

Checklist RGD & Sécurité IA

À imprimer ou remplir avec Claude · Base de la note de conformité (pièce 5 du dossier) · Formation certifiante IA — Flore Guffroy, AXIO Formation

Projet : _____ Responsable : _____ Date de validation : _____

1. Données personnelles

Identification des données

Question	Réponse	Action requise
Quelles données sont envoyées à l'IA ?		
Ces données contiennent-elles des infos personnelles ?	Oui / Non	
Si oui, lesquelles ? (nom, email, téléphone, etc.)		
Ces données sont-elles sensibles ? (santé, origine, religion, etc.)	Oui / Non	

Vérifications RGD

- ☐ **Minimisation** : Seules les données strictement nécessaires sont envoyées
- ☐ **Finalité** : L'usage des données est clairement défini et documenté
- ☐ **Base légale** : Une base légale existe (consentement, intérêt légitime, contrat)
- ☐ **Information** : Les personnes concernées sont informées de l'usage IA
- ☐ **Droits** : Les personnes peuvent exercer leurs droits (accès, rectification, suppression)

Actions correctives

Non-conformité identifiée	Action corrective	Responsable	Deadline

2. Transparence

Communication utilisateurs

- ☐ Les utilisateurs savent qu'ils interagissent avec une IA
- ☐ Le périmètre d'utilisation de l'IA est communiqué
- ☐ Les limites de l'IA sont expliquées (pas infaillible)

Communication équipe

- ☐ L'équipe est formée à l'utilisation de l'IA
- ☐ Les bonnes pratiques sont documentées
- ☐ Les interdictions sont clairement listés

Documentation

- ☐ Politique d'usage IA rédigée
 - ☐ Procédures documentées
 - ☐ Registre des traitements mis à jour
-

3. Sécurité des échanges

Protection des données

- ☐ Les échanges avec l'IA sont chiffrés (HTTPS)
- ☐ Aucune donnée sensible en clair dans les prompts
- ☐ Les credentials ne sont jamais partagés avec l'IA
- ☐ Les données de production sont anonymisées pour les tests

Gestion des accès

- ☐ Accès à l'IA limité aux personnes autorisées
- ☐ Comptes nominatifs (pas de compte partagé)
- ☐ Droits d'accès alignés sur les besoins
- ☐ Revue régulière des accès

Logs et traçabilité

- ☐ Les interactions IA sont loggées
 - ☐ Les logs sont conservés [DURÉE]
 - ☐ Les logs sont accessibles pour audit
 - ☐ Procédure d'analyse des logs définie
-

4. Gouvernance

Responsabilités

Rôle	Personne	Responsabilités
Responsable projet IA		Supervision globale
DPO / Référent RGPD		Conformité données
Responsable sécurité		Sécurité technique
Utilisateurs		Respect des règles

Processus de validation

- ☐ Validation humaine requise pour décisions critiques
- ☐ Processus d'escalade défini
- ☐ Cas limites identifiés et documentés

Gestion des incidents

- ☐ Procédure incident IA définie
- ☐ Contact d'urgence identifié
- ☐ Notification DPO prévue si violation données
- ☐ Kill switch disponible (arrêt d'urgence)

5. Fournisseur IA

Due diligence

Question	Réponse	Satisfaisant ?
Où sont hébergées les données ?		Oui / Non
Les données sont-elles utilisées pour entraînement ?		Oui / Non
Certifications sécurité (SOC 2, ISO 27001) ?		Oui / Non
DPA (Data Processing Agreement) signé ?		Oui / Non
Politique de rétention des données ?		Oui / Non

Conformité EU AI Act

Niveau de risque du cas d'usage	Classification
Risque inacceptable	INTERDIT
Risque élevé	Conformité stricte requise
Risque limité	Transparence requise
Risque minimal	Aucune obligation

Notre classification : _____

6. Bonnes pratiques utilisateurs

À faire

- ☐ Vérifier les informations critiques générées par l'IA
- ☐ Anonymiser les données personnelles avant envoi
- ☐ Utiliser des exemples fictifs pour les tests
- ☐ Signaler tout comportement anormal de l'IA
- ☐ Respecter les limites définies

À ne pas faire

- ☐ Envoyer des mots de passe ou credentials
- ☐ Partager des données de santé non anonymisées
- ☐ Utiliser l'IA pour des décisions automatiques impactantes
- ☐ Contourner les garde-fous
- ☐ Faire confiance aveuglément aux réponses

7. Validation finale

Synthèse conformité

Domaine	Conforme	Partiellement	Non conforme
Données personnelles	☐	☐	☐
Transparence	☐	☐	☐
Sécurité	☐	☐	☐
Gouvernance	☐	☐	☐
Fournisseur	☐	☐	☐

Décision

- ☐ **GO** - Conforme, projet validé
- ☐ **GO avec réserve** - Actions correctives en cours
- ☐ **NO-GO** - Non conforme, à retravailler

Signatures

Rôle	Nom	Date	Signature
Responsable projet			
DPO / Référent RGPD			
Direction			

8. Revue périodique

Planning de revue

Fréquence	Prochaine date	Responsable
Revue trimestrielle		
Audit annuel		

Points de revue

- ☐ Nouveaux usages à évaluer
- ☐ Incidents survenus à analyser
- ☐ Évolutions réglementaires à intégrer
- ☐ Feedback utilisateurs à prendre en compte
- ☐ Mise à jour documentation

Template Formation IA - Loony Agency - Août 2026