

Rapport de Transparence et de Gouvernance des Systèmes d'Intelligence Artificielle au sein de la Plateforme IOGA

Préambule Exécutif et Note de Cadrage

En ma qualité de Délégué à la Protection des Données (DPO) de la société IOGA, je vous sou mets le présent rapport de transparence. Ce document a pour vocation d'exposer de manière exhaustive, rigoureuse et intelligible la stratégie, l'architecture technique et le cadre de gouvernance éthique qui régissent l'utilisation de l'Intelligence Artificielle (IA) au sein de notre plateforme SaaS de gestion et de capitalisation des connaissances.

L'objectif de ce document est double. Premièrement, il vise à répondre au besoin légitime de réassurance de nos clients quant à la confidentialité de leurs actifs immatériels (savoir-faire, secrets industriels, données collaborateurs). Deuxièmement, il anticipe et s'aligne sur les exigences de transparence édictées par les cadres réglementaires européens actuels et futurs, notamment le Règlement Général sur la Protection des Données (RGPD) et le Règlement sur l'Intelligence Artificielle (AI Act).

Il convient de préciser en préambule que l'analyse produite ici repose sur l'ensemble des documentations techniques, juridiques et architecturales internes à IOGA. Par conséquent, les informations contenues dans ce rapport se fondent exclusivement sur les infrastructures vérifiées et les politiques documentées de l'entreprise.

Ce rapport démontrera que chez IOGA, l'IA n'est jamais une fin en soi, ni un "agent libre", mais un outil de traitement déterministe, soumis à un contrôle humain strict et à une étanchéité des données absolue.

1. Philosophie et Positionnement Stratégique : L'IA comme Service Instrumental

Pour comprendre le niveau de sécurité offert par IOGA, il est impératif de saisir la philosophie qui sous-tend notre intégration technologique. Contrairement aux modèles grand public qui visent à créer une "Intelligence Artificielle Générale" autonome, IOGA déploie une **IA Instrumentale et Servicielle**.

1.1 La Substitution Fonctionnelle : L'IA au Service de l'Humain

Le principe directeur de notre déploiement IA est celui de la "substitution fonctionnelle". Chaque fonctionnalité basée sur l'IA au sein de la plateforme IOGA a été conçue pour exécuter une tâche précise, fastidieuse et répétitive, qui était historiquement réalisée par des humains, mais avec une efficacité et une scalabilité accrues.

Lorsque nous utilisons des modèles neuronaux pour transcrire une vidéo, générer un résumé, chapitrer une vidéo ou indexer un contenu, nous ne demandons pas à la machine de "penser" ou de "créer" ex nihilo. Nous lui demandons de **traiter un signal**.

- **Transcription (Whisper)** : L'IA agit ici comme un sténotypiste virtuel. Elle convertit des ondes sonores en texte. C'est un processus de traitement du signal audio (Digital Signal Processing) couplé à de la reconnaissance de formes linguistiques.
- **Synthèse et Questionnement (LLM)** : L'IA agit comme un documentaliste ou un archiviste. Elle lit un texte (la transcription) et en extrait les points clés ou formule des questions pertinentes pour structurer le savoir.

Cette distinction est cruciale : IOGA n'utilise pas l'IA pour prendre des décisions automatisées ayant des effets juridiques sur les personnes (comme le profilage RH ou l'évaluation de crédit), mais uniquement pour **rendre des services de manipulation de l'information**. L'IA chez IOGA est un "processeur" de connaissances, pas un "auteur" de connaissances.

1.2 Absence Totale d'Usage "General Purpose" (GPAI)

Une inquiétude majeure des entreprises concerne l'accès de leurs collaborateurs à des IA génératives dites "General Purpose" (à usage général), telles que ChatGPT dans sa version publique, où les données peuvent fuir ou être utilisées à des fins d'entraînement.

IOGA affirme catégoriquement qu'il n'existe aucun usage de type "General Purpose AI" au sein de sa plateforme.

Les interfaces que nous mettons à disposition (champs de saisie, assistants de recherche) sont strictement contextuelles. Elles sont "bridées" par conception (Privacy by Design). Un utilisateur ne peut pas utiliser l'assistant IOGA pour générer du code informatique, écrire un poème, ou interroger l'IA sur des faits extérieurs à la base de connaissance de l'entreprise. Le système est conçu comme un circuit fermé (Closed Loop) : les invites (prompts) système injectées par IOGA forcent le modèle à ne travailler que sur les données fournies dans le contexte de la vidéo ou du document en cours de traitement.

