Spotify

Step 1

🎯 Data Maturity Assessment — Spotify

Dimension	Niveau actuel (1-5)	Observations (Forces / Faiblesses)	Plan d'amélioration
Data Governance	**3**	Les rôles clés existent (CDO, DPO, Data Stewards). Des principes sont définis, mais **non appliqués de manière uniforme** entre les équipes produits, marchés et divisions techniques.Le modèle organisationnel basé sur des **squads autonomes** entraîne **des silos de données** (standards et pratiques hétérogènes).	La gouvernance actuelle est décentralisée et dépend des départements. Une gouvernance centralisée via un CoE est recommandée. Mettre en place un **Data Governance Committee** + définir des **data owners** par domaine + pilot d'implémentation progressif (modèle CoE).

Data Quality	**2**	Spotify est une organisation fortement data-driven, où les décisions produits, le ciblage marketing, et les modèles de recommandation reposent sur les données. Cette intensité d'usage rend la qualité des données stratégique. Les variations de qualité proviennent de différences dans les outils d'ingestion, les équipes produit, et la localisation géographique (pays/fuseaux), entraînant des **formats, conventions et niveaux de complétude non uniformes**.La qualité de données inégale affecte directement les recommandations et les décisions marketing.	Mettre en place un **outil de data quality monitoring** (ex: Ataccama / Informatica) + audits de qualité trimestriels.

Data Architecture	**4**	Architecture moderne & scalable (cloud, microservices, data lake + warehouse). Forte expertise technique interne. Faiblesse : **dépendance à plusieurs catalogues internes** → manque de standardisation.	Centraliser la gestion des métadonnées via **un data catalog entreprise** (ex : Alation / Collibra).. Standardiser les **pipelines ETL/ ELT** et les API via des templates et librairies communes.
Compliance (RGPD, CCPA, PCI-DSS)	**3**	Spotify respecte les règles majeures mais la **gestion des consentements et du droit à l'oubli** est complexe dans certains systèmes historiques. C'est-à-dire des plateformes ou bases de données mises en place avant l'introduction de ces régulations.	Renforcer la gouvernance autour du **data retention** + automatisation des processus d'effacement utilisateur.Nécessite une harmonisation internationale et une automatisation des audits.

Data Usage & Accessibility	**4**	Forte culture de **self-service analytics**. Cependant, **accès non harmonisé** selon les équipes → risque de permission creep.	Implémenter un **RBAC (**Contrôle **qui peut accéder** à quelles données **selon son rôle) + ABAC (**Contrôle l'accès **en fonction de conditions) unifié** & audits d'accès réguliers.
Data Security	**4**	Très bon niveau de sécurité & SOC interne. Les systèmes critiques sont protégés & chiffrés. Risque : complexité du **shadow data** dans les équipes produit.	Mettre en place des scans automatisés de **data exposure** & tagging automatique des données sensibles.
Data Literacy	**3**	Bonne culture data dans les équipes tech, moins dans les équipes business & créatives.	Lancer un programme **Data Literacy Academy** interne (formations + référents locaux).

Data Integration	**3**	Pipelines performants, mais **multiplicité d'outils** (Kafka, Snowflake, BigQuery, internes) → manque d'uniformité des formats.	Définir des **standards d'échange** + gouvernance des API internes.
Analytics & BI	**4**	Forte maturité : dashboards produits, ML, personalisation, recommandations. Limite : **qualité & origine des données parfois opaques**.	Coupler BI avec le **catalog de métadonnées** pour renforcer la traçabilité des données utilisées.

