

Analyse d'Impact relative à la Protection des Données (AIPD)

Modèle pré-rempli pour les établissements scolaires

Service concerné : EvalIA - Application d'aide à l'évaluation pédagogique avec IA

Version du modèle : 1.0 - 12 février 2026

Note importante

Ce document est un modèle pré-rempli fourni par l'éditeur EvalIA pour faciliter la réalisation de l'AIPD par les établissements scolaires.

L'établissement reste responsable de traitement et doit adapter ce document à son contexte spécifique, le valider avec son DPO académique, et l'inscrire à son registre des activités de traitement.

Les sections marquées [À COMPLÉTER PAR L'ÉTABLISSEMENT] nécessitent une saisie obligatoire.

Informations de l'établissement

Nom de l'établissement : [À COMPLÉTER PAR L'ÉTABLISSEMENT]

Code UAI : [À COMPLÉTER PAR L'ÉTABLISSEMENT]

Adresse : [À COMPLÉTER PAR L'ÉTABLISSEMENT]

Responsable de traitement : [À COMPLÉTER PAR L'ÉTABLISSEMENT - Chef d'établissement]

DPO académique : [À COMPLÉTER PAR L'ÉTABLISSEMENT]

Email DPO : [À COMPLÉTER PAR L'ÉTABLISSEMENT]

Date de réalisation de l'AIPD : [À COMPLÉTER PAR L'ÉTABLISSEMENT]

Date de mise en production prévue : [À COMPLÉTER PAR L'ÉTABLISSEMENT]

1. Description du traitement

1.1 Nature du traitement

EvalIA est une application web d'aide à l'évaluation pédagogique multi-disciplines utilisant l'intelligence artificielle (Google Gemini via Vertex AI). Elle permet aux enseignants de :

Évaluation et correction :

- Générer des barèmes d'évaluation à partir de sujets d'examen
- Extraire, transcrire et améliorer des barèmes existants
- Analyser des copies d'élèves avec notation par compétences (D/A/PA/NA)
- Recevoir des copies via un lien de dépôt sécurisé (suppression automatique 24h après correction)
- Partager les corrections via des liens publics sécurisés
- Suivre la progression des élèves avec chiffrage zero-knowledge des prénoms
- Exporter des rapports PDF professionnels

TeacherStudio (création de ressources) :

- Uploader et indexer des documents sources (RAG)
- Générer des contenus pédagogiques (évaluations, fiches de cours, résumés)
- Générer des visuels pédagogiques (schémas, diagrammes, infographies)
- Configurer des chatbots IA pour les élèves

Exercices interactifs :

- Créer des exercices multi-types (QCM, vrai/faux, association, classement, texte à trous, réponse courte, ouverte)
- Distribuer aux élèves via lien + code d'accès (sans compte élève)
- Animer des sessions en temps réel façon Kahoot (mode Live)

Remédiation et Plans de Travail :

- Générer des parcours de remédiation personnalisés par IA
- Créer des plans de travail multi-activités (pédagogie Freinet) avec 3 parcours de différenciation
- Suivre la progression des élèves en temps réel

1.2 Finalités du traitement

Finalité	Base légale
Évaluation et correction assistée par IA	Exécution du contrat (Plan Établissement)
Génération de barèmes	Exécution du contrat
Création de contenus pédagogiques (TeacherStudio)	Exécution du contrat
Distribution d'exercices aux élèves	Intérêt légitime (mission pédagogique)
Plans de travail et suivi de progression	Intérêt légitime (mission pédagogique)
Remédiation personnalisée par IA	Intérêt légitime (mission pédagogique)

Chatbots pédagogiques pour élèves	Consentement
Suivi longitudinal des élèves	Intérêt légitime (suivi pédagogique)
Gestion des abonnements et facturation	Exécution du contrat

1.3 Personnes concernées

Catégorie	Estimation	Qualité
Enseignants de l'établissement	[À COMPLÉTER PAR L'ÉTABLISSEMENT]	Utilisateurs directs (compte EvalIA)
Élèves	[À COMPLÉTER PAR L'ÉTABLISSEMENT]	Personnes concernées indirectes (pas de compte)
Parents/représentants légaux	[À COMPLÉTER PAR L'ÉTABLISSEMENT]	Informés du traitement

Note : Les élèves n'ont pas de compte EvalIA. Leur interaction se fait via des liens sécurisés (exercices, dépôts de copies, plans de travail) avec authentification par code + prénom.

