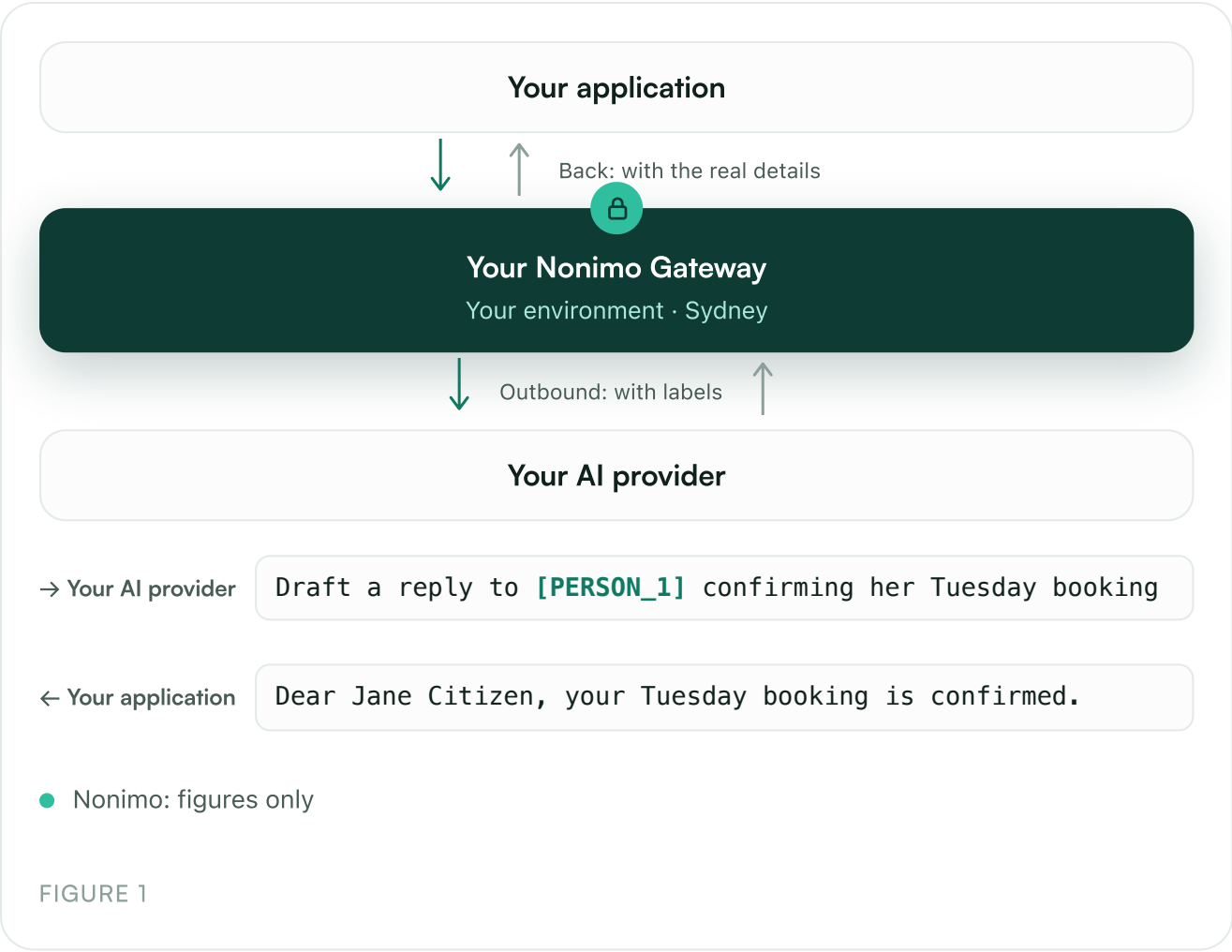

FIGURE 1

When a request arrives, the Gateway detects the personal information in it (names of people and organisations, identity document numbers, bank account details, email addresses and phone numbers) and swaps each one for a label. The request then goes to your AI provider, using your organisation's own key with that provider.