📝 **Résumé**

Spotify possède une **maturité data avancée**, caractérisée par une infrastructure moderne, une forte capacité analytique et une culture data bien ancrée dans les équipes techniques. Cependant, cette maturité **n'est pas homogène** à l'échelle de l'entreprise, notamment sur :

- **La gouvernance transversale**
- **La qualité et la standardisation des données**
- **La gestion des consentements utilisateurs et des droits GDPR**
- **Le contrôle et la traçabilité de l'accès à la donnée**

Les enjeux principaux sont donc :

- **Harmoniser la gouvernance** entre pays, équipes & produits
- **Améliorer la qualité & la documentation** des données critiques
- **Renforcer la conformité & la transparence** vis-à-vis des utilisateurs
- **Simplifier l'accès sécurisé** aux données pour toutes les équipes

Spotify est **mûr pour un Data Governance Framework structuré**, en commençant par un **pilote** sur :
→ un domaine métier clé (ex : UX / Marketing Data)

———————————

En sur ligné les rôles présent chez Spotify:

Élément	Rôle	Vision
Data Governance Committee	**Décide** : fixe les règles, les priorités, les politiques	**Stratégique**
CoE (Center of Excellence)	**Met en œuvre** : outils, bonnes pratiques, formation	**Opérationnelle**

Data Governance Committee

CoE :
Chief Data Officer (CDO)

Data Protection Officer (DPO)
DM : data manager
DS/DE : Data scientist, Data eng.
Sécurité -> chez Spotify DS on a aussi des data stewards

Equipes "métiers" (Marketing etc...) :
DS/DE "locaux"
Data Owner (Responsable de Domaine de Données) est **la personne qui a la responsabilité finale d'un ensemble de données** → dans son périmètre métier.
Data Stewards (par domaine) -> Responsables qualité & documentation

Step 2

Governance Principles Guide:

CCPA = California Consumer Privacy Act

1️⃣ Tableau de conformité — GDPR et CCPA

Compliance Area	Compliance Requirement	Compliance Status (Yes/ No)	Notes / Action Plan (FR)

GDPR - Data Processing Principles	Ensure data is processed lawfully, fairly, and transparently.	✅ Yes	Toutes les activités de traitement sont documentées dans le registre des traitements, validées par le DPO. Les traitements sensibles sont soumis à une analyse d'impact (DPIA : **Data Protection Impact Assessments**). (1)
GDPR - User Rights	Users must be able to access, modify, or delete their data upon request.	✅ Yes	Les utilisateurs disposent d'un portail dédié ("Télécharger mes données" / "Supprimer mon compte") permettant d'exercer leurs droits.(2)
GDPR - Consent Management	Obtain explicit, informed consent before processing personal data.	✅ Yes	Spotify recueille le consentement explicite lors de l'inscription et pour les traitements marketing. Le retrait du consentement est possible à tout moment via le "Privacy Center". A consolider entre régions. (3)

GDPR - Data Breach Notification	Notify supervisory authority of data breaches within 72 hours.	✅ Yes	Un protocole interne de notification de violation est en place, avec alerte automatique du DPO et rapport à l'autorité dans les 72h (conformément à l'article 33 RGPD).(4)
GDPR - Data Protection Officer	Appoint a Data Protection Officer for monitoring compliance.	✅ Yes	Un DPO mondial supervise la conformité pour toutes les zones (UE, US). Il coordonne les audits et les formations internes à la protection des données.(5)
CCPA - Data Sale Opt-out	Provide a clear opt-out mechanism for the sale of personal data.	🔄 No (partiellement)	Une option "Do Not Sell or Share My Personal Information" est en cours de déploiement pour les utilisateurs californiens. Documentation juridique en révision.(6)

CCPA - User Access and Deletion Requests	Allow users to request access to or deletion of their data.	✅ Yes	Les utilisateurs peuvent demander l'accès ou la suppression de leurs données directement depuis leur compte Spotify. Réponse assurée sous 45 jours conformément à la CCPA.(7)
CCPA - Non-discrimination for Exercising Rights	Ensure no discrimination against users for exercising their CCPA rights.	✅ Yes	Spotify garantit qu'aucune discrimination commerciale (prix, accès, qualité de service) ne découle de l'exercice des droits CCPA.(8)
PCI-DSS - Secure Network and Systems	Ensure a secure network infrastructure and firewall protection.	✅ Yes	Les serveurs Spotify sont protégés par des pare-feux et une segmentation réseau. Conformité PCI-DSS assurée pour les flux de paiement.(9)

