Architecture technique et hébergement de TokiChat

Éditeur : Codexplore Lab
Solution : TokiChat

Version : v1.0

Introduction

TokiChat est une plateforme éducative d'intelligence artificielle en cours de développement, portée par Codexplore Lab.

Le présent document décrit l'architecture technique, les principes d'hébergement, les dispositifs de sécurité et les orientations de conformité réglementaire du projet.

Il s'agit d'une vision consolidée de l'infrastructure cible : certaines fonctionnalités évoquées (micro-services, filtres IA avancés, outils d'analyse pédagogique automatisés, etc.) sont encore en phase de conception ou de prototypage.

Elles font l'objet de développements progressifs en collaboration avec nos partenaires techniques (Lonestone) et scientifiques (CREN, CATIE).

L'objectif est d'assurer une montée en maturité continue du système, dans le respect des cadres réglementaires et éthiques applicables à l'éducation et à l'intelligence artificielle.

Stack technique

Front-end : React

- Application web développée en React, avec une interface épurée, accessible et responsive.
- Utilisation de Tailwind CSS pour la cohérence visuelle et la performance.
- Architecture orientée composants, facilitant la maintenance et les évolutions rapides.

Back-end : NestJS / REST / Micro ORM

- API développée en NestJS, framework Node.js robuste et modulaire.
- Communication via des endpoints REST sécurisés.
- Gestion des données par Micro ORM, assurant des transactions performantes et un typage strict.
- Structure micro-services en préparation pour supporter la montée en charge.

Authentification : Keycloak

- Gestion centralisée des identités via Keycloak, solution open-source compatible avec le SSO (Single Sign-On).
- Intégration fluide avec les systèmes existants des établissements (ENT, AzureAD, LDAP).
- Contrôle granulaire des rôles (administrateurs, enseignants, apprenants) et des politiques d'accès.

Prestataire technique : Lonestone (Nantes)

- Studio de développement web et IA basé à Nantes, expert en conception produit, architecture logicielle et intégration d'IA.
- Lonestone assure la co-construction technique du produit et le suivi d'industrialisation.

Hébergement et souveraineté des données

Hébergeur : Scaleway (Startup Program)

- L'ensemble des environnements de production est hébergé chez Scaleway, fournisseur français reconnu pour ses datacenters situés intégralement en France.
- Infrastructure certifiée ISO 27001, garantissant la conformité RGPD.
- Codexplore Lab a été sélectionné pour le programme Scaleway Startup.
- Les données pédagogiques (consignes, cadrage des activités, niveau des élèves…), utilisateurs et de configuration sont stockées et traitées exclusivement sur le territoire français.

Environnement de test et préproduction

- Les environnements de test et de préproduction sont auto-hébergés par le studio Lonestone à Nantes, qui assure la supervision technique, la maintenance et la mise à jour des environnements internes.

Stockage des conversations par les fournisseurs d'IA

Les requêtes et réponses échangées entre TokiChat et les modèles d'IA tiers (OpenAI, Mistral, Anthropic, etc.) sont transmises **après filtrage automatique et pseudonymisation**, dans le but de réduire au maximum la présence de données personnelles.

Codexplore Lab s'engage à mettre en œuvre **tous les moyens techniques et organisationnels raisonnables** pour empêcher la transmission d'informations identifiantes, mais **ne peut garantir une absence totale de données personnelles** lorsque celles-ci sont introduites volontairement par un utilisateur final.

La responsabilité de la saisie des contenus relève donc de l'utilisateur, dans le cadre du règlement intérieur de l'établissement et des conditions d'usage de TokiChat.

