

VerifactAI — guide d'installation et d'utilisation

Ce guide vous accompagne de la création de votre espace au premier workflow sous surveillance. Comptez **30 minutes**.

Aucune connaissance technique particulière n'est requise au-delà de l'utilisation courante de n8n ou de Make.

Sommaire

1. [Comprendre ce que fait VerifactAI](#)
 2. [Créer votre espace](#)
 3. [Installer l'intégration](#)
 4. [Déclarer votre premier système](#)
 5. [Protéger un workflow](#)
 6. [Lire votre registre](#)
 7. [Passer en mode blocage](#)
 8. [Exporter le dossier de preuves](#)
 9. [Questions courantes](#)
-

1. Comprendre ce que fait VerifactAI

VerifactAI répond à une question précise : **pour un système d'IA donné, quelles obligations de l'AI Act s'appliquent, et comment prouver qu'elles ont été traitées ?**

Trois temps :

Déclarer	Vous décrivez un système une fois. VerifactAI en déduit les obligations.
Contrôler	Un nœud dans votre workflow vérifie à chaque exécution.
Prouver	Chaque contrôle laisse un maillon dans une chaîne inaltérable.

Ce que VerifactAI ne fait pas

Il ne garantit pas votre conformité, et personne ne le peut honnêtement. Certaines obligations sont organisationnelles : former vos équipes, tenir une documentation technique, organiser une supervision humaine. Aucun outil ne peut les exécuter à votre place.

VerifactAI identifie les obligations, applique celles qui sont automatisables et prouve leur exécution. Votre dossier distingue clairement les deux catégories — c'est ce qui le rend crédible devant un auditeur.

Vocabulaire

Système — un usage d'IA déclaré : un assistant de support, un générateur de fiches produit, un tri de candidatures. Un même workflow peut appeler plusieurs modèles, cela reste un système.

Contrôle — une mesure à mettre en place, par exemple informer l'utilisateur qu'il parle à une IA. Certains s'appliquent dans le flux, d'autres relèvent de votre organisation.

Preuve — l'enregistrement horodaté d'une décision. Chacun porte l'empreinte du précédent : l'historique ne peut pas être réécrit après coup.

2. Créer votre espace

2a. Choisir une formule

Sur verifactai.app, section **Tarifs**.

Formule	Systèmes	Ce qui la distingue
Découverte	1	Gratuit. Registre complet, contrôles illimités. Pas d'export du dossier.
Studio	5	Export du dossier, mode blocage.
Agence	20	Dossier en marque blanche.
Volume	75	Accès API directe, support prioritaire.

Au-delà du forfait, 9 € par système supplémentaire et par mois. **Les contrôles ne sont jamais facturés à l'unité** — vérifier chaque appel ne doit rien vous coûter de plus.

Commencez par Découverte. Elle donne accès au registre complet et aux contrôles illimités : de quoi voir vos écarts réels avant de décider.

2b. S'inscrire

Formule gratuite : bouton « Commencer gratuitement », nom d'entreprise et adresse professionnelle.

Formule payante : bouton « Choisir... », puis paiement par carte ou en crypto-monnaie.

Les adresses jetables sont refusées : vos clés API, vos factures et vos avis d'échéance passent par cette adresse.

2c. Recevoir vos clés

Vos clés arrivent par email en moins d'une minute.

Rangez-les immédiatement dans votre gestionnaire de mots de passe. Elles ne sont affichées qu'une fois : nous ne conservons que leur empreinte. Si vous les perdez, nous ne pouvons pas les retrouver — seulement en émettre de nouvelles.

Selon votre formule, vous recevez plusieurs clés. **Elles appartiennent toutes au même espace et partagent son quota de systèmes.** Utilisez-les pour séparer vos équipes ou vos clients, sans multiplier les abonnements.

Rien reçu au bout de quelques minutes ? Vérifiez vos indésirables, puis écrivez-nous par le bouton WhatsApp en bas à droite du site.