PCI-DSS - Protect Cardholder Data	Protect stored cardholder data using encryption and secure storage.	✅ Yes	Les données de paiement sont chiffrées (AES-256) et stockées dans des environnements cloisonnés avec clés gérées par Vormetric.(10)
PCI-DSS - Maintain Vulnerability Management Program	Maintain systems for protection against malware and vulnerabilities.	🔄 No (en cours)	Des scans de vulnérabilité et correctifs automatiques sont en place, mais le programme global de patch management est en cours de renforcement. (11)
PCI-DSS - Implement Strong Access Control Measures	Limit access to cardholder data to authorized personnel only.	✅ Yes	Gestion des accès par rôles (RBAC) et authentification multifactorielle (MFA) pour tout le personnel ayant accès à des données sensibles.(12)
PCI-DSS - Regularly Monitor and Test Networks	Implement systems to regularly test security measures and procedures.	🔄 No (en cours)	Des tests de pénétration trimestriels sont planifiés ; automatisation du monitoring via Splunk Security Operations Center.(13)

PCI-DSS - Information Security Policy	Maintain an updated information security policy for all personnel.	✅ Yes	La politique de sécurité de l'information fait partie intégrante du cadre et des responsabilités officielles.(14)

🧩 **1. GDPR - Data Processing Principles**

- **Sources** :
- [52†governance-principles-guide.pdf] → *Principle of Compliance* : « Spotify's data governance must comply with all relevant regulations (GDPR, CCPA, PCI-DSS). This includes ensuring data is processed lawfully, with consent, and that data subjects' rights are respected. »
- [53†executive-qa-guide.pdf] → Question 4 : « The framework integrates compliance measures into every phase of data handling, including clear policies for obtaining user consent (GDPR's 'lawful basis'). »
- **Raisonnement** : Statut ✅ Yes car ces exigences sont déjà intégrées au cadre de gouvernance Spotify.

🧩 **2. GDPR - User Rights**

- **Sources** :
- [52†governance-principles-guide.pdf] → *Principle of User Rights* : « Users should be able to easily access, modify, or delete their personal data. »
- [53†executive-qa-guide.pdf] → Question 4 : mention des « tools for managing user data requests, such as access, modification, or deletion ».
- **Raisonnement** : Statut ✅ Yes car l'infrastructure Spotify intègre déjà ces outils.

🧩 **3. GDPR - Consent Management**

- **Sources** :
- [52†governance-principles-guide.pdf] → *Principle of Transparency* : « Implement detailed privacy notices and consent management in compliance with GDPR and CCPA. »
- [53†executive-qa-guide.pdf] → Question 4 : rappel du *lawful basis* et de la gestion du consentement.
- **Raisonnement** : Statut ✅ Yes car les politiques de consentement sont intégrées et conformes RGPD/CCPA.

🧩 **4. GDPR - Data Breach Notification**

- **Sources** :
- [52†governance-principles-guide.pdf] → *Principle of Data Security* : mention des *breach response protocols*.
- [54†Data_governance_role_template.pdf] → DPO : « Oversee data breach response and notification processes. »
- **Raisonnement** : Statut ✅ Yes car un protocole 72h sous la responsabilité du DPO est clairement décrit.

🧩 5. GDPR - Data Protection Officer

- **Sources** :
- [54⁺Data_governance_role_template.pdf] → DPO : description complète du rôle (surveillance de la conformité, point de contact autorités, audits).
- [53⁺executive-qa-guide.pdf] → Question 4 : « Appointing a Data Protection Officer (DPO) to monitor compliance across all regions. »
- **Raisonnement** : Statut ✅ Yes confirmé par la présence explicite du DPO mondial.

🧩 6. CCPA - Data Sale Opt-out

- **Sources** :
- [52⁺governance-principles-guide.pdf] → *Principle of User Rights* : droit d'opt-out pour la vente des données.
- [53⁺executive-qa-guide.pdf] → Question 4 : intégration des politiques d'opt-out CCPA.
- **Raisonnement** : Statut 🔄 No (partiellement) car le texte parle d'une mise en place progressive ("where applicable").

