DATA GOVERNANCE POLICY DOCUMENT

Spotify - Cadre de Gouvernance des Données

Version : 1.0
Date d'entrée en vigueur : Décembre 2025
Approuvé par : Executive Committee Spotify
Propriétaire : Chief Data Officer : Éric Nguyen
Révision : Annuelle (ou sur évolution réglementaire majeure)

---

1. CONTEXTE ET ENJEUX STRATÉGIQUES

1.1 Situation Actuelle

L'évaluation de maturité Data Management de Spotify révèle un score de 2.7/5 (entre Reactive et Proactive selon Gartner), avec des disparités importantes entre excellence technique (Architecture 3/5, Analytics & BI 3/5) et immaturité organisationnelle (Data Governance 2/5, Compliance 2/5, Data Integration 2/5).

Cette situation crée des risques stratégiques majeurs :

Risques de Conformité :

- Score de conformité réglementaire de 62% (RGPD, CCPA, PCI-DSS)
- Exposition à des amendes jusqu'à 20M€ ou 4% du CA global (RGPD article 83)
- Délais de notification de breach (72h) non garantis
- Processus de consentement non standardisés sur 180+ juridictions

Risques Opérationnels :

- Silos de données entre départements (Marketing, Product, Engineering, Content)
- Vue fragmentée du user journey (discovery → conversion → retention)
- Inefficacité massive : duplication des efforts, délais d'accès aux données

- Qualité des données incohérente impactant les recommandations (cœur de la value proposition)

Risques Concurrentiels :

- Données de qualité variable affectant l'expérience utilisateur
- Attrition potentielle vers concurrents (Apple Music, Amazon Music, Tidal)
- Innovation produit ralentie par fragmentation des données
- Perte d'avantage concurrentiel sur la personnalisation

1.2 Objectif de la Politique

Cette Data Governance Policy établit le cadre unifié pour la gestion des données au sein de Spotify, avec trois objectifs prioritaires :

1. Assurer la conformité réglementaire (RGPD, CCPA, PCI-DSS) et protéger l'entreprise contre les risques juridiques et financiers
2. Garantir la qualité, la sécurité et l'intégrité des données pour maintenir la confiance des 450M+ utilisateurs
3. Optimiser l'exploitation des données en brisant les silos et en créant une organisation data-driven cohérente

Ambition : Atteindre un niveau de maturité de 4/5 (Managed) d'ici 18 mois.

---

2. PRINCIPES FONDAMENTAUX DE GOUVERNANCE

Cette politique repose sur 9 principes directeurs adaptés aux enjeux spécifiques de Spotify :

Principle 1 : Accountability (Responsabilité)

Énoncé : Chaque donnée a un propriétaire identifié responsable de sa qualité, sa sécurité et sa conformité.

Application Spotify :

- Nomination de Data Stewards par domaine métier (User Data, Content Metadata, Marketing Data, Financial Data)
- Reporting direct des Data Stewards au Chief Data Officer
- Responsabilité claire : le Data Steward est l'autorité finale sur son domaine de données
- Accountability inscrite dans les objectifs individuels et évaluations de performance

Actions concrètes :

- Créer une matrice RACI (Responsible, Accountable, Consulted, Informed) pour chaque dataset critique
- Intégrer la data stewardship dans les job descriptions
- Établir des KPIs de gouvernance par Data Steward

Principle 2 : Transparency (Transparence)

Énoncé : Toutes les activités de traitement des données doivent être transparentes, documentées et communiquées aux utilisateurs.

Application Spotify :

- Privacy Notices claires et accessibles sur tous les marchés (180+ pays)
- Documentation complète des traitements (registre article 30 RGPD)
- Communication proactive sur l'utilisation des données (blog, in-app notifications)
- Portail utilisateur "My Data Rights" permettant visibilité et contrôle

Actions concrètes :

- Réécrire les Privacy Policies en langage simple (Plain Language Policy)
- Créer un Data Processing Register centralisé et maintenu à jour
- Publier un rapport de transparence annuel sur les données et la privacy
- Former les équipes Customer Support à expliquer clairement l'utilisation des données

Principle 3 : Data Security (Sécurité des Données)

Énoncé : La sécurité des données est une priorité absolue, avec protection renforcée pour les données sensibles (données personnelles, paiement, contenu propriétaire).

