nonimo

SECURITY WHITE PAPER

Nonimo Gateway security: a white paper for your DPO

What happens to personal data when your applications call an AI model through Nonimo Gateway, set out article by article for UK and Irish organisations.

The Nonimo team

November 2026

nonimo.eu

SECURITY WHITE PAPER

Nonimo Gateway security: a white paper for your DPO

What happens to personal data when your applications call an AI model through Nonimo Gateway, set out article by article for UK and Irish organisations.

The Nonimo team · November 2026 · 14-minute read

What's inside

- A one-page summary your DPO can file with the DPIA
- The journey of a request, from your application to the AI provider and back
- Your own confidential machine in Ireland, and the guarantees that come with it
- What is stored, how it is protected, and who holds each key
- Controller, processor, sub-processor: a table of who does what
- UK GDPR, the Irish Data Protection Act 2018 and the articles that apply
- The monthly DPO report, the per-request log, and twelve questions answered

In short

- Each customer gets a confidential Microsoft Azure machine of their own in Ireland, and what it processes is not read by Nonimo or Microsoft staff.
- Personal data are replaced with labels before a request leaves for your AI provider, and the real data are put back in the reply, streaming included.
- Nonimo receives figures only: how many requests and how many items were redacted. The text makes its journey and does not stay.
- Your DPO gets a monthly report and a per-request log in CSV or JSONL that hold counts by type of data and never the data themselves.

Plenty of organisations in the UK and Ireland now run an internal application that sends text to a large language model: a tool that drafts client letters, a service desk that summarises tickets, a script that classifies complaints.

Each of those calls carries whatever the user typed, and that is often a name, a company, an account number or an email address. This paper explains, in the terms your data protection officer will use, what Nonimo Gateway does with that text, where it does it and what evidence it leaves behind.

It is written for the people who sign off a deployment: the DPO who updates the record of processing and the DPIA, the head of IT who wires the Gateway in, and the in-house lawyer who reviews the processing agreement. It describes what the Gateway does and the guarantees that come with it.

For the commercial terms, see our plans; for the wider security overview, see Security.

01

A one-page summary for your DPO

If your DPO reads only one section, it should be this one. Everything below it expands on a line of this table.

Question	Answer
Where is the text processed?	On a confidential Microsoft Azure machine that runs for your organisation alone, in Ireland, inside the EU.
Who can read it while it is processed?	Your applications and your Gateway. The machine's memory is encrypted by the processor, and what it handles is not read by Nonimo staff or Microsoft staff.
What reaches the AI provider?	The request with personal data replaced by labels such as `[PERSON_1]` or `[EMAIL_1]`, sent with your own key to the provider you chose.
What comes back to your users?	The provider's reply with each real item put back in its place, including streamed replies and tool calls.
What does Nonimo receive?	Figures: the number of requests and the number of items redacted, plus the licence renewal.
What is stored?	Your settings, your AI provider key and the terms you add yourself, encrypted, in the same region, readable only by your machine.
When is it erased?	With the Gateway: after three consecutive days without use during a trial (with notice a day before), at the end of a trial without a plan, at the end of a subscription, or when you ask.
What documents do you keep?	A monthly report for the DPO and a per-request log in CSV or JSONL. Both hold counts by type of data and never the data.
Our role	Processor, acting on your instructions for the text that passes through the hosted Gateway.
The processing agreement	Ask for it at hello@nonimo.ai.

You also decide, for each type of data, what the Gateway does when it finds it: redact it, stop the request, or let it through and record a warning with the count. That choice is yours and it sits in your Gateway's settings.

02

The journey of a request

The Gateway sits between your applications and the AI provider. Your developers point their existing code at your Gateway's address instead of the provider's, and change the key. The official SDKs, the models, the prompts and the application logic stay as they are.

The Gateway speaks the OpenAI API (chat completions and responses) and the Anthropic API (messages), so it works with providers such as OpenAI and Claude from Anthropic.