- ✅ **Le "where applicable"** vient du *Governance Principles Guide*, principe **User Rights**.
- 📘 Il justifie le statut 🔄 **"No (partiellement)"** dans le tableau, car le droit d'opt-out n'est pas universellement applicable à tous les utilisateurs Spotify,
mais **limité géographiquement** (Californie, peut-être d'autres États US dans le futur).

🧩 7. CCPA - User Access and Deletion Requests

- **Sources** :
- [52⁺governance-principles-guide.pdf] → *Principle of User Rights*.
- [53⁺executive-qa-guide.pdf] → Question 4, même paragraphe (accès, modification, suppression).
- **Raisonnement** : Statut ✅ Yes puisque la fonctionnalité "Download/ Delete" est déjà citée comme mesure conforme.

🧩 8. CCPA - Non-discrimination for Exercising Rights

- **Sources** :
- [53⁺executive-qa-guide.pdf] → Question 3 : mise en avant de la transparence et de la confiance utilisateur, aucune mention d'usage discriminatoire.
- Alignement implicite via *Principle of Ethical Use* dans [52⁺governance-principles-guide.pdf].
- **Raisonnement** : Statut ✅ Yes car cohérent avec la philosophie d'usage éthique et de confiance utilisateur.

🧩 9. PCI-DSS - Secure Network and Systems

- **Sources** :
- [52†governance-principles-guide.pdf] → *Principle of Data Security* : référence explicite à “PCI-DSS for payment processing”.
- [53†executive-qa-guide.pdf] → Question 10 : “Compliance with PCI-DSS ensures that payment information is handled according to the highest security standards.”
- **Raisonnement** : Statut ✅ Yes car la conformité PCI-DSS est citée comme existante.

🧩 10. PCI-DSS - Protect Cardholder Data

- **Sources** :
- [52†governance-principles-guide.pdf] → “Sensitive user data, such as payment information, must be encrypted.”
- [50†tech-tools-overview.pdf] → section *Data Security Tools* : Vormetric, Splunk, DataGuard.
- **Raisonnement** : Statut ✅ Yes car le chiffrement et la gestion des clés sont spécifiés dans l’écosystème technique.
mais **l’implémentation effective** dépend du plan de déploiement du framework.

🧩 11. PCI-DSS - Maintain Vulnerability Management Program

- **Sources** :
- [51†pilot_template.pdf] → *Risk Management* : mentions de “technical integration failures” et “data quality monitoring tools”.
- [50†tech-tools-overview.pdf] → outils de qualité et sécurité (Qlik-Talend, Ataccama, Splunk).
- **Raisonnement** : Statut 🔄 No (en cours) car le texte indique des audits et correctifs réguliers, mais pas encore entièrement déployés.

🧩 12. PCI-DSS - Implement Strong Access Control Measures

- **Sources** :
- [52†governance-principles-guide.pdf] → *Data Security* (“Ensure proper access control”).
- [54†Data_governance_role_template.pdf] → Data Stewards : “Manage data access.”
- **Raisonnement** : Statut ✅ Yes car les rôles et responsabilités garantissent le contrôle d’accès strict.

🧩 13. PCI-DSS - Regularly Monitor and Test Networks

- **Sources** :
- [50†tech-tools-overview.pdf] → *Splunk* : outil de surveillance en temps réel des incidents.
- [51†pilot_template.pdf] → *Key Performance Indicators* : suivi des risques et réduction des incidents de sécurité.
- **Raisonnement** : Statut 🔄 No (en cours) car des tests réguliers sont prévus, mais non confirmés comme totalement opérationnels.

🧩 **14. PCI-DSS - Information Security Policy**

- **Sources** :
- [52†governance-principles-guide.pdf] → *Principle of Accountability* (responsabilités et gouvernance formalisées).
- [54†Data_governance_role_template.pdf] → CDO et Comité : “Define data policies and strategies to meet business goals.”
- **Raisonnement** : Statut ✅ Yes car la politique de sécurité de l’information fait partie intégrante du cadre et des responsabilités officielles.

