VerifactAI Client Guide

VerifactAI — installation and user guide

This guide takes you from creating your workspace to your first protected workflow. Allow **30 minutes**.

No particular technical knowledge is required beyond everyday use of n8n or Make.

Contents

1. What VerifactAI does
2. Create your workspace
3. Install the integration
4. Declare your first system
5. Protect a workflow
6. Read your register
7. Switch to blocking mode
8. Export the evidence dossier
9. Common questions

---

1. What VerifactAI does

VerifactAI answers one precise question: **for a given AI system, which AI Act obligations apply, and how do you prove they were handled?**

Three stages:

Declare	You describe a system once. VerifactAI derives the obligations.
Enforce	A node in your workflow checks on every run.
Prove	Every check leaves a link in a tamper-evident chain.

What VerifactAI does not do

It does not guarantee your compliance, and nobody honestly can. Some obligations are organisational: training your staff, maintaining technical documentation, arranging human oversight. No tool can carry those out for you.

VerifactAI identifies the obligations, enforces the ones that can be automated and proves they ran. Your dossier separates the two categories explicitly — that is what makes it credible in front of an auditor.

Vocabulary

System — a declared AI use: a support assistant, a product-description generator, a CV screening tool. One workflow may call several models; that is still one system.

Control — a measure to put in place, for example telling the user they are talking to an AI. Some apply inside the flow, others belong to your organisation.

Evidence — the timestamped record of a decision. Each carries the hash of the previous one: history cannot be rewritten after the fact.

---

2. Create your workspace

2a. Choose a plan

On verifactai.app, **Pricing** section.

Plan	Systems	What sets it apart
Discovery	1	Free. Full register, unlimited checks. No dossier export.
Studio	5	Dossier export, blocking mode.
Agency	20	White-label dossier.
Volume	75	Direct API access, priority support.

Beyond the plan, €9 per additional system per month. **Checks are never billed individually** — verifying every call must cost you nothing extra.

> **Start with Discovery.** It gives you the full register and unlimited checks: enough to see your real gaps before deciding.

2b. Sign up

Free plan: “Start for free” button, company name and work email address.

Paid plan: “Choose…” button, then payment by card or in crypto.

> Disposable addresses are refused: your API keys, invoices and renewal notices all go to this address.

2c. Receive your keys

Your keys arrive by email within a minute.

Save them in your password manager straight away. They are shown once only: we keep nothing but their hash. If you lose them we cannot retrieve them — only issue new ones.

Depending on your plan you receive several keys. **They all belong to the same workspace and share its system quota.** Use them to separate your teams or your clients, without multiplying subscriptions.

> Nothing after a few minutes? Check your spam folder, then message us via the WhatsApp button at the bottom right of the site.

---

3. Install the integration

On n8n

1. Left menu → **Settings** → **Community nodes**
2. **Install a community node**
3. Enter `n8n-nodes-aiact`, tick the risk acknowledgement box
4. **Install**

Then create the connection:

1. **Credentials** → **Add credential** → search for **AI Act Compliance API**
2. **API Key**: your `ak_live_…` key
3. **Base URL**: leave the pre-filled value
4. Click **Test**

The indicator must turn green. If not, the key most likely picked up a stray space when pasted.

On Make

1. Open the invitation link we sent you
2. Confirm adding the app
3. In a scenario: **+** → `AI Act Compliance` → any module
4. **Connection** field → **Add** → paste your key

Nothing to install, nothing to restart.

---

4. Declare your first system

Do this once per AI system, not per workflow.

4a. Create a temporary workflow

This workflow will be deleted afterwards. It only serves to record the declaration.

4b. Configure the module

Field	Value
Resource / Module	**System** → **Create**, or **Declare a System** on Make
Name	The system name, e.g. `Maison Vertier support chatbot`
Declaration	see below
Strict Mode	`Dry run`

4c. Fill in the declaration

JSON. For a typical chatbot:

```
{
  "role": "provider",
  "eu_nexus": true,
  "interacts_with_humans": true,
  "generates_content": true
}
```

Two fields call for a decision.

`role` — who you are under the regulation.

- `provider`: you develop the system, or supply it under your name or your client's
- `deployer`: you use an existing tool under your own responsibility

If in doubt, an agency building a chatbot for a client is a `provider`. A deployer who puts their brand on a tool, or changes its purpose, becomes a provider.