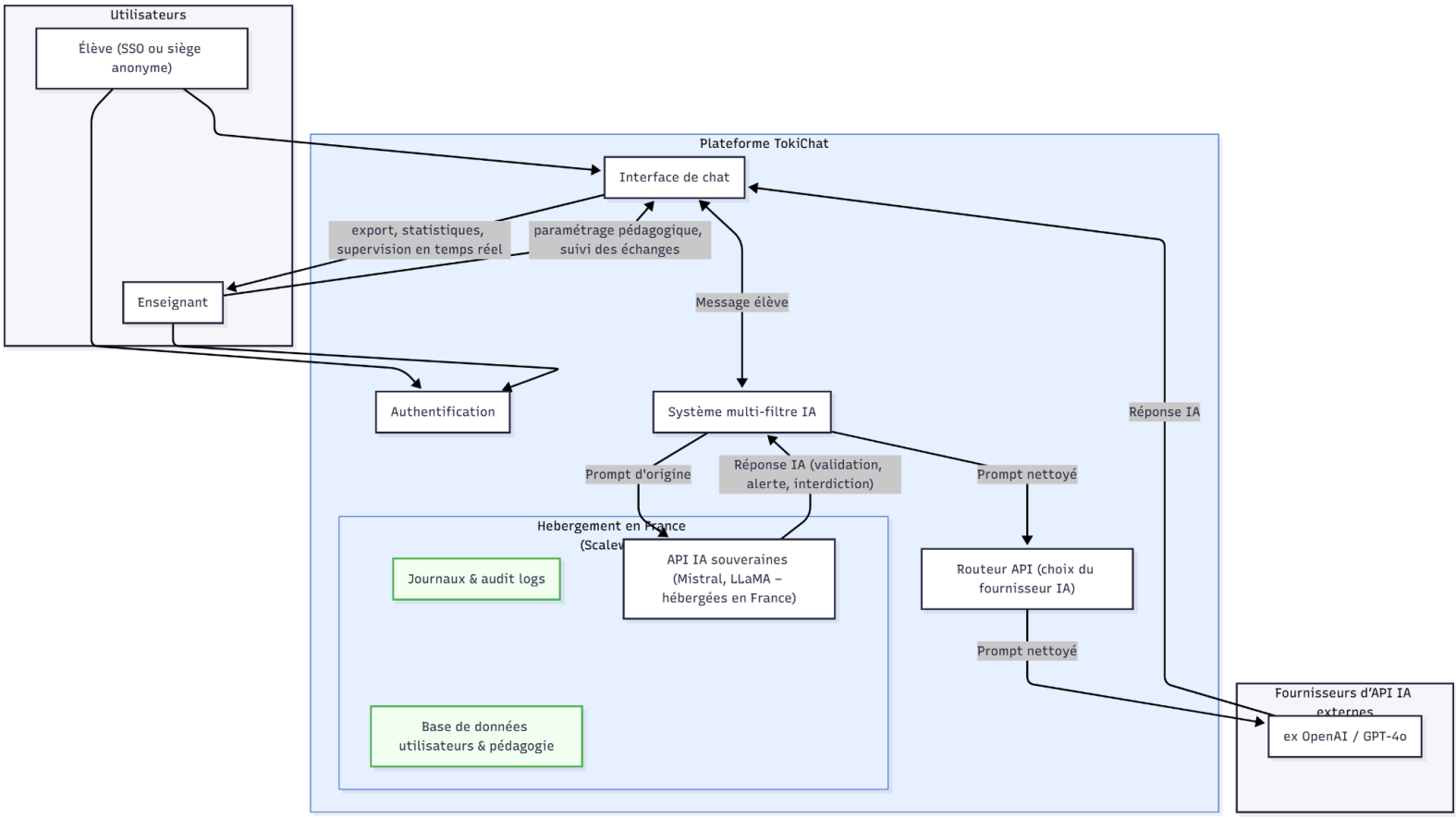
Conformément à leurs politiques publiques, les **fournisseurs d'API IA n'utilisent pas ces échanges pour l'entraînement ou le réentraînement de leurs modèles**, sauf consentement explicite de leurs clients professionnels.
CodexploreLab sélectionne exclusivement des prestataires dont les **conditions d'utilisation précisent la non-conservation durable** des requêtes à des fins autres que la fourniture du service (modération, sécurité, facturation).

La **durée de rétention technique** varie selon les fournisseurs :

- OpenAI (API) : jusqu'à 30 jours maximum pour raisons de sécurité, sans usage d'entraînement ;
- Mistral AI : conservation limitée au traitement temps réel, sans stockage des prompts ni des réponses ;
- Anthropic (Claude API) : conservation temporaire pour contrôle de conformité, sans réutilisation des données.