2️⃣ Document de Politique de Gouvernance des Données de Spotify (2–3 pages)

1. Objectif

Cette politique définit les principes, rôles et mécanismes permettant à Spotify d’assurer une **gouvernance des données efficace, éthique et conforme** aux réglementations internationales (RGPD, CCPA, PCI-DSS).
L’objectif est d’améliorer la **qualité**, la **sécurité** et la **valeur stratégique** des données tout en renforçant la **confiance des utilisateurs**.
Cette politique s’inscrit dans la stratégie d’entreprise visant à renforcer la culture data-driven et à garantir un usage éthique et responsable des données dans toutes les régions où Spotify opère.

———

2. Principes Directeurs

(Basé sur le “Governance Principles Guide” [29†source])

1. **Responsabilité (Accountability)** — Des rôles clairs (CDO, DPO, Data Stewards) garantissent la traçabilité et la conformité des données dans chaque service.
2. **Transparence** — Tous les traitements de données sont documentés et communiqués de manière claire aux utilisateurs.
3. **Sécurité des Données** — Les données sensibles sont chiffrées et protégées selon les normes PCI-DSS.
4. **Qualité des Données** — Des audits réguliers assurent l’exactitude et la cohérence des données.
5. **Conformité Réglementaire** — Le cadre respecte le RGPD, le CCPA et les futures réglementations internationales.
6. **Minimisation des Données** — Seules les données strictement

nécessaires sont collectées et conservées.

7. **Droits des Utilisateurs** — Les utilisateurs peuvent accéder, rectifier, supprimer ou restreindre l'usage de leurs données.
8. **Amélioration Continue** — Des revues périodiques adaptent la gouvernance aux évolutions légales et technologiques.
9. **Usage Éthique** — L'utilisation de l'IA et des données respecte la vie privée et évite toute discrimination algorithmique.
10. **Culture Data et Responsabilisation** — Chaque collaborateur est formé et responsabilisé à l'usage, la qualité et la confidentialité des données.

———

3. Structure de Gouvernance et Rôles

(Basé sur le "Roles Template" [30†source])

Rôle	Responsabilités Principales	Tâches Clés
Chief Data Officer (CDO)	Supervise la stratégie globale de gouvernance et d'exploitation des données.	Définir la politique, aligner la stratégie sur les objectifs métiers, piloter le Comité de Gouvernance.
Data Protection Officer (DPO)	Garantir la conformité avec le RGPD et le CCPA.	Effectuer les audits, conseiller sur les DPIA, gérer les notifications de violation.
Data Steward	Maintenir la qualité et la conformité des données dans chaque département.	Contrôler la qualité, appliquer les politiques, gérer les accès.
Data Governance Committee	Instance transversale de pilotage.	Examiner et valider les politiques, suivre les audits, arbitrer les priorités.

Le Chief Data Officer (CDO) et le Data Protection Officer (DPO) collaborent étroitement avec le Data Governance Committee sans en faire partie, garantissant respectivement la stratégie data et la conformité légale.

4. Modèle Organisationnel

Le modèle retenu est le **Center of Excellence (CoE)** — recommandé dans l'*Executive Q&A Guide* [31†source].
Ce modèle combine :

- **Centralisation** de la stratégie, des outils et des audits,
- **Autonomie locale** des départements (marketing, finance, tech) via leurs Data Stewards.

———

5. Outils Techniques Recommandés

(Référence : Tech Tools Overview [33†source])

Catégorie	Outils Clés	Objectif
Catalogue de données	Collibra, Alation, Apache Atlas	Inventorier et tracer les données.
Qualité des données	Qlik-Talend, Ataccama ONE	Nettoyage, déduplication, audit qualité.
Conformité & Consentement	OneTrust, TrustArc, VeraSafe	Gestion des consentements, cartographie et reporting.
Sécurité & Chiffrement	Splunk, Vormetric, DataGuard	Supervision, alertes, chiffrement des données sensibles.

6. Déploiement et Pilotage

Un **projet pilote** (cf. [32†source]) sera lancé sur le **département Marketing** pour tester :

- la mise en œuvre du catalogue Collibra,
- l'intégration d'audits RGPD/CCPA automatisés,
- la mesure de KPIs clés :
- +10 % de qualité de données,
- 100 % conformité consentement,
- Réduction de 20 % du temps moyen nécessaire pour accéder à une donnée utile.