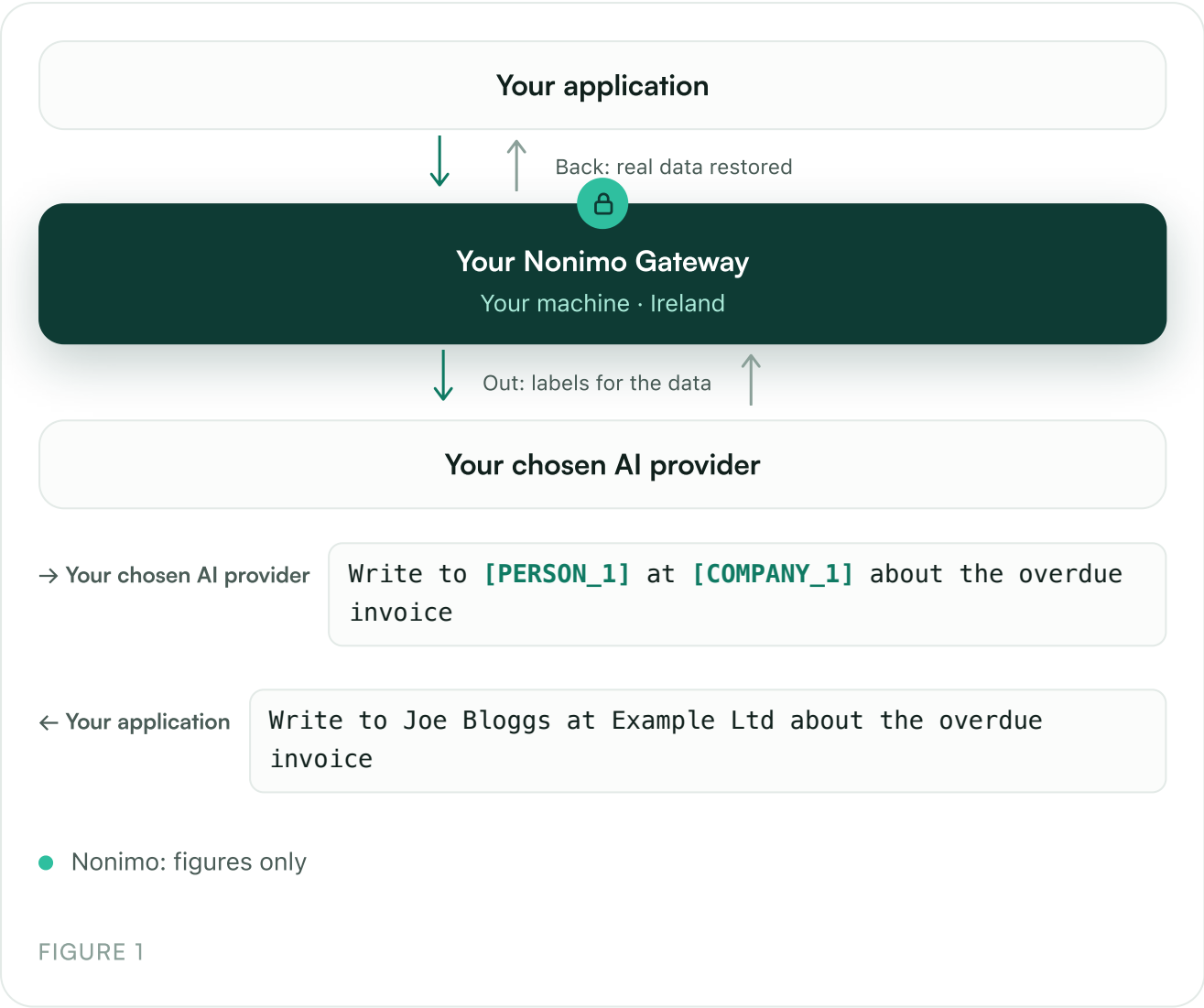

FIGURE 1

A request travels like this.