Codexplore Lab maintient à jour une **fiche de conformité par fournisseur IA**, recensant les durées de conservation déclarées, la localisation des serveurs et les politiques de traitement des données.
Les établissements partenaires peuvent consulter ces fiches sur demande afin de vérifier la conformité RGPD et IA Act des prestataires utilisés.

Schéma de gouvernance des flux de données



Tous les échanges sont chiffrés (HTTPS/TLS 1.3).

Les données envoyées aux API externes sont préalablement filtrées (prompts), anonymisées (metadata) et non persistées.

Système IA

Modèle IA utilisé

Démonstrateur actuel :

- Utilisation de ChatGPT 4o mini sur le démonstrateur de base.
- Usage limité et strictement encadré, avec aucune réutilisation des données d'apprentissage par OpenAI.
- Stockage des données de conversation sur serveur européen.

Futur proche : approche agnostique

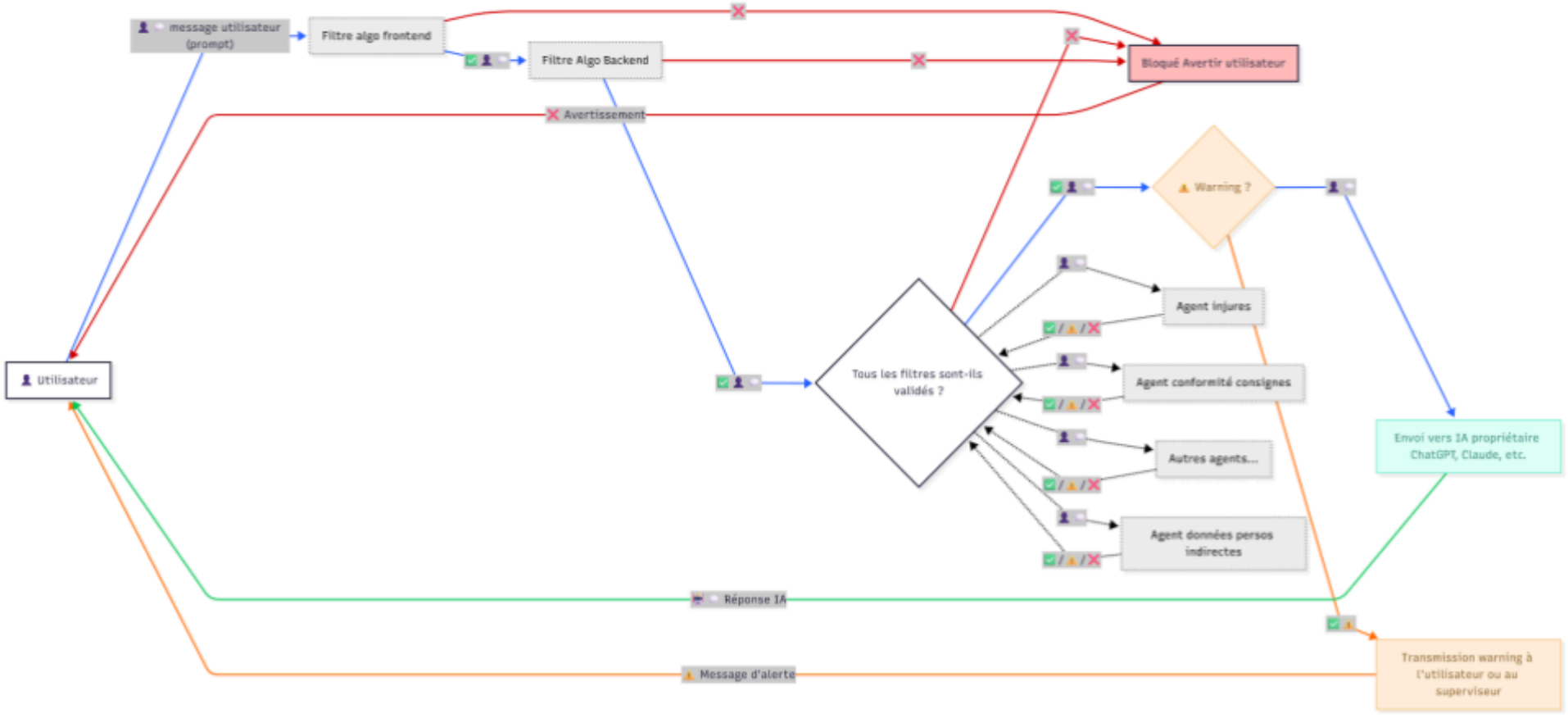
- TokiChat est agnostique des modèles IA : tout modèle compatible API (GPT, Claude, Mistral, LLaMA, etc.) peut être configuré selon les besoins du client. En l'état actuel l'outil est configuré sur une instance dédiée avec une clé d'API vers un fournisseur LLM tiers convenu avec le client.
- Cette approche garantit une indépendance vis-à-vis des fournisseurs et une adaptation continue aux standards du marché.
- L'organisme de formation pourra, via l'interface, définir les modèles autorisés et par défaut. **[À venir]**
- Le formateur pourra, via l'interface, choisir le modèle le plus adapté à chaque activité. **[À venir]**