Take a practice manager at a fictional allied health clinic who uses an internal tool to draft patient messages. The tool sends `Draft a reply to Jane Citizen confirming her Tuesday booking`. What the AI provider receives is `Draft a reply to [PERSON_1] confirming her Tuesday booking`. The provider writes its reply around the label. On the way back, the Gateway puts each real detail in its place, so the practice manager reads `Dear Jane Citizen, your Tuesday booking is confirmed.` Staff read and write normal text throughout.

This restoration also happens when the reply is streamed in pieces and when the model calls tools, which is how many AI features are built today.

You set the policy for each type of personal information. For any type, the Gateway can redact it, block the request altogether, or allow it and log that it was seen. A health provider might stop any request carrying a government identifier while redacting names; a law firm might redact everything and simply watch the counts. You can also add your own terms, such as matter names, project codenames or key client names, and they are treated like any other personal information.

Throughout, Nonimo itself receives figures only: how many requests passed and how many items were redacted. The text goes through your Gateway in Sydney on its way to your AI provider, and comes back the same way. It never passes through Cloudflare, which only runs the DNS for your Gateway's address.

03

Where your Gateway runs

Each nonimo.com.au customer has its own isolated environment in Microsoft Azure's Australia East region (Sydney), dedicated to that customer. Your text is processed in Australia.

Three guarantees come with it. Only published releases of the Gateway run there, so what handles your text is a release we have published. What the Gateway processes is not read by Nonimo staff or by Microsoft staff. And Nonimo receives figures only, not your real details.

A dedicated environment gives the question ‘who else shares this?’ a clean answer. Your Gateway serves your organisation. Its address, its keys and its stored settings belong to your deployment.

> **Note:** For many Australian organisations, the deciding point is that the text is handled onshore, in Sydney. The AI provider you choose is a separate decision, covered under APP 8 below.

04

What is kept, and when it is deleted

The Gateway keeps a small amount of configuration so it can do its job: your settings (including the policy for each type of personal information), your AI provider key and the terms you have added. All three stay in Australia East, and a new release does not ask you to set everything up again.

Request and reply text gets different treatment. It passes through your Gateway while the request is handled, and then moves on.

A Gateway has a clear life cycle, and deletion is built into it.

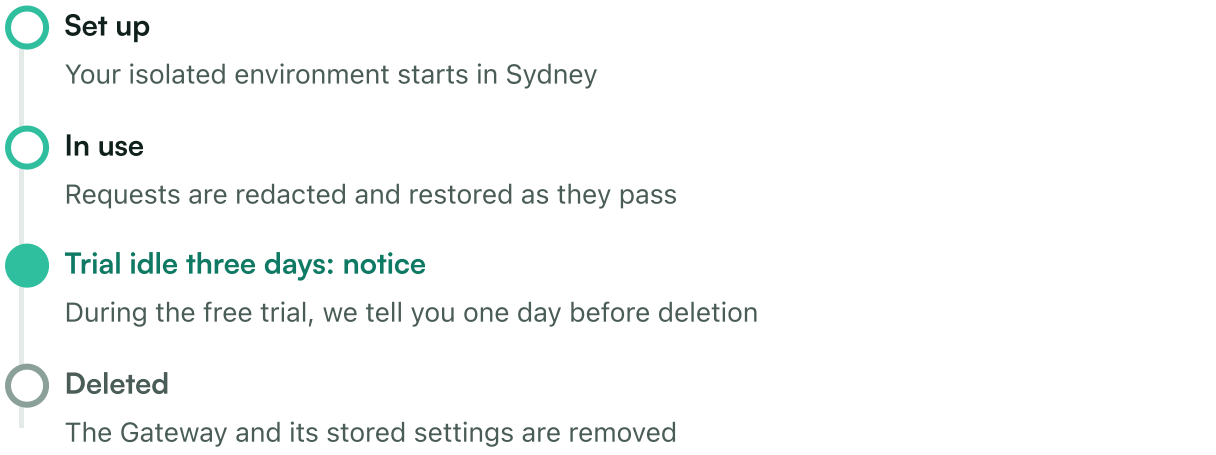

FIGURE 2

The Gateway and what it stores are deleted in four situations:

1. **During the free trial, after three days in a row without use.** We send a notice one day before, so an unused trial does not quietly linger. A paid Gateway isn't removed for being idle.
2. **When a trial ends without a plan.**
3. **When a subscription ends.**
4. **When you ask.** Your privacy officer can request deletion at any time.

