Stratégie de Gouvernance du Projet – Chatbot IA & Contrôle d'Accès Biométrique

1. Objectifs de la gouvernance

- Garantir la sécurité des données personnelles collectées (photo, nom, prénom, email).
- Encadrer l'usage de la reconnaissance faciale conformément aux obligations légales.
- Assurer une gestion responsable du cycle de vie des données (collecte, traitement, stockage, suppression).
- Établir une traçabilité des actions critiques sur le système (authentifications, préinscriptions, contrôles d'accès).
- Mettre en place une supervision continue des performances et incidents liés à l'IA.
- Préparer une conformité RGPD stricte et démontrable dès la conception (Privacy by Design).

2. Cadre juridique et conformité RGPD

2.1. Finalité des traitements

- Chatbot IA : assistance aux visiteurs pour poser des questions courantes.
- Formulaire de préinscription : collecte des données personnelles nécessaires à l'entrée en contact avec l'école.
- Reconnaissance faciale : vérification biométrique à des fins de sécurité d'accès aux locaux.

2.2. Base légale

- Consentement explicite pour la préinscription et la reconnaissance faciale (case à cocher, double validation).
- Intérêt légitime de l'établissement pour la sécurisation de l'accès.

2.3. Délégué à la protection des données (DPO)

- Un DPO doit être désigné si l'usage de la biométrie est systématique. Il ou elle supervisera la conformité et la documentation RGPD.

3. Gouvernance technique et sécurité

3.1. Responsabilités techniques

Équipe DevOps :
- Déploiement et surveillance de l'infrastructure GCP, conteneurisation (Docker), sécurisation des secrets.

Équipe Cybersécurité :
- Audits réguliers, détection d'intrusion, gestion des incidents.

Développeurs IA / backend :
- Intégration du modèle LLM, API d'authentification, gestion de la reconnaissance faciale.

Administrateur RGPD :
- Suivi des traitements, rédaction de la documentation RGPD, réponse aux demandes d'accès/suppression.

3.2. Architecture sécurisée (extrait)

- Infrastructure cloud GCP sécurisée.
- Conteneurisation via Docker pour isolation.
- Supervision via Grafana.
- Backend sous FastAPI sécurisé (TLS interne recommandé).
- Secrets gérés via Google Secret Manager.

3.3. Mesures de sécurité à respecter

- Chiffrement TLS des échanges entre services.
- Non-exécution des conteneurs en root.
- Rate limiting sur les endpoints sensibles (authentification, préinscription).
- Logs centralisés via GCP Logging ou Grafana Loki.
- Permissions minimales sur les accès aux données personnelles.

4. Cycle de vie des données

Collecte :
- Consentement explicite requis, champ obligatoire signalé.

Traitement :
- Limité à la finalité déclarée (admission, contrôle d'accès).

Stockage :
- Localisé dans des régions GCP en Europe, chiffré au repos.

Conservation :
- Préinscriptions conservées 12 mois max. Données biométriques supprimées 48h après validation d'entrée.

Suppression / Portabilité :
- Interface de demande utilisateur ou via contact DPO. Réponse en moins de 30 jours.

5. Usage de l'IA et transparence

- Fournir un disclaimer clair indiquant que les réponses du chatbot sont générées automatiquement.
- Journaliser les interactions critiques (ex : réponse automatisée ayant déclenché une action réelle).
- Mettre en place un mécanisme de supervision humaine pour les erreurs ou réclamations.
- Pour la reconnaissance faciale :
  - Explication complète du processus.
  - Option alternative manuelle si refus de traitement biométrique.

6. Journalisation & traçabilité

- Logging des accès :
  - API FastAPI.
  - Prise de photo & comparaison.
  - Accès aux données personnelles.

- Audit trail :
  - Historique des connexions administrateurs.
  - Modification des configurations critiques.

7. Suivi et révision

- Audit de sécurité trimestriel (interne ou externe).
- Mise à jour de la stratégie RGPD en fonction des évolutions réglementaires.
- Révisions annuelles des modèles IA pour biais, performances, dérives.
- Comité de gouvernance projet : réunion mensuelle pour décision stratégique, analyse de risques et feuille de route technique.