Application Spotify :

- Classification obligatoire de toutes les données (Public, Internal, Confidential, Restricted)
- Chiffrement systématique : at rest (AES-256) et in transit (TLS 1.3)
- Conformité PCI-DSS stricte pour les données de paiement (tokenization, HSM)
- Zero Trust Architecture avec principe de moindre privilège
- Multi-Factor Authentication (MFA) obligatoire pour accès aux données sensibles

Actions concrètes :

- Déployer un Data Classification Framework dans les 3 mois
- Implémenter Data Loss Prevention (DLP) sur tous les endpoints
- Audits de sécurité trimestriels par QSA (Qualified Security Assessor)
- Penetration testing annuel par cabinet externe spécialisé

Principle 4 : Data Quality (Qualité des Données)

Énoncé : Les données doivent être exactes, complètes, cohérentes et à jour pour garantir des décisions fiables et une expérience utilisateur optimale.

Application Spotify :

- Data Quality Framework avec 6 dimensions : Accuracy, Completeness, Consistency, Timeliness, Validity, Uniqueness
- Data profiling systématique sur datasets critiques (user data, content metadata)
- Monitoring continu de la qualité avec alerting automatique
- Priorisation sur données impactant directement l'expérience utilisateur (recommandations)

Actions concrètes :

- Implémenter Great Expectations ou solution équivalente pour data quality testing
- Définir Data Quality KPIs par domaine (target : 95%+ accuracy)
- Data cleansing trimestriel sur metadata de contenus
- Dashboard temps réel de qualité des données pour chaque Data Steward

Principle 5 : Compliance (Conformité Réglementaire)

Énoncé : Toutes les activités data doivent respecter strictement les réglementations applicables (RGPD, CCPA, PCI-DSS, PDPA, etc.) dans les 180+ juridictions où Spotify opère.

Application Spotify :

- Veille réglementaire proactive avec adaptation rapide aux nouvelles lois
- Privacy Impact Assessments (PIA) obligatoires pour tout nouveau traitement à risque
- Data Protection Officer (DPO) renforcé avec équipe régionale (EU, US, APAC, LATAM)
- Audits de conformité semestriels externes
- Formation compliance annuelle obligatoire pour tous les collaborateurs

Actions concrètes :

- Déployer Consent Management Platform (CMP) globale dans les 6 mois
- Implémenter système DSAR automatisé (délais : <15 jours)
- Créer Data Breach Response Plan avec simulations trimestrielles
- Atteindre 90%+ de conformité dans les 12 mois (vs. 42% actuellement)

Principle 6 : Data Minimization (Minimisation des Données)

Énoncé : Ne collecter et conserver que les données strictement nécessaires aux finalités définies et légitimes.

Application Spotify :

- Analyse systématique de la nécessité avant toute nouvelle collecte de données
- Politiques de rétention claires par type de données (logs : 90j, user data : durée compte + 30j, etc.)
- Purge automatique des données expirées (automated data lifecycle management)
- Anonymisation/pseudonymisation par défaut pour analytics et ML training

Actions concrètes :

- Documenter les finalités et bases légales pour chaque collecte
- Implémenter automated data retention policies dans les 6 mois
- Réviser les formulaires de collecte : supprimer les champs non essentiels
- Former Product Managers au Privacy by Design et Data Minimization

Principle 7 : User Rights (Droits des Utilisateurs)

Énoncé : Respecter et faciliter l'exercice des droits des utilisateurs : accès, rectification, suppression, portabilité, opposition, limitation du traitement.