APP 11 also asks organisations to destroy or de-identify personal information they no longer need. The Gateway's approach keeps that obligation small: the text passes through, and the configuration has defined end points.

05

Access and keys

Connections to your Gateway use HTTPS. Your Gateway has its own address and its own access key, which your applications use. The key for your AI provider is one you paste into your Gateway's page yourself, so the commercial and technical relationship with the provider stays with your organisation. The panel, where you set policy and read reports, has its own key, separate from the one your applications use. That separation lets you give the IT lead application access and the privacy officer panel access without either holding the other's key.

For teams whose developers use AI coding assistants such as Claude Code or Cursor, there is a local MCP connector that runs on the developer's machine. With it, the assistant can check your Gateway's status, store the keys in the project's `.env` file after the developer says yes, locate the calls to your AI provider in the code and suggest the edit, try the Gateway with invented data, and download the privacy officer's report. The keys are saved on your developer's machine and in your Gateway.

06

Who is who

Australian privacy law does not use the European split between controllers and processors. Under the Privacy Act, the organisation that collects and holds personal information stays accountable for it, including when a service provider handles it on its behalf. The table and diagram below set out the parties in those terms.

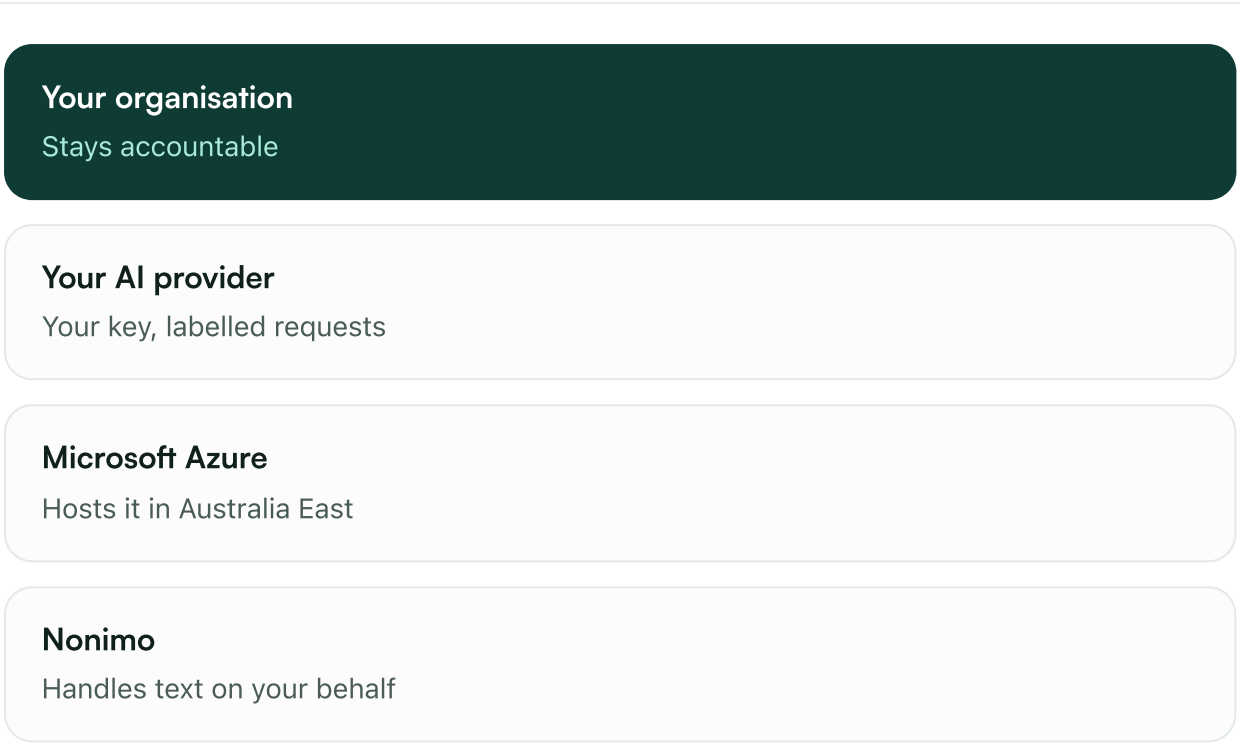

FIGURE 3

Party	Role	What it touches
Your organisation	The accountable organisation under the Privacy Act	Everything: you decide what is sent, to which provider, and the policy for each type of information
Nonimo	A service provider handling the text on your behalf	The text passes through your Gateway; Nonimo receives figures only
Microsoft Azure	Hosts your isolated environment in Australia East (Sydney)	Provides the infrastructure; its staff do not read what your Gateway processes
Your AI provider	Contracted by you, with your own key	Receives requests with labels in place of detected personal information
Cloudflare	A service provider to Nonimo: runs the DNS for your Gateway's address	Prompts and replies never pass through it
Paddle	Authorised reseller (merchant of record) that takes payment	Holds purchase details in its own right

Readers used to GDPR documents will recognise Nonimo's position as roughly what Europe calls a processor. In Australian terms, the useful sentence for your policy is this: Nonimo handles the text on your behalf, and your organisation stays accountable.

07

Reading the Gateway against the Privacy Act

This section walks through the provisions a privacy officer will raise, in the order they usually come up. It is general information to support your own assessment, not legal advice.

APP 1: open and transparent management