Système de filtres et sécurité des données

Architecture multi-filtre

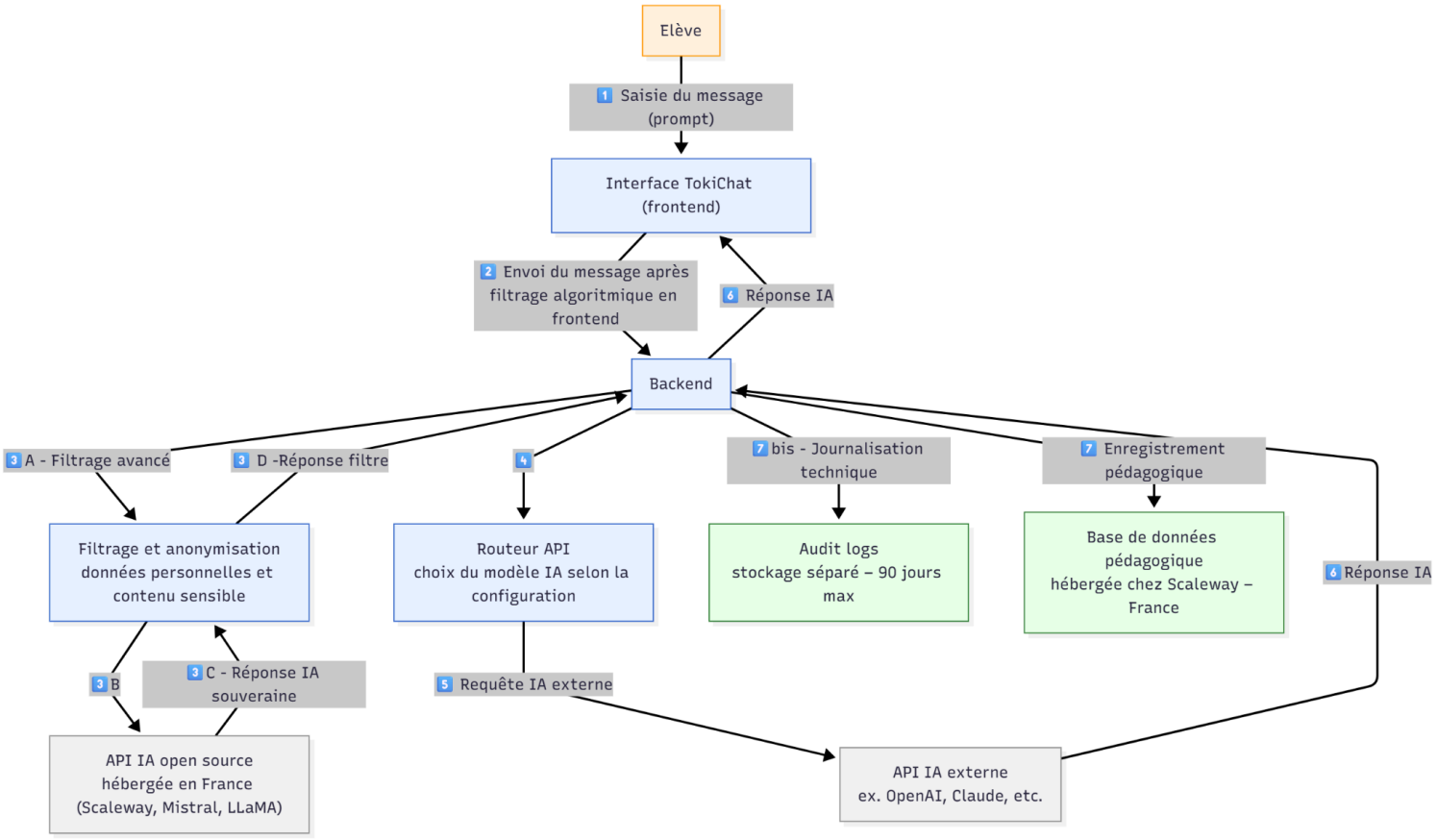
Système propriétaire de filtrage des échanges, garantissant la conformité et la sécurité des interactions :