Application Spotify :

- Portail self-service "My Data Rights" accessible 24/7 depuis le compte utilisateur
- Traitement des demandes DSAR dans les délais légaux (max 30 jours RGPD, 45 jours CCPA)
- Export des données dans formats portables et lisibles (JSON, CSV)
- Opt-out simplifié pour marketing, publicité ciblée, partage avec tiers

Actions concrètes :

- Développer portail "My Data Rights" (Q1 2026)
- Automatiser 80%+ des DSAR (access, deletion, portability)
- Former Customer Support : traiter 100% des demandes dans les délais
- KPI : User satisfaction >90% sur exercice des droits

Principle 8 : Continuous Improvement (Amélioration Continue)

Énoncé : La gouvernance des données évolue continuellement pour s'adapter aux changements réglementaires, technologiques et organisationnels.

Application Spotify :

- Revue trimestrielle de la Data Governance Policy par le Data Governance Committee
- Veille technologique sur outils de gouvernance (Data Catalog, MDM, Data Quality)
- Feedback loops avec Data Stewards et utilisateurs finaux
- Benchmarking régulier avec best practices du secteur (Netflix, Spotify, Amazon)

Actions concrètes :

- Data Governance Committee : réunion mensuelle avec ordre du jour structuré
- Baromètre semestriel de maturité data (objectif : +0.5 point tous les 6 mois)
- Participation aux conférences Data Governance (Data Council, CDO Summit)
- Budget innovation : 10% du budget data governance dédié à l'expérimentation

Principle 9 : Ethical Use (Usage Éthique)

Énoncé : L'utilisation des données, notamment via IA et ML, doit être éthique, équitable, non discriminatoire et respectueuse de la vie privée.

Application Spotify :

- AI Ethics Framework pour tous les algorithmes de recommandation et décision automatisée
- Audit de biais algorithmiques semestriel (diversité des recommandations, fairness)
- Explicabilité des décisions automatisées (RGPD article 22)
- Interdiction de profiling sensible (origine ethnique, opinions politiques, santé, etc.)

Actions concrètes :

- Créer un AI Ethics Committee avec représentants Product, Data Science, Legal, DPO
- Implémenter fairness metrics dans les pipelines ML (demographic parity, equal opportunity)
- Documenter les algorithmes : purpose, data sources, logic, potential biases
- Publier un AI Transparency Report annuel

3. CADRE ORGANISATIONNEL DE GOUVERNANCE

3.1 Data Governance Committee

Composition :

- Chief Data Officer (Chair)
- Chief HR Officer (les HR sont indispensables comme Sponsor pour initier la culture Data)
- Data Protection Officer
- Chief Information Security Officer (CISO)
- Head of Engineering
- Legal Counsel
- Marketing Director
- Product Management Representative
- Data Stewards (rotating seat)

Responsabilités :

- Définir et approuver les politiques de gouvernance des données
- Arbitrer les conflits cross-départements sur la propriété et l'usage des données
- Prioriser les initiatives de gouvernance et allouer les ressources
- Monitorer les KPIs de gouvernance et conformité
- Valider les exceptions aux politiques (cas par cas)

Rythme : Réunion mensuelle (2h) + réunions extraordinaires si nécessaire (incident majeur, nouvelle réglementation)

3.2 Rôles et Responsabilités Clés

Chief Data Officer (CDO)

Mission : Piloter la stratégie data et la gouvernance de Spotify, maximiser la valeur business des données tout en assurant conformité et sécurité.

Responsabilités :

- Définir et porter la vision data de l'entreprise
- Présider le Data Governance Committee
- Superviser les Data Stewards et garantir la qualité des données
- Piloter les initiatives Data Quality, Master Data Management, Data Catalog
- Aligner la stratégie data avec les objectifs business
- Reporting mensuel au COMEX sur l'état de la gouvernance et des risques

Reporting : CEO ou COO (niveau Executive Committee). Le **CDO préside** mais ne **valide pas seul** : le Comité garde le pouvoir d’arbitrage collectif

Data Protection Officer (DPO)

Mission : Garantir la conformité avec RGPD, CCPA, PCI-DSS et toutes réglementations data protection applicables.