3. Installer l'intégration

Sur n8n

1. Menu de gauche → **Settings** → **Community nodes**
2. **Install a community node**
3. Saisir `n8n-nodes-aiact`, cocher la case de reconnaissance des risques
4. **Install**

Puis créer la connexion :

1. **Credentials** → **Add credential** → chercher **AI Act Compliance API**
2. **API Key** : votre clé `ak_live_...`
3. **Base URL** : laissez la valeur pré-remplie
4. Cliquez sur **Test**

Le voyant doit passer au vert. Sinon, la clé comporte probablement un espace en trop au collage.

Sur Make

1. Ouvrez le lien d'invitation que nous vous avons transmis ou dans le footer App Make
2. Confirmez l'ajout de l'app
3. Dans un scénario : + → `AI Act Compliance` → n'importe quel module
4. Champ **Connection** → **Add** → collez votre clé

Rien à installer, rien à redémarrer.

4. Déclarer votre premier système

À faire une fois par système IA, pas à chaque workflow.

4a. Créer un workflow temporaire

Ce workflow sera supprimé après usage. Il ne sert qu'à enregistrer la déclaration.

4b. Configurer le module

Champ	Valeur
Resource / Module	System → Create , ou Declare a System sur Make
Name	Le nom du système, ex. <code>Chatbot support Maison Vertier</code>
Declaration	voir ci-dessous
Strict Mode	<code>Dry run</code>

4c. Remplir la déclaration

Du JSON. Pour un chatbot classique :

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

Deux champs demandent une décision.

role — qui vous êtes au sens du règlement.

- **provider** : vous développez le système ou le livrez sous votre nom, ou celui de votre client
- **deployer** : vous utilisez un outil existant sous votre responsabilité

En cas de doute pour une agence qui construit un chatbot pour un client : **provider**. Un déployeur qui appose sa marque ou change la finalité d'un outil devient fournisseur.

eu_nexus — le système est utilisé dans l'Union européenne, ou ses résultats y sont utilisés. Presque toujours **true**. Si **false**, le règlement ne s'applique pas et aucune obligation ne remontera.

La liste complète des champs est en [annexe A](#).

4d. Exécuter et noter l'identifiant

Cliquez sur **Execute step** (n8n) ou **Run once** (Make). La sortie contient :

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

Le `pack_ref` est épinglé à cet instant : votre système sera toujours évalué contre cette version du droit, jusqu'à migration explicite. C'est ce qui permet de rejouer une décision de mars avec le droit de mars.

4e. Supprimer le workflow temporaire

Ne laissez jamais ce module dans un workflow de production : il créerait un système en double à chaque exécution.

5. Protéger un workflow

Le montage permanent, quatre étapes.

```
[Déclencheur] → [Contrôle VerifactAI] → [Aiguillage] → [Votre IA]
                                                    └───→ [Repli
humain]
```

Le contrôle se place AVANT l'appel à l'IA

- ☒ Déclencheur → Contrôle → Aiguillage → Agent IA
- ☒ Déclencheur → Agent IA → Contrôle

Placé à la fin, vous apprendriez qu'un appel relevait d'une pratique interdite *après* l'avoir exécuté. Votre chatbot aurait déjà répondu.

Configurer le contrôle

Champ	Valeur
Operation	Run Check / Run a Compliance Check
System	choisir dans la liste déroulante
Model	gpt-5 — consigné dans la preuve
Purpose	customer_support — consigné dans la preuve
Dry Run	coché , les deux premières semaines
Fail on Block (n8n)	décoché

La liste **System** se remplit automatiquement. Si elle est vide, la connexion ne fonctionne pas : retournez à l'étape 3.

