

Parcours A-Z : quoi remplir, pourquoi, et dans quel ordre.

Ce document explique le démarrage d'un espace DPO vide. Il sert de repère pour savoir quoi collecter, quoi saisir dans la plateforme, et quel livrable obtenir à chaque étape.

1. Le principe du parcours

La plateforme ne rend pas une organisation conforme avec un seul bouton. Elle transforme des informations réelles en registre, sous-traitants, risques, preuves et plan d'action. Le parcours commence donc par le cadrage, puis avance vers le registre et les contrôles.

Ce que vous donnez

Le contexte de l'organisation : activité, effectif, sites, responsables, outils, traitements et prestataires.

Ce que la plateforme produit

Des fiches de registre, des priorités, des contrôles AIPD, des preuves et un plan d'action.

2. Étape 1 - Cadrage

Le cadrage sert à comprendre le périmètre avant de créer des fiches. Sans cadrage, on ne sait pas qui est responsable, quels outils traitent des données, ni quels services interroger.

- Nom exact de l'organisation.
- Secteur d'activité et effectif approximatif.
- Sites ou entités concernés.
- Responsable légal et contact DPO.
- Adresse de contact RGPD.
- Contacts métiers : RH, DSI, commerce, support, direction.
- Outils utilisés : paie, CRM, messagerie, signature, stockage, support.
- Premiers traitements à créer : RH, clients, prospection, support.

3. Étape 2 - Registre des traitements

Une fiche de registre décrit une activité qui utilise des données personnelles. La première version n'a pas besoin d'être parfaite : elle doit être assez claire pour être vérifiée avec les métiers.

Champ à remplir	Exemple	Pourquoi c'est important
Nom du traitement	Gestion des ressources humaines	Permet d'identifier l'activité auditée.
Finalité	Paie, absences, contrats, obligations sociales	Explique pourquoi les données sont utilisées.

Champ à remplir	Exemple	Pourquoi c'est important
Base légale	Contrat, obligation légale, intérêt légitime	Justifie le traitement au regard du RGPD.
Catégories de données	Identité, coordonnées, données bancaires	Montre le niveau de sensibilité.
Conservation	5 ans après départ	Évite de garder les données trop longtemps.

4. Étape 3 - Sous-traitants

Un sous-traitant est un prestataire qui traite des données pour l'organisation. Chaque outil listé au cadrage doit être vérifié : contrat, pays, DPA, sécurité et date de revue.

- Nom du prestataire et contact privacy.
- Traitement concerné : RH, clients, prospection, support, etc.
- Pays d'hébergement ou de traitement.
- Contrat DPA signé ou manquant.
- Risque : faible, moyen ou élevé.
- Preuve attendue : contrat, clause, audit, politique sécurité.

5. Étape 4 - Risques et AIPD

Les risques ne sont pas une opinion. Ils viennent de critères concrets : données sensibles, volume important, surveillance, décision automatisée, transfert hors UE, accès larges ou conservation floue.

AIPD probable

Traitement avec données sensibles, scoring, surveillance, volume important ou conséquences fortes pour les personnes.

Action simple

Traitement courant avec risques limités, mais preuve ou contrat à compléter.

6. Étape 5 - Plan d'action

Le plan d'action transforme les constats en tâches : qui fait quoi, pour quand, et avec quelle preuve. Une action sans responsable, sans date ou sans preuve attendue n'est pas exploitable.

1. Choisir un responsable.
2. Fixer une échéance.
3. Décrire la preuve attendue.
4. Passer l'action en validation quand la preuve est prête.

7. Checklist de démarrage

- Organisation renseignée.
- Responsable légal identifié.
- Contact DPO renseigné.
- Adresse RGPD connue.
- Services métiers listés.
- Outils principaux listés.
- 3 premiers traitements choisis.
- Sous-traitants critiques notés.
- Points de vigilance notés.
- Premières actions créées.

8. Exemple simple pour Société Lambda

CADRAGE

Secteur : services aux entreprises. Effectif : 42 salariés. Sites : siège social + 2 antennes.

REGISTRE

Premières fiches : gestion RH, gestion clients, prospection B2B, support client.

SOUS-TRAITANTS

Silae, Microsoft 365, HubSpot, DocuSign, SharePoint, Crisp.

PLAN D'ACTION

Vérifier les DPA, clarifier les durées de conservation, documenter le canal de droits RGPD.

Document de travail. Il ne remplace pas l'analyse juridique du DPO, mais sert de trame pour ne pas démarrer à vide.