Responsabilités :

- Superviser la conformité réglementaire (RGPD, CCPA, PDPA, etc.)
- Point de contact avec les autorités de contrôle (CNIL, ICO, etc.)
- Conduire Privacy Impact Assessments (PIA)
- Gérer les Data Subject Access Requests (DSAR)
- Piloter le Data Breach Response Plan
- Former les équipes aux obligations privacy et compliance
- Audits de conformité trimestriels

Reporting : Indépendance organisationnelle - Reporting direct au CEO ou General Counsel

Data Stewards (par domaine)

Domaines définis :

1. User Data Steward : Données utilisateurs, préférences, comportements, démographie
2. Content Metadata Steward : Tracks, albums, podcasts, artists, metadata
3. Marketing Data Steward : Campagnes, engagement, analytics marketing, attribution
4. Financial Data Steward : Subscriptions, billing, payments, revenue data

Responsabilités communes :

- Garantir la qualité, l'exactitude et la complétude des données de son domaine
- Définir les standards de données et les règles de gestion (data dictionary)
- Approuver les accès aux données sensibles de son domaine
- Résoudre les problèmes de qualité et documenter les incidents
- Collaborer avec Engineering pour implémenter les contrôles de qualité
- Représenter son domaine au Data Governance Committee

Reporting : Chief Data Officer

Head of Engineering

Mission : Fournir l'infrastructure technique pour collecter, stocker, traiter et sécuriser les données conformément aux politiques de gouvernance.

Responsabilités :

- Implémenter les contrôles techniques : encryption, access control, monitoring
- Déployer les outils de gouvernance : Data Catalog, MDM, Data Quality platform
- Garantir la scalabilité et la résilience de l'infrastructure data
- Piloter la sécurité des données (collaboration avec CISO)
- Implémenter automated data lifecycle management
- Support technique aux Data Stewards

Reporting : CTO

Legal Team

Mission : Fournir le cadre juridique pour la gouvernance des données et gérer les risques légaux.

Responsabilités :

- Réviser et approuver toutes les politiques de gouvernance des données
- Conseiller sur l'interprétation des réglementations (RGPD, CCPA, etc.)
- Gérer les contrats data avec tiers (vendors, partners, data processors)
- Représenter Spotify en cas de contentieux data-related
- Collaboration étroite avec le DPO

Reporting : General Counsel

3.3 Processus Décisionnels

Principe : Décisions basées sur une matrice d'autorité claire avec escalation si nécessaire.

Type de Décision	Autorité	Escalation si conflit
Définition des standards de qualité par domaine	Data Steward	CDO
Approbation d'accès aux données sensibles	Data Steward + DPO	Data Governance Committee
Lancement de nouveau traitement de données	Data Steward + DPO (PIA)	Data Governance Committee
Exception aux politiques de gouvernance	CDO	Data Governance Committee
Décisions stratégiques data	Data Governance Committee	Executive Committee
Gestion de crise (data breach)	DPO + CISO + Legal	CEO

---

4. MISE EN ŒUVRE ET ROADMAP

4.1 Phase 1 - Fondations (0-6 mois) : Score 2.7 → 3.5

Objectif : Établir les bases de la gouvernance et traiter les risques critiques.

Priorités :

1. Data Governance Committee : Constitution et première réunion (M1)
2. Data Stewards : Nomination et formation (M1-M2)
3. Data Breach Response Plan : Rédaction et simulations (M2-M3) - CRITIQUE
4. Consent Management Platform : Sélection et déploiement (M3-M6) - CRITIQUE
5. DSAR Automation : Système automatisé de gestion des droits utilisateurs (M4-M6)
6. Data Classification : Framework et classification de 80% des données critiques (M3-M6)
7. Registre des traitements : Documentation article 30 RGPD (M1-M4)

Livrable clé : Conformité réglementaire à 70% (vs. 42% actuellement)

4.2 Phase 2 - Standardisation (6-18 mois) : Score 3.5 → 4.2

Objectif : Industrialiser les processus de gouvernance et briser les silos.