1.3 Le Mandat de "Non-Entraînement" (No-Training Policy)

C'est le pilier central de notre contrat de confiance. **IOGA ne réalise aucun entraînement (training) ni aucun ajustement fin (fine-tuning) de modèles d'IA avec les données de ses clients.**

Dans l'industrie de l'IA, il existe une différence fondamentale entre "l'inférence" (l'utilisation du modèle) et "l'entraînement" (l'apprentissage du modèle).

- **Chez IOGA** : Nous faisons uniquement de l'inférence. Les données de nos clients traversent le modèle pour être traitées, mais ne s'y arrêtent pas. Elles ne modifient pas les poids synaptiques du réseau de neurones. Le modèle est identique avant et après le traitement de vos données.
 - **La garantie** : Cela signifie que si un client A dépose une vidéo contenant un secret de fabrication confidentiel, le modèle d'IA ne "l'apprend" pas. Il est donc mathématiquement impossible que ce secret soit révélé ultérieurement à un client B via une réponse de l'IA, car le modèle n'a gardé aucune trace mémorielle de l'information.
-

2. Architecture Technique et Souveraineté des Données

La sécurité des données ne repose pas sur des promesses, mais sur une architecture tangible et vérifiable. IOGA a mis en place une infrastructure hybride (Multi-Cloud) sophistiquée, conçue pour maximiser la sécurité tout en respectant scrupuleusement les exigences de souveraineté des données européennes.

2.1 Le Socle de Persistance : AWS France (Paris)

Le cœur de la plateforme IOGA—le lieu où vos données résident de manière permanente—est hébergé par **Amazon Web Services (AWS)**, exclusivement dans la région **Europe (Paris) / eu-west-3**.

Cette localisation garantit que le "Gold Copy" (la version maître) de toutes vos données (fichiers vidéo sources, fichiers encodés, bases de données utilisateurs, métadonnées, documents annexes, etc.) est physiquement stocké sur le territoire français. Ce stockage est soumis au droit français et européen.

- **Ségrégation Logique** : Les données de chaque client sont isolées logiquement. Il n'existe pas de "lac de données" (*data lake*) commun où les informations pourraient se mélanger.
- **Chiffrement** : Toutes les données stockées sont chiffrées au repos (*At Rest*) utilisant le standard AES-256. Les clés de chiffrement sont gérées de manière sécurisée, rendant les données inintelligibles pour toute personne ne disposant pas des droits d'accès applicatifs.

2.2 La Couche Cognitive : Azure OpenAI en Suisse

Pour les traitements d'intelligence artificielle les plus avancés (notamment les modèles de langage GPT-4o mini et la transcription Whisper), IOGA a fait le choix stratégique de s'appuyer sur le partenariat **Microsoft Azure OpenAI Service**.

Cependant, nous n'utilisons pas la région par défaut. Nous avons spécifiquement configuré nos

services pour qu'ils soient exécutés dans la région Azure Suisse Nord (Zurich).

Pourquoi ce choix de la Suisse?

1. **Excellence de la Confidentialité** : La Suisse dispose de l'une des législations sur la protection des données les plus strictes au monde (LPD/nLPD), offrant un niveau de protection reconnu comme "adéquat" par la Commission Européenne (ce qui facilite les transferts de données depuis l'UE sans complexité juridique additionnelle).
2. **Infrastructure de Pointe** : Les datacenters suisses de Microsoft sont équipés des dernières générations de GPU nécessaires pour faire tourner des modèles comme GPT-4o avec une latence minimale.
3. **Neutralité et Souveraineté** : En plaçant le traitement cognitif en Suisse, nous ajoutons une couche de neutralité géographique au traitement de l'information sensible.

2.3 Le Flux de Données "Air Gap" (Cloisonnement Fonctionnel)

Il est essentiel de comprendre le cycle de vie de la donnée lors d'un traitement IA.