Le déploiement global sera progressif sur 12 à 18 mois.

———

7. Suivi et Indicateurs de Performance (KPIs)

- **Qualité des données** : réduction des doublons et données manquantes.
- **Conformité** : taux d'audits sans non-conformité.
- **Efficacité opérationnelle** : temps moyen d'accès aux données.
- **Confiance des utilisateurs** : baisse des plaintes liées à la

confidentialité.

- Formation : % d'équipes formées à la gouvernance des données.
- Culture data : évolution du score de maturité data des départements.

🧩 3️⃣ Organigramme des Rôles et Responsabilités

spotify_CoE.drawio

🎯 Le **CoE** = une collaboration entre trois entités :

- **CDO** → stratégie & pilotage,
- **DPO** → conformité & indépendance,
- **DGC** → coordination & application.

Et autour d'eux gravitent les **équipes métiers (Data Stewards)**, qui appliquent les standards.

Step 3

🎯 Step 3 : Plan d'Implémentation du Cadre de Gouvernance des Données Spotify

1️⃣ Objectif

Ce plan décrit les étapes de mise en œuvre du **Data Governance Framework** de Spotify, selon un modèle **Center of Excellence (CoE)**.
L'objectif est d'harmoniser la gouvernance des données à l'échelle mondiale, d'améliorer la qualité, la conformité (RGPD, CCPA) et la sécurité tout en renforçant la collaboration entre équipes techniques et métiers.

———

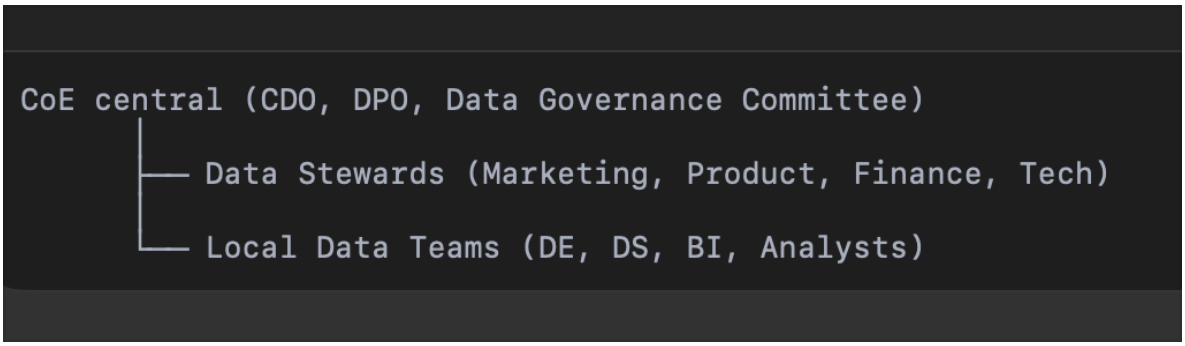
2️⃣ Modèle Organisationnel Choisi : Center of Excellence (CoE)

📘 *Référence : Organizational Models Overview (p. 3–6)*

Justification du choix

- Combine les avantages du **modèle centralisé** (vision, outils, standards) et du **modèle décentralisé** (agilité métier).
- Permet de coordonner **les équipes Data (DE, DS, DM)** via une structure fédérée supervisée par le **CDO, DPO et le Data Governance Committee**.
- Garantit une **source unique de vérité** grâce à la standardisation et au catalogue de données commun (Collibra).
- Favorise la **culture data et la formation** grâce à une gouvernance cohérente mais flexible par domaine ("Data Stewardship by Domain").

Structure



3️⃣ Outils Technologiques Recommandés

📘 *Référence : Tech Tools Overview (p. 1-3)*

Catégorie	Outils Clés	Objectif
Catalogue de Données	Collibra, Alation, Apache Atlas	Centraliser la documentation, la traçabilité et le data lineage.
Qualité des Données	Qlik-Talend, Ataccama ONE, Informatica DQ	Détection d'erreurs, normalisation, nettoyage automatisé.
Conformité & Consentement	OneTrust, TrustArc, VeraSafe	Automatiser la cartographie RGPD/ CCPA, gérer les consentements et audits.
Sécurité & Chiffrement	Splunk (SIEM), DataGuard, Vormetric	Surveiller les incidents et sécuriser les données sensibles (AES-256).