1.4 Catégories de données collectées

Catégorie	Données	Sensibilité
Identification enseignant	Email, discipline, niveaux enseignés	Standard
Barèmes	Sujets d'examen, critères d'évaluation	Standard
Copies d'élèves (analyse directe)	Contenu de la copie (image/PDF)	Transient — RAM uniquement, jamais stocké
Copies d'élèves (dépôts)	Fichiers uploadés par les élèves	Temporaire — supprimé 24h après correction
Corrections	Notes par compétences, commentaires IA, feedback	Standard
Prénoms élèves (suivi)	Prénom uniquement	Chiffré zero-knowledge (côté client)
Exercices	Contenu, réponses élèves (pseudonyme)	Standard
Plans de travail	Activités, progression (code + prénom)	Standard
TeacherStudio	Sources RAG, contenus générés, chatbots	Standard
Logs techniques	IP, horodatage, user-agent	Standard
Abonnement	Identifiant technique, statut, dates	Standard

1.5 Durées de conservation

Type de données	Durée
Comptes enseignants actifs	Durée de l'abonnement
Comptes après fin de contrat	2 ans d'inactivité puis suppression
Corrections et barèmes	Jusqu'à suppression par l'enseignant ou 2 ans d'inactivité
Copies d'élèves (analyse directe)	Jamais stockées (RAM)
Copies d'élèves (dépôts)	24h après correction
Exercices et réponses	Jusqu'à suppression par l'enseignant
Plans de travail	Année scolaire + 1 an
TeacherStudio	Jusqu'à suppression ou 3 ans maximum
Logs IA	12 mois
Logs d'audit	24 mois

2. Sous-traitant et flux de données

2.1 Sous-traitant principal

Éditeur : Thomas Cavil

Contact : contact.EvalIA@oriantation.fr

Accord de sous-traitance : Signé conformément à l'article 28 du RGPD

2.2 Sous-traitants ultérieurs

Prestataire	Fonction	Localisation	Garanties
Google Firebase	Base de données, authentification, stockage	europe-west1 (Belgique)	DPA Google Cloud
Google Vertex AI	IA générative (Gemini 2.5 Flash/Pro)	europe-west1 (Belgique)	Pas d'entraînement sur données utilisateurs
Vercel	Hébergement frontend et API	Edge européen	DPA Vercel
Sentry	Monitoring erreurs	UE (Francfort, Allemagne)	SOC 2 Type II, PII scrubbing
LemonSqueezy	Paiement, abonnements	USA (Merchant of Record)	PCI-DSS, SCCs Art. 46.2.c

2.3 Flux de données

```
Enseignant / Élève
  ↓
  Navigateur (HTTPS/TLS 1.3)
  ↓
  Vercel (Edge européen) – Frontend + API
  ↓
  Firebase Auth (europe-west1, Belgique)
  ↓
  API Routes (server-side)
  ↓
  Firestore (europe-west1, Belgique) ↔ Vertex AI (europe-west1, Belgique)
  ↓
  Firebase Storage (europe-west1, Belgique) – Dépôts copies et sources RAG
```

Garantie : Toutes les données personnelles et pédagogiques sont traitées et stockées exclusivement au sein de l'**Union Européenne**. Seules les données d'abonnement (email, identifiant technique) transitent vers LemonSqueezy (USA) pour la gestion des paiements, encadrées par les SCCs. Aucune donnée pédagogique ni donnée d'élève n'est transmise hors UE.