1. **Extraction** : L'application IOGA (hébergée en France sur AWS) extrait le segment de texte ou d'audio nécessaire.
2. **Transit Sécurisé** : Ce segment est envoyé via un tunnel chiffré (TLS 1.2+) vers l'instance Azure en Suisse.
3. **Traitement Éphémère (Stateless)** : Le modèle Azure traite la donnée en mémoire vive (RAM). C'est une opération "sans état". Dès que le résultat (la transcription ou le résumé) est généré, la donnée d'entrée est purgée de la mémoire du processeur.
4. **Retour et Stockage** : Le résultat est renvoyé en France (AWS) pour y être stocké durablement.
5. **Conclusion** : À aucun moment la donnée source n'est stockée de manière persistante sur les serveurs de traitement en Suisse. Elle n'y fait qu'un passage éclair, le temps du calcul. On pourra se référer à [cette ressource](#) pour en savoir plus sur la politique d'Azure OpenAI à ce sujet.

2.4 Le Rôle Complémentaire d'AWS Bedrock

En complément d'Azure, IOGA utilise également Amazon Bedrock, hébergé dans les régions Europe (Paris) ou Francfort. Ce service est principalement utilisé pour des tâches de vectorisation (Embedding) ou pour accéder à des modèles spécifiques (comme la famille Claude ou Titan) si le besoin s'en fait sentir.

L'utilisation de Bedrock permet de maintenir certains traitements IA (comme la recherche de similarité) strictement au sein du périmètre AWS, évitant même le transit réseau vers Azure pour ces tâches spécifiques. Cela renforce encore la souveraineté en gardant le traitement au plus près de la donnée stockée.

3. Analyse Détaillée des Composants IA et Mécanismes de Sécurité

La transparence exige de descendre dans le détail technique. Nous ne nous contentons pas de dire "il y a de l'IA", nous expliquons "quelle IA fait quoi".

3.1 La Transcription Automatisée (Speech-to-Text)

Composant : Whisper (hébergé sur Azure OpenAI ou AWS SageMaker).

Ce module est la porte d'entrée de la valorisation des connaissances. Il transforme la parole en texte.

- **Fonctionnement** : Le modèle analyse le spectre audio pour identifier des phonèmes et reconstruire des mots. Il est capable de distinguer les locuteurs (diarisation) et de gérer le vocabulaire technique spécifique aux métiers de nos clients.
- **Sécurité** : Le modèle Whisper utilisé est une instance privée, spécifique à IOGA, dans une infrastructure sous son contrôle. Contrairement aux outils de transcription grand public gratuits, aucune donnée audio n'est conservée par le fournisseur pour améliorer sa reconnaissance vocale globale. Le traitement est strictement isolé.

3.2 L'Organisation des Connaissances (Recherche de Similarité)

Composant : Modèles d'Embeddings (Vectorisation) via AWS Bedrock ou Azure.

C'est l'intelligence "structurelle" de IOGA. Elle permet de créer des liens invisibles entre les contenus.

- **Le Concept de Vecteur** : L'IA transforme le texte des vidéos en une série de chiffres (un vecteur) qui représente le *sens* du contenu. Par exemple, elle comprend que "maintenance hydraulique" est sémantiquement proche de "réparation de pompe", même si les mots sont différents.
- **Confidentialité par Obfuscation** : Les vecteurs stockés dans nos bases de données (OpenSearch sur AWS) sont illisibles pour un humain. Si un attaquant volait ces vecteurs, il ne pourrait pas reconstruire le texte original sans le modèle exact et les clés de décodage. C'est une forme de pseudonymisation mathématique de la connaissance.

3.3 L'Assistance Générative (LLM : GPT-4o mini)

Composant : GPT-4o mini (via Azure OpenAI Service).

Nous utilisons ce modèle pour sa rapidité et son efficacité (faible latence). Il intervient à deux moments clés :

1. **En amont (Aide à la création)** : Il génère des questions pertinentes pour guider l'utilisateur qui s'apprête à enregistrer une vidéo. *Exemple* : "Pour une vidéo sur la sécurité

incendie, posez les questions : Quels sont les types d'extincteurs? Comment donner l'alarme?"

2. **En aval (Synthèse)** : Il analyse la transcription pour générer un résumé exécutif, des chapitres logiques et des mots-clés (tags).
- **Contrôle par "System Prompts"** : IOGA injecte des instructions invisibles (System Prompts) qui interdisent à l'IA d'inventer des faits (hallucinations). L'instruction est typiquement : *"Tu es un assistant d'archivage. Résume ce texte en utilisant uniquement les informations présentes. N'ajoute aucune connaissance externe."* Cela garantit la fidélité du résultat par rapport à la source client.