Priorités :

1. Data Catalog : Déploiement (Collibra, Alation) pour cartographier toutes les données
2. Master Data Management (MDM) : Implémentation sur entités critiques (users, content, artists)
3. Data Quality Platform : Monitoring continu et alerting (Great Expectations, Monte Carlo Data)
4. Self-Service BI : Démocratisation de l'accès aux données avec gouvernance intégrée
5. Data Lineage : Traçabilité complète des flux de données
6. PCI-DSS Certification : Audit QSA et certification complète
7. AI Ethics Framework : Gouvernance des algorithmes ML

Livrable clé : Conformité à 90% + Vue 360° des utilisateurs + Réduction 50% du time-to-data

4.3 Phase 3 - Excellence (18-36 mois) : Score 4.2 → 4.5+

Objectif : Devenir référence marché en Data Governance et maximiser la valeur business.

Priorités :

1. ISO 27001 & SOC 2 Type II : Certifications sécurité
2. Federated Data Governance : Autonomisation des équipes avec guardrails centralisés
3. Data Products : Création de data products réutilisables et gouvernés
4. Advanced Analytics Governance : Gouvernance des notebooks, expérimentations ML
5. Data Monetization Ethics : Framework pour monétisation éthique des insights
6. Industry Leadership : Publications, conférences, thought leadership

Livrable clé : Spotify reconnu comme leader Data Governance dans le secteur tech/streaming

4.4 KPIs de Gouvernance

KPI	Baseline	Target 6M	Target 18M	Mesure
Data Maturity Score (Gartner)	2.7/5	3.5/5	4.2/5	Évaluation trimestrielle
Compliance Score	64%	80%	90%	Audit externe semestriel
Data Quality Score	N/A	85%	95%	DQ platform metrics
DSAR Response Time	N/A	<20 jours	<10 jours	Système tracking
Data Catalog Coverage	0%	50%	95%	% datasets documentés
Time-to-Data (jours)	~15j	7j	3j	Moyenne demandes d'accès
Data Incidents	N/A	<5/trim	<2/trim	Breach + quality issues
Data Literacy (% trained)	~30%	70%	95%	Tracking formation

---

5. GOUVERNANCE ET RÉVISION DE LA POLITIQUE

5.1 Propriété de la Politique

- Propriétaire : Chief Data Officer
- Approbateur : Executive Committee Spotify
- Contributeurs : Data Governance Committee

5.2 Révision et Mise à Jour

- Révision annuelle obligatoire (Q4 chaque année)
- Révision extraordinaire en cas de :
    - Nouvelle réglementation majeure (ex: nouvelle loi data protection)
    - Changement organisationnel significatif (acquisition, restructuration)

- Incident de sécurité majeur nécessitant révision des processus
- Évolution technologique majeure (nouveau stack data, migration cloud)

5.3 Communication et Formation

- Communication : Publication interne (intranet) + session de lancement pour tous les managers
- Formation obligatoire :
  - Tous les collaborateurs : Data Governance Basics (1h e-learning annuel)
  - Équipes data/tech : Data Governance Advanced (4h workshop annuel)
  - Data Stewards : Data Stewardship Certification (2 jours formation + exam)
  - Management : Data Governance for Leaders (2h session)
  - Tous les managers devront valider la certification Data Literacy niveau 1 sous 12 mois

5.4 Mesure de l'Efficacité

- Dashboard de gouvernance mis à jour mensuellement et présenté au Data Governance Committee
- Audit annuel externe par cabinet spécialisé Data Governance
- Baromètre utilisateurs internes semestriel : satisfaction accès aux données, confiance data quality
- Benchmarking annuel vs. peers (Netflix, Amazon, Google) sur maturité data

---

Intégration du AI Governance Framework

1. Objectif

L'**AI Governance Framework** constitue une extension directe du dispositif de gouvernance des données de Spotify.
Il vise à garantir que tous les systèmes d'intelligence artificielle et de machine learning développés ou utilisés par Spotify soient :

- conformes aux réglementations applicables (RGPD, CCPA, futur **AI Act européen**),
- transparents et explicables,
- exempts de biais discriminatoires,
- alignés avec les principes éthiques et de respect de la vie privée définis par l'entreprise.