3. Analyse des risques

3.1 Contexte spécifique : IA et éducation

Le traitement utilise l'intelligence artificielle dans un contexte éducatif. Ce contexte implique :

- **Règlement IA (AI Act)** : La fonction de correction de copies (analyze-copy) est classée **système à risque élevé** (Annexe III, point 3.b — évaluation des résultats d'apprentissage)
- **RGPD** : Données d'élèves nécessitant protection appropriée
- **Architecture Human-in-the-Loop** : L'enseignant valide, modifie ou rejette chaque proposition IA. L'IA ne prend **aucune décision autonome**.

3.2 Matrice des risques

Risque	Gravité	Vraisemblance	Niveau initial	Mesures	Niveau résiduel
Notation IA erronée	Élevée	Possible	Important	Validation obligatoire par l'enseignant, édition complète possible	Mineur
Biais algorithmiques (lisibilité, style)	Moyenne	Possible	Significatif	Score de lisibilité explicite, notation par compétences standardisée	Mineur

Accès non autorisé aux copies	Élevée	Peu probable	Important	Copies RAM (analyse directe), expiration 24h (dépôts), Firestore rules, HTTPS	Mineur
Profilage non consenti des élèves	Élevée	Peu probable	Important	Prénoms chiffrés zero-knowledge, pas de nom complet, purge automatique	Mineur
Transfert données hors UE (LemonSqueezy)	Moyenne	Certaine	Significatif	SCCs, aucune donnée pédagogique transmise, PCI-DSS	Mineur
Faible technique / fuite de données	Élevée	Rare	Significatif	3703 tests, CSP strict, sanitization, Firestore rules deny-by-default	Mineur

3.3 Impacts potentiels sur les droits et libertés

Impact	Description	Niveau
Préjudice académique	Note incorrecte influençant le parcours scolaire	Moyen (mitigé par validation enseignant)
Atteinte vie privée	Divulgateion de copies ou corrections d'élèves	Élevé (mitigé par chiffrement, RAM, purge)
Discrimination	Biais algorithmiques dans l'évaluation	Moyen (mitigé par compétences D/A/PA/NA)
Perte d'autonomie	Dépendance excessive à la notation IA	Faible (enseignant décideur final)

4. Mesures de sécurité mises en œuvre par l'éditeur

4.1 Sécurité technique

Mesure	Description
Authentification	Firebase Authentication avec vérification email
Autorisation	Règles Firestore strictes (deny by default, isolation userId)
Chiffrement transit	HTTPS/TLS 1.3 systématique
Chiffrement repos	AES-256 (Firebase/GCP)
Chiffrement zero-knowledge	Prénoms élèves chiffrés côté client (serveur ne voit que le chiffré)
Protection XSS	Sanitization (<code>lib/sanitize.ts</code>),

	CSP headers strict
Protection injection prompt	30+ patterns détectés et bloqués
Validation fichiers	Types MIME whitelist, taille max 10 MB
Rate limiting	20-30 requêtes/minute par utilisateur

4.2 Sécurité IA

Mesure	Description
Traitement UE	Endpoints Vertex AI europe-west1 (Belgique)
Non-entraînement	Données non utilisées pour entraîner les modèles Google
Protection prompt injection	Clauses de sécurité dans tous les prompts système
Reproductibilité	Temperature 0, seed 42 (résultats déterministes)
Human-in-the-Loop	Validation obligatoire par l'enseignant pour chaque note

4.3 Gestion des droits

Droit	Mise en œuvre
Accès	Données visibles dans l'interface (corrections, barèmes, exercices)
Rectification	Modification directe dans l'application
Effacement	Suppression de compte et données associées
Portabilité	Export des données sur demande (JSON/CSV)

