

Fiche 1 – Initier les processus de gouvernance de la donnée

Objectif détaillé

Structurer et rendre visible l'ensemble du cycle de vie de la donnée signifie :

- **Qualité** : la donnée est exacte, complète, cohérente et à jour.
- **Sécurité** : la donnée est protégée contre les accès non autorisés, la perte et l'altération.
- **Conformité** : le traitement des données respecte le RGPD, les lois locales, et les normes spécifiques au secteur (ex : ISO 27001, HDS pour la santé).
- **Visibilité** : chaque collaborateur concerné sait où se trouve la donnée, qui en est responsable, et comment elle circule.

Impact stratégique attendu : prise de décision fiable, confiance accrue dans les données, réduction des risques juridiques et réputationnels.

Actions à mener

1. Cartographier le cycle de vie des données

- Étapes : **Collecte** → **Stockage** → **Traitement** → **Diffusion** → **Archivage/ Destruction**.
- Outil : schéma visuel (ex : Miro, Lucidchart, PowerPoint simple au début).
- Méthode :
 - Identifier les **sources de données** (ex : CRM, ERP, formulaires web, capteurs IoT).
 - Identifier les **systèmes de stockage** (bases SQL, data lake, fichiers partagés).
 - Identifier les **usages** (reporting, IA, décisionnel, marketing).
 - Identifier les **canaux de diffusion** (BI, API, exports).
 - Identifier les **modalités d'archivage** (durées légales, destruction sécurisée).

2. Associer des responsabilités claires

- Définir pour chaque étape :
 - **Data Owner** (responsable métier de la donnée, ex : directeur marketing).
 - **Data Steward** (responsable opérationnel de la qualité de la donnée).
 - **Data Custodian** (responsable technique de l'infrastructure et de la sécurité).
- Formaliser ces rôles dans un **RACI** (Responsible, Accountable, Consulted, Informed).

3. Définir les règles

- **Qualité** : règles de format (ex : emails valides), règles de complétude (pas de champ vide critique), référentiels de valeurs.
- **Sécurité** : chiffrement des données sensibles, gestion des accès basée sur les rôles, journalisation.

- **Conformité** : respect du RGPD (bases légales, minimisation, droits des personnes, registre de traitement), normes ISO, exigences internes.
- Documenter ces règles dans une **charte de gouvernance des données**.

4. Rédiger une documentation claire

- Formats possibles : Wiki interne (Confluence, Notion), guide PDF, portail de données.
- Contenu minimum :
 - Procédures standards (collecte, mise à jour, suppression).
 - Glossaire métier (qu'est-ce qu'un client actif, un prospect, une transaction).
 - Règles de nommage et d'organisation des fichiers / tables.
- Objectif : **accessible et compréhensible par les métiers, pas seulement les IT.**

5. Mettre en place des outils pour la traçabilité

- Solutions possibles :
 - **Data catalog** (Collibra, Talend, Atlan, Alation, Microsoft Purview).
 - **ETL/ELT traçables** (Informatica, Talend, dbt, Airflow).
 - **Audit log** pour suivre qui a accédé à quoi et quand.
- Automatiser :
 - Historique des transformations de données.
 - Alertes en cas d'anomalies.

Indicateurs de succès

1. **% de processus documentés et validés**
→ Objectif : 80 % des processus critiques documentés après 6 mois.
2. **Taux de conformité réglementaire**
→ Mesure via audit interne/externe (RGPD, normes ISO).
3. **Nombre d'incidents liés à la donnée (avant/après)**
→ Suivi des erreurs de saisie, fuites de données, incohérences dans les rapports.
4. **Délai moyen de mise à disposition d'une donnée fiable**
→ Exemple : passer de 5 jours à 24h pour fournir un rapport fiable aux métiers.

Points de vigilance

1. **Cartographie trop théorique** :
 - Risque : livrer un schéma joli mais inutilisable.
 - Solution : travailler à partir de cas réels (ex : "parcours d'un client du formulaire web jusqu'au CRM").
2. **Manque d'implication des métiers** :
 - Risque : gouvernance perçue comme un projet IT uniquement.
 - Solution : impliquer dès le départ les directions métiers (finance, marketing, RH) dans la définition des règles.
3. **Outils mal adoptés** :

- Risque : déploiement d'un catalogue ou d'un référentiel que personne ne consulte.
- Solution : intégrer la gouvernance dans les processus métier quotidiens (ex : validation obligatoire via workflow).

Bonnes pratiques

1. **Co-construire la cartographie avec les équipes opérationnelles**
→ Organiser des ateliers collaboratifs pour faire émerger les flux de données.
2. **Commencer par un périmètre pilote**
→ Ex : données "client" ou "RH" sur un seul département.
→ Tester la méthodologie, prouver la valeur (KPI concrets), puis élargir progressivement.
3. **Créer une culture de la donnée**
 - Former les collaborateurs (sensibilisation RGPD, bonnes pratiques de qualité).
 - Valoriser les succès (ex : rapport automatisé gagnant 2 jours de travail/semaine).
4. **Mettre en place une gouvernance itérative**
→ Plutôt qu'un gros projet figé, avancer par cycles courts (quick wins + amélioration continue).

Résultat attendu si bien appliqué

- Une **cartographie vivante** des données, lisible par tous.
- Des **responsabilités clarifiées**, évitant les zones grises ("ce n'est pas moi, c'est l'IT").
- Une **réduction mesurable des incidents** liés aux données.
- Une **confiance accrue** des métiers dans les décisions basées sur la donnée.
- Une **maturité de gouvernance** permettant ensuite de passer à des projets plus avancés (IA, analytique temps réel, data mesh).