1. A user in one of your applications writes something that contains personal data. Take a credit controller who types: `Write to Joe Bloggs at Example Ltd about the overdue invoice`.
2. The application sends the request over HTTPS to your Gateway, using your Gateway's own address and access key.
3. Your Gateway detects the personal data (names, companies, identity documents, bank accounts and contact details) and replaces each item with a label. What leaves for the provider reads `Write to [PERSON_1] at [COMPANY_1] about the overdue invoice`.
4. The provider you chose, under your own contract and with your own key, writes its answer using the labels.
5. When the reply arrives, your Gateway puts each real item back where its label was. The credit controller reads a normal letter addressed to Joe Bloggs at Example Ltd. This also happens when the provider streams its answer piece by piece and when the model calls one of your tools.

Labels stay consistent across a conversation, so `[PERSON_1]` refers to the same person from the first message to the last and the model's reasoning holds together.

Alongside the request, Nonimo receives a count: one request, two items redacted. That count and the licence renewal are all that reach us. The text itself makes the journey from your application to your confidential machine, on to the provider and back, and does not stay.

> **Note:** your organisation can also add its own terms in the Gateway's dashboard, such as project code names or the names of key clients. The Gateway redacts them in the same way as any other personal data and restores them in the reply.

03

Where your Gateway runs

Each customer has their own Gateway on their own confidential machine. Your requests are processed apart from every other customer's. For customers of nonimo.eu, in the UK and Ireland alike, that machine runs in Microsoft Azure's Ireland region, inside the European Union.

The machine is a confidential container on Azure, built on AMD SEV-SNP. This is public Microsoft technology, documented on Microsoft's own site [7]: the processor encrypts the machine's memory while it works, so what is held in memory stays encrypted from the system that hosts the machine.

Two guarantees follow from it, and they are the ones your DPO will want written down.

- Only published versions of the Gateway start. The machine runs a released version of the Gateway and nothing else.
- What the machine processes is not read by Nonimo staff or Microsoft staff. The text, the labels and the replies are held in encrypted memory for as long as the request is in flight.

For a DPIA, this answers the question of who, beyond your own people, could see the content. The answer is: the AI provider you already contract with, and it receives labels where the personal data were.

04

What is stored, and who holds the keys

Some information has to persist so that your Gateway keeps working after a restart or an update. It comes down to three things:

- your settings, including what to do with each type of data;
- the key for your AI provider;
- the terms you have added yourself.

These are stored encrypted, in the same region as your machine. Only your machine, running a published version of the Gateway, can decrypt them, and they survive restarts and updates.

The text of requests and replies is not part of this list: it passes through and is gone when the request ends. The table that links each placeholder to its real value lives in memory for the length of the request and is never written to disk.

Access and keys

Three keys exist, each with a single job.

Key	Who holds it	What it opens
Gateway access key	Your applications	Sending requests to your Gateway's own address, over HTTPS
Dashboard key	The people who manage the Gateway	The dashboard, the monthly report and the per-request log
AI provider key	Your organisation, pasted into your Gateway's own page	Your account with the AI provider

The dashboard key is separate from the access key, so the developers who connect an application and the people who read the DPO report can be different people with different credentials. Your AI provider key is pasted by you into the page of your own Gateway and stays there, encrypted.

Coding assistants

Many teams now let an AI coding assistant (Claude Code, Cursor and similar tools) do the wiring. Nonimo provides a local connector for these assistants that runs on the developer's own computer.

Through it, the assistant can check the Gateway's status, save the keys in the project's environment file once the developer confirms, find where the code calls the AI provider and propose the change, run a test with made-up data and download the DPO report.

The keys travel from your developer's machine straight to your Gateway, without passing through Nonimo.

05

When a Gateway is erased

A Gateway and everything stored with it are erased in four situations: after three consecutive days without use during a trial, at the end of a trial that does not continue into a plan, at the end of a subscription, and whenever you ask.

For the first case we send notice one day before, so a Gateway that is still wanted can be kept simply by using it.