`eu_nexus` — the system is used in the European Union, or its output is used there. Almost always `true`. If `false`, the regulation does not apply and no obligation will come back.

The full list of fields is in Appendix A.

4d. Run it and note the identifier

Click **Execute step** (n8n) or **Run once** (Make). The output contains:

```
{
  "id": "sys_de8bf1da22d44308",
  "pack_ref": "eu-ai-act@2026.08.1",
```

```
  "strict_mode": "dry_run"
}
```

The `pack_ref` is pinned at that moment: your system will always be evaluated against that version of the law, until you migrate it explicitly. That is what lets you replay a March decision under March's law.

4e. Delete the temporary workflow

Never leave this module in a production workflow: it would create a duplicate system on every run.

---

5. Protect a workflow

The permanent setup, four steps.

```
[Trigger] → [VerifactAI check] → [Branch] → [Your AI]
                                          └──────→ [Human fallback]
```

The check goes BEFORE the AI call

✅ `Trigger → Check → Branch → AI agent`
❌ `Trigger → AI agent → Check`

Placed at the end, you would learn that a call fell under a prohibited practice *after* running it. Your chatbot would already have answered.

Configure the check

Field	Value
Operation	**Run Check / Run a Compliance Check**
System	pick from the dropdown
Model	`gpt-5` — recorded in the evidence
Purpose	`customer_support` — recorded in the evidence
Dry Run	**ticked**, for the first two weeks
Fail on Block (n8n)	**unticked**

> The **System** list fills automatically. If it is empty, the connection is not working: go back to step 3.

The module returns:

```
{
  "decision": "warn",
  "risk_level": "transparency",
  "controls_missing": ["disclose_ai_interaction",
"interaction_logging"],
```

```
  "would_block_in_strict": ["disclose_ai_interaction",
"interaction_logging"],
  "evidence_id": "evt_msqbyepizp9adnt"
}
```

Branch on the decision

On n8n — an **IF** node:

Field	Value
Left value	`{{ $json.decision }}`
Operator	**is not equal to** (string)
Right value	`block`

On Make — a **Router**, with a filter on the first branch:

Field	Value
Left value	`{{2.decision}}`
Operator	**Not equal to**
Right value	`block`

The 2 is the number of the check module, shown on its tile. Insert the variable from the suggested list rather than typing it.

The second branch stays **without a filter**: Make sends everything that fails the first one there.

The two branches

Allowed branch — your AI processing, unchanged.

Fallback branch — a message such as: “This request cannot be handled automatically. An adviser will take over.”

That branch is your safety net. Without it, the user faces silence.

---

6. Read your register

On verifactai.app, **Access** section, paste your key.

The four counters

Counter	What it tells you
Systems	How many are declared
With gaps	At least one required control is not in place
Never checked	Declared but never passed through the gateway

Counter	What it tells you
High risk	Classified high risk, even if the obligations do not bite yet

The sort order puts what needs action first: blocked, then never checked, then gaps.

The Controls column

A gauge, for example `3/5`, and beneath it `1 enforceable in the flow`.

That second line is the important one. It says how many missing controls can be fixed technically. The others belong to your organisation, and no tool can settle them.

A system's detail page

Click a name. You get the classification, the enforceable obligations with the facts that triggered them, those coming with their date, and the controls grouped by category.

> **A system can show "Compliant" and "High risk" at the same time.** That is not an error. Since the Digital Omnibus, the high-risk obligations of Annex III are only enforceable from 2 December 2027. The classification warns, the obligations wait.

---

7. Switch to blocking mode

Three stages. Do not skip them.

Weeks 1-2 — Observe

The system is in `dry_run`. Nothing is blocked. On every run, `would_block_in_strict` shows what would fall.

In between — Close the gaps

For each control enforceable in the flow, two routes.

Put it in place. For `disclose_ai_interaction`: add "This assistant is an artificial intelligence" at the opening of your chatbot.

Declare it in place. In a temporary workflow, module **System → Update**, tick the relevant controls under **Implemented Controls**.

> **That field replaces the list, it does not add to it.** Tick every control still in place, not just the new ones — otherwise you lose the previous ones.

Week 3 — Enable

Same manoeuvre, **Strict Mode** set to `On`. Controls enforceable in the flow now block calls.

