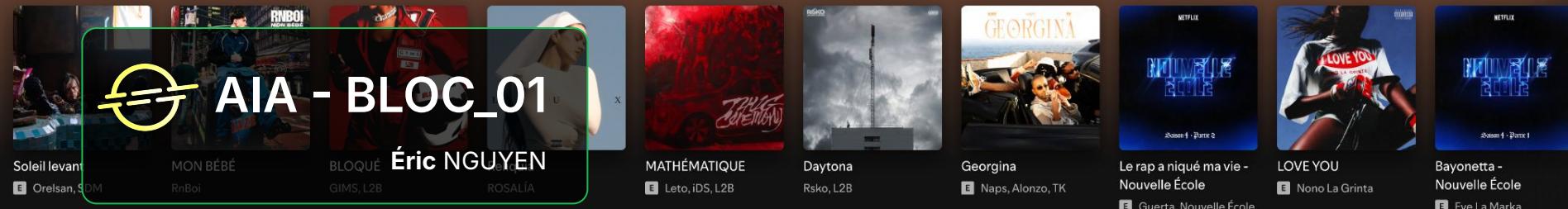


Trending songs

Show all



Popular artists

Show all



Popular albums and singles

Show all





Brief



Présent dans plus de **180 pays avec plus de 450 millions d'abonnés**, Spotify utilise massivement les données pour personnaliser l'expérience utilisateur, concevoir des campagnes marketing ciblées et sélectionner du contenu. Cette dépendance aux données soulève des défis en matière de **gestion, de qualité, de sécurité et de conformité réglementaire**.

Une Data Governance devient nécessaire.

- Data Maturity Assessments
- Compliance Checklist
- Compliance Policy
- Data Governance Implementation