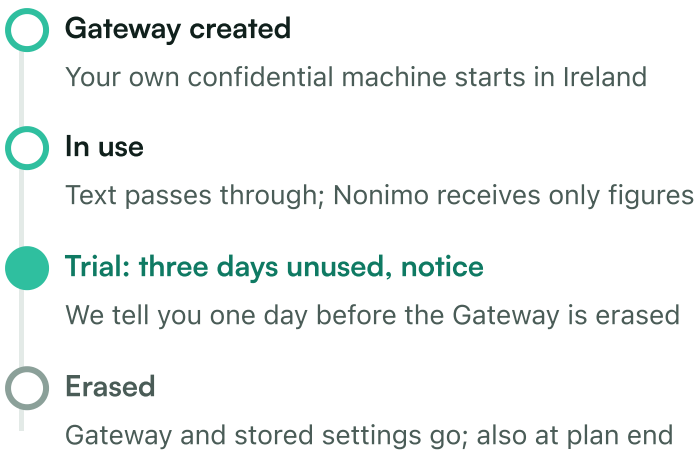

FIGURE 2

This gives your record of processing a clear retention line. The content of requests is held only for the life of each request. The settings, provider key and added terms are held for the life of the Gateway, and go with it.

06

Who is who

Data protection law asks you to name each party and its role. For the hosted Gateway, the arrangement is as follows.