Le module renvoie :

```
{
  "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"
}
```

Aiguiller sur la décision

Sur **n8n** — un nœud **IF** :

Champ	Valeur
Valeur de gauche	<code>{{ \$json.decision }}</code>
Opérateur	is not equal to (chaîne)
Valeur de droite	<code>block</code>

Sur **Make** — un **Router**, avec un filtre sur la première branche :

Champ	Valeur
Valeur de gauche	<code>{{2.decision}}</code>
Opérateur	Not equal to
Valeur de droite	<code>block</code>

Le **2** est le numéro du module de contrôle, affiché sur sa vignette. Insérez la variable depuis la liste proposée plutôt que de la taper.

La seconde branche reste **sans filtre** : Make y envoie tout ce qui ne passe pas le premier.

Les deux branches

Branche autorisée — votre traitement IA, inchangé.

Branche de repli — un message du type : « Cette demande ne peut pas être traitée automatiquement. Un conseiller va prendre le relais. »

Cette branche est votre garde-fou. Sans elle, l'utilisateur fait face à un silence.

6. Lire votre registre

Sur verifactai.app, section **Accès**, collez votre clé.

Les quatre compteurs

Compteur	Ce qu'il dit
Systèmes	Le nombre déclaré
Avec écarts	Au moins un contrôle exigé n'est pas en place
Jamais contrôlés	Déclarés mais jamais passés par la passerelle
Haut risque	Classés haut risque, même si les obligations ne mordent pas encore

Le tri met devant ce qui demande une action : bloqué, puis jamais contrôlé, puis écarts.

La colonne Contrôles

Une jauge, par exemple `3/5`, et en dessous `1 applicable dans le flux`.

Cette seconde ligne est la plus importante. Elle dit combien de contrôles manquants sont corrigeables techniquement. Les autres relèvent de votre organisation, et aucun outil ne peut les régler.

La fiche d'un système

Cliquez sur un nom. Vous obtenez la classification, les obligations opposables avec les faits qui les ont déclenchées, celles à venir avec leur date, et les contrôles groupés par catégorie.

Un système peut afficher « Conforme » et « Haut risque » à la fois. Ce n'est pas une erreur. Depuis le Digital Omnibus, les obligations haut risque de l'annexe III ne sont opposables qu'au 2 décembre 2027. La classification alerte, les obligations attendent.

7. Passer en mode blocage

Trois temps. Ne les sautez pas.

Semaines 1-2 — Observer

Le système est en `dry_run`. Rien n'est bloqué. À chaque exécution, `would_block_in_strict` indique ce qui tomberait.

Entre les deux — Fermer les écarts

Pour chaque contrôle applicable dans le flux, deux voies.

Le mettre en place. Exemple pour `disclose_ai_interaction` : ajoutez « Cet assistant est une intelligence artificielle » en ouverture de votre chatbot.

Le déclarer en place. Dans un workflow temporaire, module **System** → **Update**, cochez les contrôles concernés dans **Implemented Controls**.

Ce champ remplace la liste, il ne l'enrichit pas. Cochez tous les contrôles encore en place, pas seulement les nouveaux — sinon vous perdez les précédents.

Semaine 3 — Activer

Même manœuvre, **Strict Mode** sur **On**. Les contrôles applicables dans le flux bloquent désormais les appels.

Pourquoi cette progression ? Passer directement en blocage coupe votre production sur un contrôle dont personne ne soupçonnait l'absence, un vendredi soir.

Une exception : une pratique interdite par l'article 5 bloque dans tous les cas, quel que soit le mode. Ce n'est pas une option de configuration.

8. Exporter le dossier de preuves

Sur la fiche d'un système, deux boutons : **Ouvrir le dossier** et **Enregistrer en PDF**. Une ligne en dessous propose la **version anglaise**.

La langue du dossier est celle de l'audit, pas celle de votre interface. Une agence française auditée par un groupe international a besoin de la version anglaise du même document.

Le dossier contient : le verdict, l'identification du système, les obligations retenues avec leurs faits déclencheurs, les contrôles par catégorie, et la vérification d'intégrité de la chaîne de preuves.

Il ne dit jamais que vous êtes conforme. Il dit ce qui a été identifié, constaté et appliqué. C'est précisément ce qui le rend utilisable devant un auditeur.