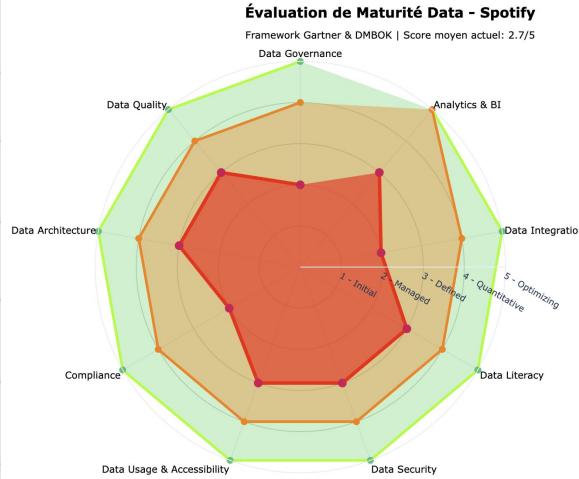
Data Maturity Assessment

DATA MATURITY ASSESSMENT	NIVEAU GARTNER	FORCE	FAIBLESSE	PLAN D'ACTION
Data Governance	2 Reactive	Reconnaissance de l'importance de la gouvernance ; présence d'un DPO et CDO ; volonté managériale d'amélioration ; conscience des enjeux et volonté d'agir.	Absence de framework formel unifié ; pas de politique documentée ; rôles et responsabilités flous ; absence de Data Stewards identifiés ; pas de comité de gouvernance ; processus décisionnels ad-hoc. Les départements gèrent leurs données de façon indépendante, créant des silos et un manque de responsabilité partagée	Établir une politique de gouvernance formelle ; créer un Data Governance Committee ; définir et documenter rôles/responsabilités (Chief Data Officer) ; nommer des Data Stewards par domaine ; implémenter un cadre décisionnel structuré
Data Quality	3 Proactive	Utilise activement les données pour améliorer les recommandations. Conscience de l'importance qualifiée pour les recommandations et les analyses. Culture de l'amélioration	Processus non standardisés et ad-hoc ; incohérences cross-départements ; métadonnées potentiellement obsolètes et erronées (métadonnées et préférences utilisateurs) ; pas de Data Quality metrics formels, absence de data profiling systématique, impact direct sur l'expérience utilisateur	Implémenter un Data Quality Framework (profiling, cleansing, monitoring) ; définir des DQ KPIs mesurables ; automatiser les contrôles qualité ; établir des data quality rules par domaine ; prioriser les datasets critiques (user data, content metadata)
Data Architecture	3 Proactive	Infrastructure technique sophistiquée (data lakes, cloud, bases relationnelles) ; capacités temps réel ; scalabilité démontrée ; architecture moderne	Silos architecturaux entre départements ; fragmentation des sources ; manque d'intégration globale ; absence d'architecture de référence documentée ; pas de data catalog centralisé	Définir une architecture de référence enterprise ; implémenter un data catalog ; standardiser les patrons d'intégration ; documenter les flux de données ; créer une cartographie des systèmes sources
Compliance (GDPR, CCPA, PCI-DSS)	2 Reactive	DPO en place ; conscience des obligations réglementaires ; présence d'une équipe Legal	Risques de non-conformité majeurs sur 180+ juridictions ; processus de consentement non standardisés ; mécanismes DSAR (Data Subject Access Requests) immatures ; documentation des traitements insuffisante ; explications données RGPD (20M€ ou 4% CA) ; délais breach (72h) non garantis	Audit de conformité immédiat RGPD/CCPA ; standardiser les processus de consentement ; implémenter un système DSAR automatisé ; documenter le registre des traitements ; formation compliancy ; renforcer la culture de la conformité et des assessments (PIA). Orienter vers un Privacy By Design
Data Usage & Accessibility	3 Proactive	Usage extrêmement proactif et sophistiqué des données pour améliorer produits/services, culture data-driven ancrée, exploitation ML/IA avancée ; appétit pour l'exploitation data	Silos départementaux bloquant l'accès ; données fragmentées et difficiles d'accès ; absence de self-service BI ; pas de data catalog ; inefficacité opérationnelle ; duplication des demandes ; délais d'accès aux données pénalisants	Implémenter une plateforme de data catalog ; développer des capacités self-service BI ; définir une politique d'accès aux données ; créer des data products réutilisables ; briser les silos par des data domains transverses
Data Security	3 Proactive	Mesures de sécurité existantes ; infrastructure cloud sécurisée ; sensibilisation aux risques	Standards de sécurité non uniformes ; absence de politique centralisée ; classification des données non formalisée ; contrôles d'accès hétérogènes ; risques de breach non quantifiés ; pas de data loss prevention (DLP) systématique	Définir une politique de sécurité data unifiée ; implémenter une classification des données (public, internal, confidential, restricted) ; standardiser les contrôles d'accès (RBAC) ; déployer des solutions DLP ; conduire des audits de sécurité réguliers. S'orienter vers Zero Trust Model
DATA LITERACY	3 Proactive	Culture data-driven forte ; équipes techniques compétentes ; appétence pour les données ; capacités analytiques avancées	Compréhension limitée des principes de gouvernance ; formation compliance insuffisante ; awareness privacy variable ; pas de programme de formation structuré ; compétences data governance faibles au-delà de la tech	Créer un programme de Data Literacy structuré ; former aux principes de gouvernance et compliance ; sensibiliser à la privacy by design ; certifier les Data Stewards ; communication régulière sur les enjeux data
Data Integration	2 Reactive	Reconnaissance du problème ; volonté d'améliorer les synergies ; capacités techniques d'intégration	Fragmentation majeure cross-départements ; vue parcellaire du user journey (discovery → conversion) ; duplication des efforts ETL ; absence de stratégie d'intégration formelle ; pas de MDM (Master Data Management) ; données non réconciliées	Définir une stratégie d'intégration enterprise ; implémenter un MDM pour entités critiques (users, content) ; standardiser les processus ETL/ELT ; créer un golden record strategy ; développer des API data standardisées
Analytics & BI	3 Proactive	Capacités ML/IA avancées ; moteur de recommandation world-class ; exploitation analytique forte ; mesure de performance établie ; culture data-driven	Analyses limitées par les silos de données ; manque de vue 360° utilisateur ; potentiel analytique non pleinement exploité ; insights fragmentés ; collaboration analytique entravée	Créer des data products intégrés pour vue 360° ; développer des analytics cross-fonctionnels ; implémenter une gouvernance des modèles ML ; standardiser les metrics business ; favoriser le partage d'insights. Pourquoi AI Governance Framework (compliance)