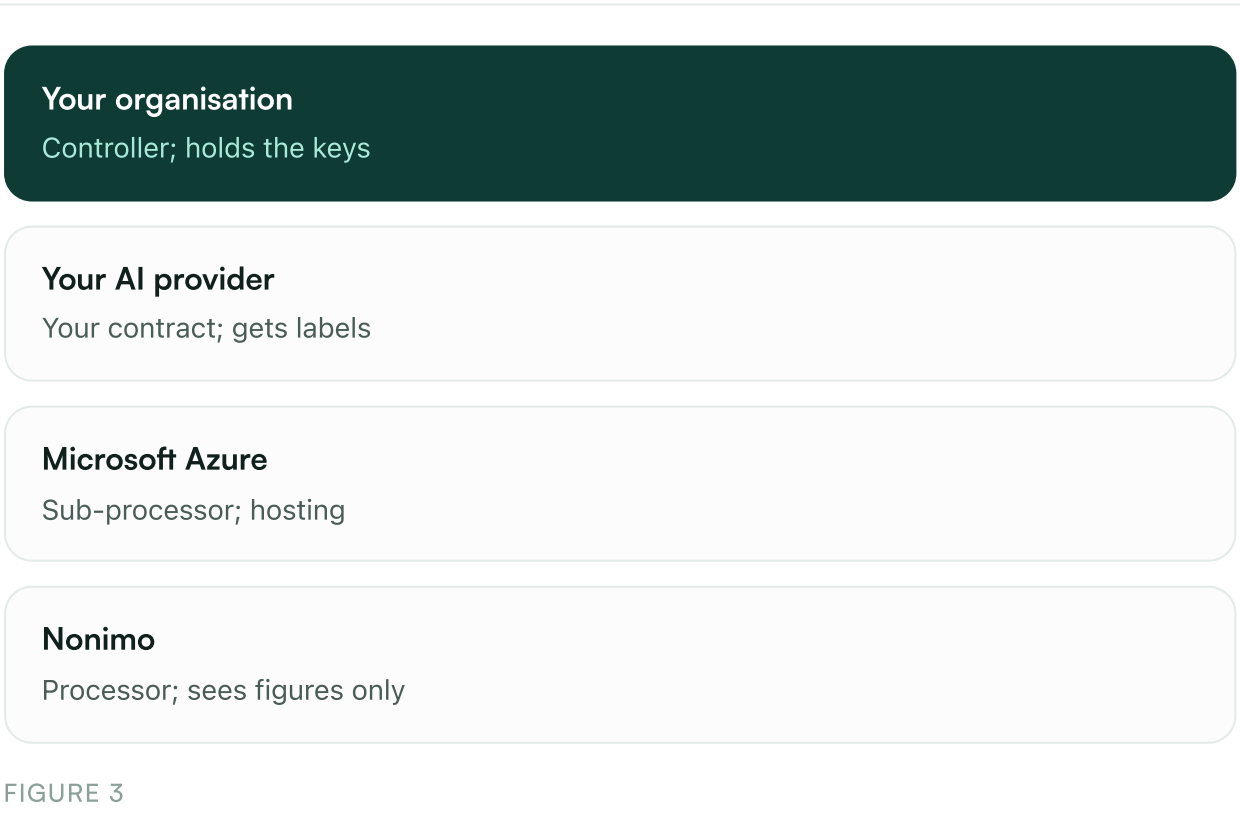

FIGURE 3

Party	Role	What it does
Your organisation	Controller	Decides the purposes, the applications and the AI provider, and holds the keys
Nonimo	Processor	Handles the text on your behalf in your Gateway, under a processing agreement
Microsoft Azure	Sub-processor	Hosts the confidential machine in Ireland
Your AI provider	Under your own contract	Receives the request with labels in place of the personal data, and replies
Cloudflare	Service provider to Nonimo	Handles licences and counts; it plays no part in handling the text and is not a sub-processor
Paddle	Authorised reseller (merchant of record)	Takes payment and acts as independent controller of the purchase data

A word on the AI provider. You chose it, you hold the account and you agreed its terms, and that relationship stays as it is. What the Gateway changes is the content the provider receives: labels in place of the personal data you decided to redact.

07

The legal frame in the UK and Ireland

Irish organisations apply the GDPR directly, together with the Data Protection Act 2018 and the supervision of the Data Protection Commission [3][4]. UK organisations apply the UK GDPR [2] alongside the UK's Data Protection Act 2018 [9], supervised by the Information Commissioner's Office [5].

The UK GDPR keeps the GDPR's article numbering, so the references below work on both sides of the Irish Sea. The table maps each obligation to what the Gateway gives you.

Provision	What it asks	How the Gateway helps
Art. 5(1)(c), data minimisation	Personal data adequate, relevant and limited to what is necessary	The provider receives labels where names, companies, documents, accounts and contacts were
Art. 25, data protection by design and by default	Technical measures built into processing, with pseudonymisation given as an example	Redaction happens on every request, before it leaves, with your settings as the default
Art. 28, processor	A written contract with each processor	Nonimo acts as processor; ask for the agreement at hello@nonimo.ai
Art. 30, records of processing	A record of processing activities	The monthly report and the log supply the figures for the AI processing entry
Art. 32(1)(a), security of processing	Measures including pseudonymisation and encryption	Labels in place of the data, a machine with encrypted memory, encrypted stored settings
Art. 35, DPIA	An assessment where processing is likely to be high risk	The summary table, the role table and the report feed the assessment
Chapter V, international transfers	Conditions on data sent outside the UK or EEA	What travels to the provider carries labels where the personal data were

A note on pseudonymisation as a legal concept

Article 4(5) defines pseudonymisation as processing personal data so that they can no longer be attributed to a specific person without additional information kept separately and protected [1]. Recital 26 places anonymous data outside the Regulation altogether.

The European Data Protection Board adopted its Guidelines 01/2025 on pseudonymisation for public consultation in January 2025 [6]; they are worth reading alongside this paper.

On 4 September 2025 the Court of Justice ruled in case C-413/23 P, EDPS v SRB, that pseudonymised data are not necessarily personal data for a recipient that has no reasonable means of re-identifying the person, and that the question is assessed from each recipient's point of view [8].

That ruling is useful when you consider the AI provider's position, and it should be applied with care. For your organisation, the data remain personal data: the information needed to put the real values back lives in your Gateway, which runs for your organisation alone. Your DPIA should treat the processing on that basis.

In the UK, the ICO has published guidance on AI and data protection [5], which your DPO can read alongside this paper when scoping the DPIA.

