Analyse d'impact relative à la protection des donnée

Modèle conforme à la méthodologie CNIL (PIA v3) · adapté à un déploiement Scope · version 2026.04.28-v1 · 2026-04-28

1. Contexte et finalité

Le présent document accompagne le Client dans la réalisation d'une AIPD lorsque l'usage de Scope déclenche un des critères de l'article 35 du RGPD (traitement à grande échelle, données vulnérables, surveillance systématique, etc.). Scope met à disposition les éléments à compléter côté responsable de traitement.

Responsable du traitement : À renseigner — raison sociale + adresse + représentant légal.

Délégué à la Protection des Données (DPO) : À renseigner — nom, email, mode de désignation.

Sous-traitant : Amir KELLOUSIDHOUM EI (Scope), SIRET 917 709 024 00017.

2. Description du traitement

À compléter par le Client en s'appuyant sur les éléments factuels suivants, fournis par Scope :

- Finalité principale : transformer un input (brief, audio, document) en livrables structurés (note de cadrage, propale, audit, RFP).
- Catégories de données : voir DPA, article 3.
- Catégories de personnes concernées : voir DPA, article 4.
- Durée de conservation : durée de l'abonnement + 30 jours, hors obligations comptables.
- Destinataires : utilisateurs habilités côté Client, sous-traitants ultérieurs listés en Annexe 3 du DPA.
- Transferts hors UE : encadrés par les Clauses Contractuelles Types (CCT) UE 2021/914.

3. Nécessité et proportionnalité

3.1 Finalités explicites, déterminées et légitimes

Le traitement répond à une finalité opérationnelle bien définie (production de livrables de cadrage). Aucune autre finalité, en particulier publicitaire ou de profilage, n'est poursuivie par Scope.

3.2 Base légale

- Exécution d'un contrat (article 6.1.b RGPD) — relation entre l'utilisateur et son employeur.
- Intérêt légitime du responsable de traitement (article 6.1.f RGPD), à apprécier au cas par cas.

3.3 Minimisation

Le Client est invité à charger uniquement les informations nécessaires au cadrage. Scope ne demande aucune donnée sensible. Une option « Mode IA souverain » permet de restreindre les sous-traitants IA aux fournisseurs UE.

3.4 Qualité des données

Les utilisateurs peuvent éditer, corriger et supprimer les Documents de cadrage à tout moment via l'interface (droit de rectification automatisé, article 16 RGPD).

4. Risques sur la vie privée

4.1 Accès illégitime aux données

- Sources : compromission d'un compte utilisateur, fuite côté sous-traitant.
- Mesures Scope : MFA, audit log, RLS, scope minimum des clés API, alerting Sentry/GlitchTip.
- Vraisemblance : faible. Gravité : significative. Risque résiduel : faible.

4.2 Modification non désirée des données

- Sources : bug applicatif, action malveillante d'un utilisateur interne.
- Mesures Scope : audit log immutable, snapshots Postgres quotidiens, contrôle d'accès par rôle.
- Vraisemblance : faible. Gravité : limitée. Risque résiduel : faible.

4.3 Disparition des données

- Sources : panne d'un sous-traitant, suppression accidentelle.
- Mesures Scope : sauvegardes quotidiennes, réplication multi-AZ, plan de continuité documenté.
- Vraisemblance : très faible. Gravité : significative. Risque résiduel : faible.

5. Mesures complémentaires recommandées

- Activer le SSO Google ou Entra ID dès le tier Team pour centraliser la gouvernance des identités.
- Restreindre l'accès aux exports sensibles via les rôles internes du Client.
- Activer le « Mode IA souverain » sur les comptes Enterprise traitant des contenus régaliens.
- Définir un référent sécurité côté Client pour la coordination des incidents (article 33 RGPD).

6. Validation

Avis du DPO : À compléter (favorable / favorable avec réserves / défavorable).

Décision du responsable de traitement : À compléter (autorisation, conditions, échéances).

Date de réexamen : Au plus tard 24 mois après la mise en service ou en cas de changement substantiel.