4.4 Spécificités de protection des données élèves

- **Copies** : traitées en RAM uniquement (analyse directe), supprimées 24h après correction (dépôts)
- **Prénoms** : chiffrement zero-knowledge — le serveur ne peut techniquement pas lire les prénoms en clair
- **Exercices** : accès par code + prénom, pas de compte élève, pas de nom complet
- **Plans de travail** : accès par code + prénom, progression supprimée à la clôture du plan
- **Aucun tracking** : pas de cookies, pas d'analytics, `noindex/nofollow`
- **Tests** : 3703 tests automatisés dont tests de sécurité spécifiques

5. Mesures complémentaires de l'établissement

5.1 Information des personnes concernées

[À COMPLÉTER PAR L'ÉTABLISSEMENT]

- ☐ Information des enseignants (réunion pédagogique / note de service)
- ☐ Information des élèves (document distribué / affichage ENT)
- ☐ Information des parents (courrier / réunion parents / ENT)
- ☐ Mention de l'utilisation de l'IA dans les évaluations

Document d'information utilisé : [À COMPLÉTER PAR L'ÉTABLISSEMENT]

5.2 Formation des utilisateurs

[À COMPLÉTER PAR L'ÉTABLISSEMENT]

- ☐ Formation des enseignants à l'utilisation d'EvalIA
- ☐ Sensibilisation à la vérification systématique des notes IA
- ☐ Consignes pour la protection des données élèves
- ☐ Information sur les limites du système IA

5.3 Procédure de gestion des incidents

[À COMPLÉTER PAR L'ÉTABLISSEMENT]

Référent sécurité établissement : _____

Procédure en cas de violation de données :

1. Notification immédiate à l'éditeur (contact.EvalIA@orientation.fr)
2. Évaluation de la gravité avec le DPO académique
3. Notification CNIL sous 72h si risque élevé
4. Information des personnes concernées si nécessaire

6. Avis du DPO académique

6.1 Avis

[À COMPLÉTER PAR LE DPO ACADÉMIQUE]

- ☐ Favorable sans réserve
- ☐ Favorable avec réserves (détailler ci-dessous)
- ☐ Défavorable (détailler ci-dessous)

Observations :

6.2 Recommandations

[À COMPLÉTER PAR LE DPO ACADÉMIQUE]

7. Décision du responsable de traitement

7.1 Décision

[À COMPLÉTER PAR LE CHEF D'ÉTABLISSEMENT]

Après examen de la présente analyse d'impact et de l'avis du DPO académique :

- ☐ J'autorise le déploiement d'EvalIA dans l'établissement
- ☐ Je reporte le déploiement en attente de mesures complémentaires
- ☐ Je refuse le déploiement

Justification :

7.2 Inscription au registre

- ☐ Traitement inscrit au registre des activités de traitement de l'établissement

Numéro de registre : [À COMPLÉTER PAR L'ÉTABLISSEMENT]

8. Signatures

Chef d'établissement (Responsable de traitement)

Nom et prénom : _____

Date : _____

Signature :

DPO académique

Nom et prénom : _____

Date : _____

Signature :

Annexes

Annexe A - Documents de référence

- Accord de sous-traitance article 28 RGPD (signé avec EvalIA)
- Politique de confidentialité EvalIA (<https://evalia.orientation.fr/politique-confidentialite>)
- Mentions légales et CGU (<https://evalia.orientation.fr/mentions-legales>)
- AIPD complète de l'éditeur (v2.8, disponible sur demande)
- Annexe AI Act EvalIA (v2.0, disponible sur demande)

Annexe B - Contact éditeur

EvalIA

Thomas Caviel - Éditeur

Email : contact.EvalIA@orientation.fr

Site : <https://evalia.orientation.fr>

Annexe C - Historique des révisions

Version	Date	Auteur	Modifications
1.0	[DATE]	[ÉTABLISSEMENT]	Création initiale

Ce modèle a été préparé par EvalIA pour faciliter la conformité RGPD et Règlement IA des établissements scolaires. Il doit être adapté et validé par le responsable de traitement et le DPO académique.