3.4 L'Assistant de Recherche (Chatbot RAG)

Composant : GPT-4o / RAG Architecture.1

Cette fonctionnalité permet aux utilisateurs de "dialoguer" avec leur base de connaissances.

- **Mécanisme RAG (Retrieval-Augmented Generation)** : C'est le point crucial pour la sécurité. Lorsque vous posez une question, l'IA ne répond pas avec sa "mémoire" publique (ce qu'elle a appris sur Internet).
 - Étape 1 : IOGA cherche dans vos documents et données les passages pertinents.
 - Étape 2 : IOGA envoie ces passages + votre question à l'IA.
 - Étape 3 : L'IA formule une réponse grammaticalement correcte basée *uniquement* sur ces passages.
 - **Implication** : L'IA n'a pas besoin de connaître vos secrets pour vous répondre. Elle agit comme un processeur linguistique sur les données qu'on lui présente à l'instant T.
-

4. Cadre Réglementaire et Conformité (RGPD et AI Act)

IOGA ne se contente pas de suivre la réglementation, elle l'intègre dans la conception même de son produit (*Compliance by Design*).

4.1 Conformité au RGPD (Règlement 2016/679)

En tant que plateforme SaaS B2B, IOGA agit principalement en qualité de **Sous-Traitant** (Data Processor) au sens de l'article 28 du RGPD. Nos clients restent les **Responsables de Traitement** (Data Controllers).

- **Accords de Protection des Données (DPA)** : Nous sommes engagés via des DPA stricts avec tous nos sous-traitants ultérieurs (notamment Microsoft et Amazon). Ces accords incluent les *Clauses Contractuelles Types* (CCT) de la Commission Européenne, garantissant que même si un traitement a lieu en Suisse ou aux USA (pour les métadonnées de facturation par exemple), le niveau de protection reste équivalent à celui

de l'UE.

- **Minimisation** : Nous ne transmettons aux services IA que les données strictement nécessaires (le texte ou l'audio par exemple). Aucune métadonnée utilisateur (nom, email, IP) n'est envoyée aux modèles d'IA, assurant une anonymisation fonctionnelle lors du traitement cognitif.

4.2 Alignement avec l'AI Act Européen

Bien que l'AI Act soit en cours de déploiement progressif et sera peut-être révisé prochainement, IOGA s'est déjà alignée sur ses principes directeurs.

- **Qualification du Rôle** : IOGA se positionne comme un **Déployeur** (Deployer) de systèmes d'IA intégrés.
- **Classification des Risques** : Les usages de l'IA dans IOGA (gestion de connaissances, transcription) relèvent des catégories à **Risque Minimal** ou **Limité**. Par exemple, nous ne pratiquons aucune identification biométrique à distance, aucun scoring social, ni aucune prise de décision automatisée affectant les droits fondamentaux des personnes.
- **Transparence (Art. 50)** : Nous respectons l'obligation de transparence en informant clairement les utilisateurs lorsqu'ils interagissent avec un contenu généré par IA (mentions "Transcription automatique", "Résumé généré par IA").

4.3 Gestion de la Rétention et "Zero Data Retention" (ZDR)

Par défaut, les fournisseurs comme Azure conservent les prompts pendant 30 jours uniquement pour des finalités de détection d'abus (Abuse Monitoring - lutte contre les contenus haineux, pédopornographiques, etc.). Cependant, IOGA est consciente des exigences de confidentialité extrême de certains clients. Il convient de noter que, le cas échéant, les accès aux données conservées pour traces d'abus sont strictement encadrés et que IOGA n'a pas accès à ces données. Seuls des personnes investies d'une autorité idoines pourraient y avoir accès.

Nous exploitons les capacités de configuration Zero Data Retention (ZDR) offertes par nos fournisseurs pour les cas d'usage éligibles. Lorsqu'activée, cette option garantit qu'aucune trace des données (prompts ou réponses) n'est conservée, même pour l'analyse d'abus. Les données sont traitées de manière totalement volatile.

5. Conclusion : Une Approche Maîtrisée

L'intégration de l'IA chez IOGA n'est pas une course à la technologie, mais une quête d'efficacité au service du capital humain. Nous avons construit une "boîte de verre" plutôt qu'une "boîte noire".

Nos clients peuvent avoir l'assurance que :

1. **L'IA ne vole pas leurs données** : Le non-entraînement des modèles est garanti

contractuellement et techniquement.