---

2. Gouvernance et articulation organisationnelle

L'AI Governance est intégrée au sein du dispositif global via les interactions suivantes :

Instance / Rôle	Responsabilité clé
AI Governance Committee	Supervise la conformité, l'éthique et la performance des modèles IA ; valide les audits de biais et les plans de remédiation.
Chief Data Officer (CDO)	Pilote la stratégie IA responsable et s'assure de l'alignement entre la politique Data et les pratiques IA.
Data Protection Officer (DPO)	Garantit la conformité réglementaire des modèles (protection des données, minimisation, explicabilité).
Data Science & MLOps Teams	Documentent les modèles (Model Cards), suivent les métriques d'équité et de dérive (bias, drift) et remontent les alertes au Comité IA.

---

3. Processus et contrôles

Les modèles IA doivent suivre un cycle de vie contrôlé selon les principes suivants :

1. **Entraînement responsable** – utilisation de données validées, traçables et non biaisées ; anonymisation et minimisation systématiques.

2. **Documentation et traçabilité** – chaque modèle est accompagné d'une *Model Card* précisant les données d'entraînement, la finalité, les métriques de performance et les biais potentiels.

3. **Évaluation éthique et conformité** – audit préalable avant déploiement ; validation conjointe du **DPO** et du **Comité IA**.

4. **Surveillance continue (MLOps)** – contrôle de dérive de modèle (*model drift monitoring*), détection de biais réintroduits, alertes automatiques.

5. **Transparence utilisateur** – communication claire sur la présence d'algorithmes de recommandation ou de décision automatisée.

---

4. Indicateurs de suivi (AI Governance KPIs)

Indicateur	Description	Cible
% de modèles documentés avec Model Card	Niveau de traçabilité des modèles IA	100 %
% de modèles audités éthiquement avant déploiement	Couverture du contrôle AI Governance	90 %
Dérive moyenne des modèles (drift rate)	Mesure de stabilité dans le temps	<5 % par trimestre
Nombre d'incidents IA signalés	Cas de biais, non-conformité ou impact négatif utilisateur	0 incident majeur

5. Alignement stratégique

L'AI Governance Framework s'intègre directement aux **principes 5 (Conformité)** et **9 (Utilisation Éthique)** de la présente Politique.
Il constitue le **volet opérationnel** permettant d'appliquer ces principes aux technologies d'intelligence artificielle, assurant que l'innovation chez Spotify reste **responsable, transparente et conforme**.

6. CONCLUSION

Cette Data Governance Policy constitue le socle fondateur pour transformer la gestion des données chez Spotify. Elle adresse les 3 risques majeurs identifiés :

1. ✅ Risque de conformité : Framework RGPD/CCPA/PCI-DSS pour atteindre 90% de conformité
2. ✅ Risque opérationnel : Briser les silos via Data Stewards, Data Catalog, MDM
3. ✅ Risque concurrentiel : Data Quality Framework pour maintenir l'excellence des recommandations

Message clé : La Data Governance n'est pas une contrainte, c'est un enabler stratégique qui permettra à Spotify de :

- Innover plus rapidement (time-to-market réduit grâce à l'accès facilité aux données)
- Maintenir la confiance de 450M+ utilisateurs (compliance + security + transparency)
- Protéger l'entreprise (conformité réglementaire + réduction des risques)
- Maximiser la valeur des données (qualité + intégration + exploitation optimale)

L'inaction n'est pas une option. Avec un score de conformité de 42% et une exposition à des amendes de 20M€+, Spotify doit agir immédiatement.

Cette politique entre en vigueur dès approbation par l'Executive Committee et engage toute l'organisation Spotify.

Approuvé par :

[Signature CEO Spotify]

[Signature Chief Data Officer]

[Signature Data Protection Officer]

Date d'approbation : [À compléter]

Version : 1.0

Prochaine révision : [Date] + 12 mois