08

The evidence you keep

When questions come, a DPO needs something to show. The Gateway produces two documents for that purpose, and both hold figures only.

The monthly report

Each month the dashboard produces a report written for the DPO. It states how many items of personal data were redacted and of which types, in figures only. An illustrative month looks like this:

November (illustrative)	Items redacted
People	4,108
Companies	1,256
Identity documents	1,874
IBANs	962
Emails and phone numbers	1,117
Total	**9,317**

The report slots into your Article 30 record as the measure applied to AI processing, and into the DPIA as evidence that the measure is working.

The per-request log

For each request, the log records the time, the provider, the model and the count by type of data. You can export it as CSV or JSONL and load it into whatever your security team already uses. The log holds counts and metadata only, never the data itself.

These two documents cover the questions you are most likely to be asked: by your own board when it approves the use of AI, by a client whose contract asks how its information is handled, or by an auditor reviewing your controls.

09

Questions your DPO may ask us

These are the questions a DPO or in-house lawyer in the UK or Ireland is likely to put to us, with the short answer to each.

1. **Where is our data processed?** On a confidential Microsoft Azure machine in Ireland, inside the EU, that runs for your organisation alone.
2. **Do Nonimo staff read our requests?** No. The machine only starts published versions of the Gateway, and what it processes is not read by Nonimo staff or Microsoft staff.

3. **What does Nonimo receive from our Gateway?** Figures: the number of requests and of items redacted, plus the licence renewal.
4. **What does our AI provider receive?** Your request with labels in place of the personal data you chose to redact, sent with your own key under your own contract.
5. **Do our users see labels in the answers?** They read normal text. The Gateway restores each real item in the reply, including streamed replies and tool calls.
6. **What is stored, and where?** Your settings, your provider key and your added terms, encrypted in the same region and readable only by your machine.
7. **How long is anything kept?** Request content lasts as long as the request. Stored settings last as long as the Gateway, which is erased after three idle days during a trial (with notice), at the end of a trial or subscription, or on request.
8. **What is Nonimo's role under UK GDPR or the GDPR?** Processor for the text that passes through the hosted Gateway. You remain the controller.
9. **Who are the sub-processors?** Microsoft Azure, which hosts the confidential machine. Cloudflare is a service provider to Nonimo: it handles licences and counts, and the text stays outside its path.
10. **Can we have a processing agreement?** Yes. Ask for it at hello@nonimo.ai.
11. **What do we put in the DPIA?** The summary table and the role table from this paper, the stored-data list, the retention line and the monthly report as ongoing evidence.
12. **Can we choose what happens to each type of data?** Yes. For each type you can redact it, stop the request or record a warning with the count.

If your DPO has a question that is not on this list, send it to hello@nonimo.ai and we will answer it in writing. To see how the Gateway fits with the rest of Nonimo, start at the Nonimo home page.

10

Sources

1. Regulation (EU) 2016/679 (General Data Protection Regulation), Articles 4(5), 5(1)(c), 25, 28, 30, 32(1)(a), 35, Chapter V and Recital 26 — https://eur-lex.europa.eu/eli/reg/2016/679/oj
2. UK GDPR (Regulation (EU) 2016/679 as it applies in the UK) — https://www.legislation.gov.uk/eur/2016/679/contents
3. Data Protection Act 2018 (Ireland) — https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html
4. Data Protection Commission (Ireland) — https://www.dataprotection.ie
5. Information Commissioner's Office, guidance on AI and data protection — https://ico.org.uk
6. European Data Protection Board, Guidelines 01/2025 on Pseudonymisation — https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en
7. Microsoft, Azure confidential computing documentation — https://learn.microsoft.com/azure/confidential-computing/
8. Court of Justice of the European Union, judgment of 4 September 2025, Case C-413/23 P, EDPS v SRB — https://curia.europa.eu/juris/liste.jsf?num=C-413/23

9. Data Protection Act 2018 (United Kingdom) — https://www.legislation.gov.uk/ukpga/2018/12/contents