- Filtre algorithmique **[implémenté]** : détection des données personnelles et expressions sensibles avant envoi au LLM.
- Filtres IA spécialisés **[À venir]** : agents IA open source (Mistral, LLaMA) hébergés via API Scaleway France pour un contrôle souverain.
- Automatisation de l'audit de performance de ces filtres via des tests générés par IA et exécutés à intervalles réguliers **[À venir]**
- À long terme **[À l'étude]** : filtres IA open source, hébergement dédié et fine-tuné pour les tâches pédagogiques.



Système multi filtre TokiChat
(En cours de développement)

Schéma : Parcours d'un prompt saisi par un apprenant



Légende :

🟧 **Utilisateur (élève / apprenant)**	Point d'origine du prompt. Les échanges sont saisis via l'interface TokiChat dans un espace pédagogique dédié et sécurisé.
🔵 **Système TokiChat (frontend, filtre, routeur)**	Ensemble des modules internes contrôlés par Codexplore Lab. Inclut l'authentification, le filtrage, le routage des requêtes et la supervision pédagogique.
⚫ **API IA souveraine (Scaleway, Mistral, LLaMA)**	Modèles IA hébergés en France, opérant dans la zone souveraine. Le traitement y reste sous contrôle de TokiChat (aucune conservation externe des prompts).
⚪ **API IA externe (OpenAI, Claude, etc.)**	Modèles IA tiers accessibles via API sécurisée (TLS 1.3). Les prompts sont anonymisés avant envoi. Aucun entraînement ni stockage n'est autorisé côté fournisseur.

🟩 **Stockage souverain (Scaleway – France)**	Bases de données et journaux techniques hébergés exclusivement en France, certifiés ISO 27001. Séparation stricte entre données pédagogiques et logs techniques.

Vision technique à long terme

CodexploreLab poursuit une trajectoire de développement continue visant à renforcer la confiance, la transparence et la conformité de TokiChat.

1. Système IA de confiance

TokiChat évolue dans le cadre des recommandations actuelles du ministère de l'Éducation nationale et anticipe le futur **cadre européen de certification des systèmes d'IA**.
L'objectif est d'assurer une transparence complète sur les modèles utilisés, leurs sources et leurs limites, tout en garantissant un contrôle humain à chaque étape d'usage.

2. Analyse pédagogique et accompagnement humain

Des travaux de recherche sont menés, en partenariat avec des acteurs académiques et techniques, pour explorer des **outils d'analyse qualitative des échanges IA–apprenant**.
Ces outils visent à assister les enseignants dans le suivi pédagogique, sans automatiser de décisions d'évaluation.

3. Traçabilité et sécurité des échanges

La traçabilité des interactions entre apprenants et IA est déjà assurée via un système de **journalisation horodatée** accessible sur demande des administrateurs. Ce dispositif permet un audit pédagogique et technique, dans le respect du principe de minimisation des données défini par le RGPD.