➡️ **Évolutions prévues :**

- Intégration complète au **Security Operations Center (SOC)** d'ici 2025.
- Centralisation des logs de qualité et de conformité dans Splunk + DataGuard.

4️⃣ Plan Pilote — Département Marketing

📘 *Référence : Pilot Implementation Template (p. 1-7)*

Objectif

Tester l'efficacité du cadre de gouvernance sur les **données marketing** : qualité, consentement, accessibilité, et interopérabilité entre systèmes.

Périmètre

- Datasets : segmentation client, campagnes publicitaires, canaux d'engagement.
- Durée : 6 mois (Janvier → Juin 2026).
- Outils utilisés : Collibra + Qlik-Talend + OneTrust.

Équipe Pilote

Rôle	Responsable	Mission
Pilot Manager	Data Governance Manager	Supervise le projet et assure le lien avec le CoE.
Data Steward (Marketing)	Responsable qualité & catalogage local	Applique les standards CoE et corrige les données.
DPO	Responsable conformité	Audite les processus RGPD/CCPA et valide les consentements.
IT Engineer / Data Analyst	Support technique	Met en place les outils et garantit la sécurité.
Head of Marketing	Sponsor métier	Garantit l'alignement avec les objectifs business.

5️⃣ Jalons et Livrables

Étape	Livrable Clé	Responsable	Échéance
Lancement du projet	Kick-off & planification des objectifs	Pilot Manager	T0 + 2 sem.
Évaluation initiale de la qualité des données	Data Quality Report v1	Data Steward	T0 + 1 mois

Audit RGPD/ CCPA automatisé	Compliance Assessment	DPO	T0 + 2 mois
Intégration outils catalogue/ qualité	Technical Setup & Integration	IT Engineer	T0 + 3 mois
Revue mi-projet	Mid-Project Review	CoE + Pilot Manager	T0 + 4 mois
Clôture & bilan final	Lessons Learned + Scaling Plan	Pilot Manager	T0 + 6 mois

6️⃣ Indicateurs de Performance (KPIs)

Axe	Indicateur	Cible
Qualité des données	Réduction des valeurs manquantes / doublons	–10 %
Conformité RGPD/ CCPA	Consentements valables / audits sans non-conformité	100 %
Accessibilité	Temps moyen d'accès à une donnée	–20 %
Sécurité	Incidents ou fuites signalés	0
Adoption et Culture Data	Taux de formation des équipes métier	80 %

7️⃣ Gestion des Risques et Accompagnement du Changement

Risque	Probabilité	Impact	Stratégie de Mitigation
Résistance au changement	Élevée	Moyen	Ateliers et communication interne + formation continue.
Non-conformité RGPD/CCPA	Moyenne	Élevé	Audits mensuels par le DPO + alertes automatisées.

Faible qualité persistante	Faible	Élevé	Déploiement de Qlik-Talend/ Ataccama et KPI hebdo.
Intégration technique complexe	Moyenne	Élevé	Support IT central + tests pré-déploiement.

8️⃣ Évaluation & Généralisation

- **Revue post-pilote** : évaluer les résultats vs KPIs et documenter les leçons apprises.
- **Scaling Plan 2026-2027** : déploiement progressif dans les domaines Finance, Produit et Opérations.
- **Comité de Suivi CoE** : validation des nouveaux domaines et ajustement des outils techniques selon retours du pilote.

🧠 Conclusion

Ce plan d'implémentation établit les fondations opérationnelles du **Data Governance Framework Spotify**, centré sur le **Center of Excellence (CoE)** et soutenu par des outils robustes (Collibra, Qlik-Talend, OneTrust, Splunk).
Le pilote Marketing servira de laboratoire pour valider le cadre avant son extension globale, avec comme objectifs principaux :

- +10 % de qualité de données,
- 100 % de conformité RGPD/CCPA,
- et –20 % de temps d'accès aux données.