L'export est inclus dès la formule Studio. En Découverte, vous consultez tout à l'écran mais ne pouvez rien emporter.

9. Questions courantes

La liste System est vide. La connexion ne fonctionne pas. Ouvrez-la, cliquez sur **Test**. Si le voyant est rouge : clé erronée, ou barre oblique en trop à la fin de l'adresse.

« **Clé API inconnue** » sur le site. Un espace s'est glissé au collage. Retapez-la, ou collez-la d'abord dans un éditeur de texte pour vérifier qu'elle tient sur une seule ligne.

Un système apparaît deux fois. Le module de déclaration est resté dans un workflow de production. Supprimez-le. Le doublon peut être ignoré.

`would_block_in_strict` est vide alors que des contrôles manquent. Normal : les contrôles restants sont organisationnels, aucun outil ne peut les appliquer.

J'ai perdu ma clé. Elle est irrécupérable par conception. Écrivez-nous sur WhatsApp, nous en émettons une nouvelle et révoquons l'ancienne.

Je veux supprimer mes données. Même canal. Nous supprimons le compte, les systèmes et les clés. La chaîne de preuves est conservée le temps légal si vous nous le demandez pour un audit en cours, sinon elle part aussi.

J'ai atteint mon quota de systèmes. Le message de refus indique le prix d'une extension. Vous pouvez ajouter des systèmes à 9 € par mois chacun, ou passer à la formule supérieure. **Rien n'est facturé sans que vous le déclenchiez.**

Annexe A — Tous les champs de déclaration

Les champs « conditionnels » ne sont pertinents que si leur parent vaut `true`.

Identité

Champ	Valeurs
role	provider, deployer, importer, distributor
eu_nexus	true / false

Interaction

Champ	Valeurs
interacts_with_humans	true / false
generates_content	true / false
content_already_live	conditionnel — en production avant le 2 août 2026
deepfake	conditionnel — imite des personnes ou événements réels
published_text_public_in terest	conditionnel — textes d'information publique
human_editorial_review	conditionnel — relecture engageant une responsabilité

Biométrie

Champ	Valeurs
emotion_recognition	true / false
emotion_workplace_education	conditionnel — interdit si true
biometric_categorisation	true / false
biometric_sensitive_traits	conditionnel — interdit si true

Pratiques interdites

Tout `true` ici entraîne un blocage définitif.

`social_scoring · manipulative_techniques · exploits_vulnerabilities · untargeted_face_scraping · nudification`

Domaine

Champ	Valeurs
<code>annex_iii</code>	<code>none, employment_hr, credit_scoring, education, biometrics, essential_services, law_enforcement, critical_infrastructure, justice_democracy</code>
<code>embedded_regulate_d_product</code>	<code>true / false</code> — composant de sécurité d'un produit marqué CE
<code>gpai_provider</code>	<code>true / false</code> — met sur le marché un modèle à usage général

Annexe B — Déclarations types

Chatbot de support client

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

Générateur de contenu marketing

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

Avatars vidéo ou voix de synthèse

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

Tri de candidatures

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

Annexe C — Que faire face à chaque décision

Décision	Signification	Action
allow	Contrôles identifiés et déclarés en place	Rien
warn	Des contrôles manquent, rien n'est bloqué	Fermer les écarts, sans urgence
review	Classification haut risque	Revue humaine, préparer le dossier

Décision	Signification	Action
block	Pratique interdite, ou mode strict et contrôle manquant	Arrêter et corriger

Un `block` sur pratique interdite ne se contourne pas. Aucun réglage ne le lève : l'usage doit cesser.

Besoin d'aide ?

Bouton WhatsApp en bas à droite de verifactai.app.
C'est aussi par là pour toute demande de suppression de données.

VerifactAI identifie les obligations applicables à un système déclaré et consigne les contrôles exécutés. Ce service ne constitue pas un avis juridique et ne garantit pas la conformité.