APP 1 expects you to have practices, procedures and systems that ensure compliance, and a clearly expressed privacy policy. An AI tool that your staff use daily belongs in that picture. The Gateway gives you something concrete to describe: a defined path for the text, a stated location, documented roles and a report you can produce on request. The data processing terms are available at support@nonimo.ai for your records.

APP 6: use and disclosure

Sending client or patient information to an AI provider will in most cases be a disclosure, and APP 6 limits disclosure to the primary purpose of collection or a permitted secondary purpose. The Gateway works on the size of that disclosure. With names, identity numbers, bank details and contact details replaced by labels, what goes to the provider is the task and its context. Your privacy officer still makes the call on whether a given use is within purpose. The Gateway narrows what is disclosed while that call is made.

APP 8 and section 16C: cross-border disclosure

This is where many assessments slow down. Your AI provider may well process requests outside Australia. Under APP 8, before disclosing personal information to an overseas recipient you must take reasonable steps to ensure the recipient does not breach the APPs, and under section 16C your organisation can be held accountable if that recipient handles it in a way that would breach them.

The Gateway changes the facts that feed this analysis in two ways. First, the handling of your text before it leaves happens in Sydney. Second, what crosses the border to the provider carries labels in place of the personal information the Gateway detects. Whether labelled text remains personal information in the provider's hands is a question your privacy officer assesses in context, since your organisation can always re-link the labels to the people they stand for. Either way, the Gateway reduces both the amount and the sensitivity of what crosses, and that is the kind of step an APP 8 assessment weighs.

APP 11: security of personal information

APP 11 requires reasonable steps to protect personal information from misuse, interference, loss and unauthorised access. Since the 2024 amendments, APP 11.3 states expressly that reasonable steps include technical and organisational measures. The Gateway is a technical measure you can name: redaction before disclosure, an isolated environment in Australia East dedicated to you, no real details sent to Nonimo, settings kept in Australia East, separate keys for applications and the panel, and defined deletion. Your AI use policy and staff training are the organisational measures that sit beside it.

The Notifiable Data Breaches scheme (Part IIIC)

When an incident is assessed under the NDB scheme, the first thing anyone asks is what information was involved. The per-request log answers that for AI traffic: for each request, when it was sent, to which provider and model, and how many items of each type were redacted. Because the provider received labels, your assessment starts from a precise picture of what left.