- 2. **L'IA ne remplace pas l'humain** : Elle prépare le travail (transcription, pré-classement) pour que l'humain puisse se concentrer sur la validation et l'expertise.
- 3. **L'IA respecte les frontières** : Le stockage est français, le traitement est européen/suisse, et l'architecture est étanche.

IOGA s'engage à maintenir ce niveau de transparence et à mettre à jour ce document à chaque évolution majeure de nos modèles ou de nos infrastructures, garantissant ainsi une pérennité de la conformité pour nos clients.

Annexe : Description Technique des Éléments IA Mis en Œuvre

Conformément à notre engagement de transparence, cette section détaille les composants spécifiques d'Intelligence Artificielle intégrés à la plateforme IOGA. Ces informations sont fournies pour permettre à nos clients de mettre à jour leurs propres registres de traitement et analyses d'impact.

Note : Les versions exactes des modèles sont susceptibles d'évoluer pour bénéficier des améliorations de performance, mais le cadre de confidentialité (non-entraînement) reste immuable.

Tableau Récapitulatif des Composants IA

Composant / Fonctionnalité	Technologie / Modèle (Placeholder)	Fournisseur & Hébergement	Localisation du Traitement	Données en Entrée (Input)	Données en Sortie (Output)	Finalité du Traitement
Transcription Audio (Speech-to-Text)	Whisper [Version: v3 via Azure OpenAI]	Microsoft Azure (ou AWS SageMaker selon config.)	Suisse (Zurich) (Région: Switzerland North)	Fichier audio extrait de la vidéo (WAV/MP3).	Fichier texte brut avec horodatage (JSON/SRT).	Convertir la parole en texte pour l'accessibilité et la recherche.
Génération de Questions (Assistant Créateur)	GPT-4o mini [Version: 2024-07-18]	Microsoft Azure OpenAI	Suisse (Zurich) (Région: Switzerland North)	Titre de la vidéo, sujet, ou mots-clés fournis par l'utilisateur.	Liste de 5 à 10 questions suggérées pour l'interview.	Aider l'utilisateur à structurer son intervention vidéo.
Synthèse et Résumé (Post-Production)	GPT-4o mini [Version: 2024-07-18]	Microsoft Azure OpenAI	Suisse (Zurich) (Région: Switzerland North)	Transcription textuelle complète de la vidéo.	Résumé court (Abstract), liste des points clés.	Permettre une consommation rapide du contenu sans visionnage

Composant / Fonctionnalité	Technologie / Modèle (Placeholder)	Fournisseur & Hébergement	Localisation du Traitement	Données en Entrée (Input)	Données en Sortie (Output)	Finalité du Traitement
						complet.
Recherche de Similarité / Chaptering	Titan Embeddings ou Cohere ``	AWS Bedrock	France (Paris) ou Allemagne (Francfort)	Segments de texte de la transcription.	Vecteurs (Embeddings) : tableaux numériques.	Identifier les passages similaires, suggérer des chapitres et des vidéos connexes.
Assistant de Recherche (Chatbot RAG)	GPT-4o [Version: 2024-05-13]	Microsoft Azure OpenAI	Suisse (Zurich) (Région: Switzerland North)	Question de l'utilisateur + Extraits pertinents des transcriptions.	Réponse en langage naturel synthétisant les extraits.	Répondre aux questions des utilisateurs en se basant uniquement sur la base documentaire.
Traduction Automatique	Azure AI Translator ou AWS Translate	Microsoft Azure ou AWS	Europe (France ou Suisse)	Texte source (transcription).	Texte cible (traduction).	Générer des sous-titres multilingues.

Précisions sur les Flux de Données :

- Stockage Persistant** : Toutes les données générées (transcriptions, résumés, vecteurs) sont rapatriées et stockées uniquement sur **AWS France (Paris)** dans les bases de données IOGA (RDS/DynamoDB/S3).
- Statut des Modèles** : Tous les modèles listés ci-dessus sont utilisés en mode **"Inférence Seule"**. Aucune donnée client n'est stockée dans le modèle lui-même.
- Identifiants Personnels** : Les identifiants directs des utilisateurs (Noms, Emails) ne sont pas transmis aux API des modèles d'IA, sauf s'ils sont prononcés oralement dans la vidéo ou écrits dans le texte à traiter.

Ce document est valide à la date de sa rédaction et sera révisé annuellement ou lors de changements architecturaux significatifs.