

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

Modèle pré-rempli pour les établissements scolaires

Service concerné : OriAntation - Application d'aide à l'orientation scolaire avec IA

Version du modèle : 1.0 - 17 janvier 2026

Note importante

Ce document est un modèle pré-rempli fourni par l'éditeur OriAntation 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

OriAntation est une application web d'aide à l'orientation scolaire utilisant l'intelligence artificielle. Elle permet aux élèves de :

- Réaliser un test de personnalité et générer un profil d'orientation

- Tenir un journal de bord numérique de leur réflexion
- Explorer 1 000+ métiers et 30 000+ formations
- Interagir avec un chatbot IA disponible 24h/24
- Créer un CV professionnel
- Planifier leur parcours Parcoursup

Les enseignants peuvent :

- Suivre la progression de leurs élèves via un tableau de bord
- Communiquer avec les élèves via une messagerie sécurisée
- Annoter les journaux de bord (carnet de suivi privé)

1.2 Finalités du traitement

Finalité	Base légale
Accompagnement personnalisé à l'orientation	Exécution mission d'intérêt public (Parcours Avenir)
Suivi pédagogique par les enseignants	Exécution mission d'intérêt public
Communication enseignants-élèves	Intérêt légitime (protection des mineurs)
Génération de recommandations par IA	Consentement
Suivi académique (notes)	Consentement spécifique
Génération de CV	Consentement spécifique

1.3 Personnes concernées

Catégorie	Estimation
Élèves (majoritairement mineurs 15-18 ans)	[À COMPLÉTER PAR L'ÉTABLISSEMENT]
Enseignants	[À COMPLÉTER PAR L'ÉTABLISSEMENT]
Personnel de direction	[À COMPLÉTER PAR L'ÉTABLISSEMENT]

1.4 Catégories de données collectées

Catégorie	Données	Sensibilité
Identification	Prénom, nom, email, établissement, classe	Standard
Profil orientation	Réponses questionnaires, centres d'intérêt,	Standard

	spécialités	
Journal de bord	Notes personnelles, réflexions, objectifs	Potentiellement sensible
Données académiques (optionnel)	Notes par matière et trimestre	Standard
Messages	Échanges enseignants-élèves	Potentiellement sensible
Données CV (optionnel)	Téléphone, adresse postale	Standard
Logs techniques	IP, horodatage connexion	Standard

1.5 Durées de conservation

Type de données	Durée
Comptes élèves actifs	Durée de la scolarité
Comptes après départ	1 an puis suppression automatique
Archives messages	4 ans (obligation légale Éducation Nationale)
Logs de sécurité	1 an

2. Sous-traitant et flux de données

2.1 Sous-traitant principal

Éditeur : Thomas Cavil

Contact : contact@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	europe-west1 (Belgique)	DPA Google Cloud
Google Vertex AI	IA générative (Gemini)	europe-west1 (Belgique)	Pas d'entraînement sur données utilisateurs
Netlify	Hébergement frontend	CDN européen	DPA Netlify
Brevo	Emails transactionnels	France	Entreprise française, RGPD

2.3 Flux de données

```
Élève/Enseignant
↓
Navigateur (HTTPS)
↓
Netlify (France/UE) – Frontend
↓
Firebase Auth (europe-west1, Belgique)
↓
Cloud Functions (europe-west3, Francfort)
↓
Firestore (eur3, Francfort) ↔ Vertex AI (europe-west1, Belgique)
```

Garantie : Toutes les données personnelles sont traitées et stockées exclusivement au sein de l'Union Européenne.

3. Analyse des risques

3.1 Contexte spécifique : IA et mineurs

Le traitement utilise l'intelligence artificielle dans un contexte éducatif avec des personnes majoritairement mineures. Ce contexte implique :

- **Règlement IA (AI Act)** : Système à risque élevé (article 6, annexe III - éducation et formation professionnelle)
- **RGPD** : Données de mineurs nécessitant protection renforcée (article 8)

3.2 Matrice des risques

Risque	Gravité	Vraisemblance	Niveau initial	Mesures	Niveau résiduel
Accès non autorisé aux données	Élevée	Peu probable	Important	Auth Firebase, règles Firestore, HTTPS	Mineur
Conseils IA biaisés/erronés	Élevée	Possible	Important	Avertissements UI, pas de décision auto, prompts cadrés	Significatif
Fuite données via faille	Élevée	Rare	Significatif	Traitement UE, chiffrement, DPA Google	Mineur
Contenu inapproprié (messaging)	Élevée	Possible	Important	Filtrage 72 mots-clés, modération IA, limites horaires/volume	Significatif
Divulgaration données CV (téléphone, adresse)	Élevée	Possible	Important	Consentement spécifique, partage optionnel, token sécurisé	Significatif
Vulnérabilité XSS	Élevée	Possible	Important	Sanitization DOMPurify, CSP headers	Mineur

3.3 Impacts potentiels sur les droits et libertés

Impact	Description	Niveau
Atteinte vie privée	Divulgateion informations personnelles (journal, messages)	Élevé
Discrimination	Biais algorithmiques dans recommandations IA	Moyen
Perte d'autonomie	Décisions d'orientation influencées par IA	Moyen
Préjudice psychologique	Contenus inappropriés, stress lié à l'orientation	Élevé (mineurs)

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 (rôle, schoolId, classId)
Chiffrement transit	HTTPS/TLS 1.3 systématique
Chiffrement repos	AES-256 (Firebase/GCP)
Protection XSS	Sanitization DOMPurify, CSP headers
Protection messagerie	Filtrage 72 mots-clés + modération IA Gemini

4.2 Sécurité IA

Mesure	Description
Traitement UE	Endpoints Vertex AI europe-west1 (Belgique)
Non-entraînement	Données non utilisées pour entraîner les modèles
Protection prompt injection	Clauses de sécurité dans tous les prompts
Données non envoyées à l'IA	Email, nom de famille, UID, nom établissement

4.3 Gestion des droits

Droit	Mise en œuvre
Accès	Export JSON/CSV depuis profil
Rectification	Modification directe dans l'application
Effacement	Fonction suppression compte (délai 30 jours max)
Portabilité	Export JSON structuré
Opposition marketing	Désinscription automatique Brevo

4.4 Purge automatique des données

- Marquage automatique des élèves de Terminale (1er juillet)
- Suppression programmée : scolarité + 1 an
- Avertissement email 30 jours et 7 jours avant
- Conservation archives légales : 4 ans (obligation Éducation Nationale)
- Purge automatique mensuelle des archives expirées

5. Mesures complémentaires de l'établissement

5.1 Information des personnes concernées

[À COMPLÉTER PAR L'ÉTABLISSEMENT]

- ☐ Information des élèves (document distribué / affichage ENT)
- ☐ Information des parents (courrier / réunion parents)
- ☐ Information des enseignants (réunion pédagogique)
- ☐ Recueil des consentements pour les mineurs de moins de 15 ans

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 de l'application
- ☐ Sensibilisation aux risques liés à l'IA
- ☐ Consignes pour la messagerie sécurisée

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@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'OrIAntation 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 OrIAntation)

- Politique de confidentialité OriAntation (<https://oriantation.fr/guides/confidentialite.html>)
- Mentions légales et CGU (<https://oriantation.fr/guides/mentions-legales.html>)
- AIPD complète de l'éditeur (disponible sur demande)

Annexe B - Contact éditeur

OrIAntation

Thomas Caviel - Éditeur

Email : contact@oriantation.fr

Site : <https://oriantation.fr>

Annexe C - Historique des révisions

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

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