The OAIC's guidance on commercially available AI

In October 2024 the OAIC published guidance on privacy and the use of commercially available AI products [2]. It recommends, as a matter of best practice, that organisations avoid entering personal information, particularly sensitive information, into publicly available AI tools, and it makes clear that Privacy Act obligations apply to what is entered. For health and NDIS providers, whose records are full of health information, that recommendation carries extra weight. The Gateway applies that advice to the request itself, before it reaches the tool.

The Privacy and Other Legislation Amendment Act 2024

The 2024 amending Act [3] brought two changes worth noting here. A statutory tort for serious invasions of privacy has applied since 10 June 2025, which raises the stakes on how personal information moves. And from 10 December 2026, privacy policies must explain when personal information is used in automated decisions that significantly affect individuals. If AI plays a part in such decisions at your organisation, the Gateway's log tells you which providers and models were used and when, which helps you write that part of the policy accurately.

08

The evidence that stays with you

The Gateway produces two kinds of evidence for your records, and neither contains personal information.

The monthly report lives in the panel and is written for the privacy officer. It is signed, it shows how many items of personal information were redacted and of which type, as figures only, and it records the version of the Gateway that ran. A fictional month might read: November, 9,317 items redacted, made up of people 4,108, organisations 1,256, identity documents and bank account details 2,836, and email addresses and phone numbers 1,117.

The per-request log notes, for every request, when it happened, which provider and model it went to, and how many items of each type were redacted. It exports to CSV or JSONL. It holds counts and metadata only, so you can hand it to an auditor without exposing anyone's details.

Together, these support:

- your APP 1 documentation and your register of AI tools in use;
- a privacy impact assessment for a new AI feature, with real volumes instead of estimates;
- an answer to a client, a funder or an auditor who asks how you handle their information with AI;
- the NDB assessment described above, should one ever be needed.

> **Note:** A professional services firm can attach the monthly report to its annual privacy review, and an NDIS provider can file it with its information management records.

09

Questions your privacy officer can ask us

Short answers to twelve questions a privacy review will usually raise. Any of them can be followed up at support@nonimo.ai.

1. **Where is our text processed?** In Sydney, in an isolated environment in Microsoft Azure's Australia East region, dedicated to your organisation.
2. **Can anyone at Nonimo read our requests?** No. What your Gateway processes is not read by Nonimo or Microsoft staff, and only published releases of the Gateway run in your environment.
3. **What does Nonimo get?** Numbers only: how many requests, how many items redacted, and the licence renewal.
4. **And the AI provider?** The request with labels standing in for any personal information found, sent under your own key.
5. **Do our staff see labels?** They see normal text. The reply returns with the real details, streamed replies and tool calls included.
6. **Can we set rules per type of information?** Yes. Each type can be redacted, can block the request, or can be allowed through and logged.
7. **Can we protect our own sensitive terms?** Yes. Add matter names, project codenames or client names in the panel and they are redacted too.
8. **What does the Gateway keep, and where?** Your settings, AI provider key and added terms, in Australia East. Nonimo receives figures only, not your real details.
9. **When is everything deleted?** When a trial Gateway sits unused for three days in a row (we warn you the day before), when a trial finishes without a plan, when a subscription finishes, or whenever you ask. A paid Gateway stays in place while it's idle.
10. **What evidence do we get?** A signed monthly report for the privacy officer, which also records the Gateway version that ran, plus a per-request log you can export as CSV or JSONL; both hold counts and metadata only.
11. **Who are the parties, in Privacy Act terms?** Your organisation stays accountable; Nonimo handles the text on your behalf; Microsoft Azure hosts your environment; your AI provider is contracted by you.
12. **Can we see the data processing terms?** Yes. Ask at support@nonimo.ai.

For how the wider protections fit together, see Security. For plans, see Pricing, and for practical walkthroughs on AI and privacy, our Guides.

10

Sources

1. Privacy Act 1988 (Cth), including Schedule 1 (Australian Privacy Principles), section 16C and Part IIIC — https://www.legislation.gov.au/C2004A03712/latest
2. OAIC, Guidance on privacy and the use of commercially available AI products (21 October 2024) — https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products
3. Privacy and Other Legislation Amendment Act 2024 (Cth) — https://www.legislation.gov.au/C2024A00128/latest