> **Why this progression?** Going straight to blocking cuts your production on a control nobody suspected was missing, on a Friday evening.

One exception: a practice prohibited by Article 5 blocks in every case, whatever the mode. That is not a configuration option.

---

8. Export the evidence dossier

On a system's page, two buttons: **Open the dossier** and **Save as PDF**. A line below offers the other language.

> The dossier's language follows your interface, but the other version stays available: a French agency audited by an international group needs the English version of the same document.

The dossier contains: the verdict, the system identification, the obligations retained with their triggering facts, the controls by category, and the integrity verification of the evidence chain.

It never says you are compliant. It states what was identified, observed and applied. That is precisely what makes it usable in front of an auditor.

Export is included from the Studio plan. On Discovery you see everything on screen but cannot take anything away.

---

9. Common questions

The System list is empty. The connection is not working. Open it, click **Test**. If the indicator is red: wrong key, or a trailing slash on the address.

"Unknown API key" on the site. A space slipped in when pasting. Retype it, or paste it into a text editor first to check it sits on a single line.

A system appears twice. The declaration module was left in a production workflow. Delete it. The duplicate can be ignored.

`would_block_in_strict` is empty although controls are missing. Normal: the remaining controls are organisational, no tool can apply them.

I lost my key. It is unrecoverable by design. Message us on WhatsApp, we issue a new one and revoke the old.

I want my data deleted. Same channel. We delete the account, the systems and the keys. The evidence chain is kept for the legally required period if you ask us to for an ongoing audit — otherwise it goes too.

I hit my system quota. The refusal message states the price of an extension. You can add systems at €9 per month each, or move up a plan. **Nothing is billed unless you trigger it.**

Appendix A — All declaration fields

Fields marked "conditional" only matter if their parent is `true`.

Identity

Field	Values
`role`	`provider`, `deployer`, `importer`, `distributor`
`eu_nexus`	`true` / `false`

Interaction

Field	Values
`interacts_with_humans`	`true` / `false`
`generates_content`	`true` / `false`
`content_already_live`	conditional — live before 2 August 2026
`deepfake`	conditional — resembles real people or events
`published_text_public_interest`	conditional — texts of public interest
`human_editorial_review`	conditional — review carrying responsibility

Biometrics

Field	Values
`emotion_recognition`	`true` / `false`
`emotion_workplace_education`	conditional — **prohibited** if `true`
`biometric_categorisation`	`true` / `false`
`biometric_sensitive_traits`	conditional — **prohibited** if `true`

Prohibited practices

Any `true` here triggers a definitive block.

`social_scoring·manipulative_techniques·exploits_vulnerabilities·untargeted_face_scraping·nudification`

Domain

Field	Values
`annex_iii`	`none`, `employment_hr`, `credit_scoring`, `education`, `biometrics`, `essential_services`, `law_enforcement`, `critical_infrastructure`, `justice_democracy`
`embedded_regulated_product`	`true` / `false` — safety component of a CE-marked product
`gpai_provider`	`true` / `false` — places a general-purpose model on the market

Appendix B — Typical declarations

Customer support chatbot

```
{
  "role": "provider",
  "eu_nexus": true,
  "interacts_with_humans": true,
  "generates_content": true
}
```

Marketing content generator

```
{
  "role": "provider",
  "eu_nexus": true,
  "generates_content": true
}
```

Video avatars or synthetic voice

```
{
  "role": "deployer",
  "eu_nexus": true,
  "generates_content": true,
  "deepfake": true
}
```

CV screening

```
{
  "role": "deployer",
  "eu_nexus": true,
  "annex_iii": "employment_hr"
}
```

Appendix C — What to do with each decision

Decision	Meaning	Action
`allow`	Controls identified and declared in place	Nothing
`warn`	Controls missing, nothing blocked	Close the gaps, no urgency
`review`	High-risk classification	Human review, prepare the dossier
`block`	Prohibited practice, or strict mode with a missing control	Stop and fix

A `block` on a prohibited practice cannot be worked around. No setting lifts it: the use must stop.

Need help?

WhatsApp button at the bottom right of verifactai.app. That is also the channel for any data deletion request.

VerifactAI identifies the obligations applicable to a declared system and records the controls carried out. This service is not legal advice and does not guarantee compliance.