4. Gouvernance et évolution responsable

CodexploreLab maintient une veille active sur le futur **régime européen de certification IA** (prévu par l'IA Act) afin d'anticiper ses exigences.
Les évolutions techniques seront alignées sur ce cadre, dans une logique de **responsabilité partagée entre fournisseurs, établissements et utilisateurs**.

Gestion et rétention des données

Principe général

TokiChat applique une politique stricte de rétention, d'anonymisation et de purge automatique des données afin de garantir une utilisation conforme aux cadres réglementaires et adaptée aux besoins des établissements éducatifs.

Toutes les données collectées (comptes, conversations, métadonnées) sont conservées uniquement le temps nécessaire à l'usage pédagogique, administratif ou scientifique explicitement autorisé.
Les durées de conservation sont paramétrables selon le cadre institutionnel de l'établissement client (Éducation nationale, CFA, organisme privé, etc.).

Durées de rétention configurables

Chaque établissement peut définir ses propres politiques de conservation :

- Comptes utilisateurs : durée maximale fixée selon les contraintes réglementaires.
    - Exemple : suppression automatique des comptes au 15 août pour le cadre scolaire.
- Conversations et journaux pédagogiques : conservation limitée (par défaut 12 mois) avec possibilité d'export avant purge.
- Logs techniques : 90 jours maximum pour la maintenance.

Purge automatique et traçabilité

- Système automatisé de suppression ou anonymisation programmée des données à échéance.
- Chaque purge fait l'objet d'un journal d'événement (date, type, volume supprimé) garantissant la transparence et la conformité auditable.

- Les enseignants et administrateurs peuvent déclencher manuellement une purge anticipée ou une suppression ciblée. **[À venir]**

Anonymisation des données à visée de recherche

Les échanges utilisés dans les travaux de recherche (CREN, CATIE) sont anonymisés en amont :

- Suppression de toute donnée nominative ou sensible.
- Remplacement des identifiants par des pseudonymes aléatoires.
- Conservation séparée des correspondances d'identifiants (clé de hachage).

  Ces données anonymisées servent exclusivement à l'analyse pédagogique et scientifique, **jamais à l'entraînement de modèles externes.**

Localisation et souveraineté

- Toutes les opérations de stockage, d'archivage et de purge, hors conversations IA, sont effectuées sur les serveurs Scaleway (France), garantissant la conformité RGPD.
- Les environnements de test auto-hébergés par Lonestone respectent les mêmes politiques de conservation et de destruction des données.
- Le stockage des conversations IA dépend du modèle choisi par le client (OpenAI pour le démonstrateur actuel).
- Les contrats passés entre le fournisseur IA et Codexplore Lab respectent les conditions suivantes :
    - Conversations stockées en Europe.
    - Non-entraînement des modèles sur les conversations.
    - Délais de rétention des données connus / non rétention
    - L'IA Act full compliance est recherchée mais non requise : Codexplore Lab ne peut garantir une conformité complète à l'IA Act, notamment en raison de l'opacité de certains acteurs sur les données d'entraînement.
    - Le client final reste maître de l'arbitrage entre performance et conformité IA Act.
    - Codexplore Lab a un devoir de conseil et une obligation de moyens pour garantir la sécurité des échanges via son système de filtres.

Gouvernance des données

- Chaque client dispose d’un registre des traitements et des durées associées.
- Ce registre peut être audité par les autorités compétentes (CNIL, DNE) ou par le délégué à la protection des données de l’établissement.
- Les utilisateurs sont informés des durées de conservation dans la politique de confidentialité.
- Ils peuvent exercer leurs droits d’accès, de rectification ou de suppression à tout moment.

Annexes

- Annexe 1 - AIPD-cadre - Plateforme TokiChat
- Annexe 2 - Charte d'engagement moral et de conformité – IA éducative
- Annexe 3 - Schéma de gouvernance des flux de données (HD)
- Annexe 4 - Schéma : Parcours d'un prompt saisi par un apprenant (HD)
- Annexe 5 - Schéma : système multi filtre TokiChat (HD)