Document détaillé

Note global
2,7/5



- Cible long terme (3-5 ans)
- Cible moyen terme (12-24 mois)
- Maturité actuelle (Spotify)



Data Maturity (en bref)



5 Forces (atouts majeurs)

01 Culture data-driven forte et ancrée

L'ADN produit repose sur la donnée (recommandation, personnalisation, analytics produit)

02 Infrastructure technologique robuste et moderne

Architecture cloud (AWS, GCP, Snowflake, Databricks) favorisant la scalabilité, la performance et l'intégration des données.

03 Équipes analytiques et data science matures

Forte expertise interne (ML, AI, BI) et adoption généralisée des outils analytiques dans les équipes produit et marketing.

04 Sécurité et gestion des accès solides

Mise en œuvre de pratiques "Zero Trust", authentification forte, conformité PCI-DSS dans les flux de paiement.

05 Leadership engagé et vision claire du potentiel data

Le CDO et les comités exécutifs soutiennent la gouvernance des données comme levier stratégique de croissance et de conformité.



5 Faiblesses (axes d'amélioration)

01 Gouvernance data fragmentée et non industrialisée

Politiques et processus de gouvernance hétérogènes selon les départements

02 Conformité partielle aux réglementations (RGPD, CCPA)

Gestion manuelle des droits utilisateurs, consentement...

03 Qualité et traçabilité des données inégales

Manque de standardisation, d'audits qualité automatisés et de vision de bout en bout (data lineage).

04 Faible formalisation de l'AI Governance

Absence de cadre éthique documenté pour les algorithmes de recommandation et les modèles de ciblage.

05 Niveau de Data Literacy hétérogène

Les compétences data varient selon les métiers, limitant l'adoption d'une culture de gouvernance cohérente.



Compliance Check List

Score de Conformité Global : 64%

Distribution par statut :

- **✓ YES (Conforme 90-100%)** : 4 items (29%) -
Bases solides établies
- **⚠ PARTIAL (Partiellement conforme 40-89%)** :
9 items (64%) - Majorité à optimiser
- **✗ NO (Non conforme <40%)** : 1 item (7%) -
Security Policy formelle absente

Spotify dispose d'une base de conformité respectable (64%) mais fragmentée, typique d'une scale-up en hyper-croissance. Nous ne sommes pas en crise, mais dans une **fenêtre d'opportunité stratégique** pour passer de "compliant par défaut" à "leader compliance".



Document détaillé

Compliance Area	Requirement Description	Compliance %	Notes	Action Plan
GDPR - Data Processing Principles	Ensure data is processed lawfully, fairly, and transparently.	50% <div style="width: 50%;"></div>	PARTIAL	<ul style="list-style-type: none"> Documentation des traitements nécessaires (Article 30 RGPD) Procédures standardisées entre pays et départements Liens organisationnels créant des incertitudes dans le traitement Transparence et clarté sur les marchés géographiques Altérance de la Politique d'Intimité et Assurances (PIA) systématiques
GDPR - User Rights	User must be able to access, modify, or delete their data upon request.	55% <div style="width: 55%;"></div>	PARTIAL	<ul style="list-style-type: none"> Accès à la demande (manuel et efficace) Transparence et clarté des délais (dès rendant difficile l'exercice des droits) Obligation de traitement non gérant (RGPD) 1 mois maximum Abus de portefeuille service pour l'exercice des droits Processus de vérification d'identité non standardisé Contrôle et suivi des demandes de droits
GDPR - Consent Management	Obtain explicit, informed consent before processing personal data.	80% <div style="width: 80%;"></div>	YES	<ul style="list-style-type: none"> Abus de Consent Management Platform (CMP) unique globalement Transparence et clarté des modalités de consentement entre les 180+ marchés Généralisation insuffisante (pas de consentement légitime pour les données sensibles) Traceur et archivage des preuves de consentement
GDPR - Data Breach Notification	Notify supervisory authority of data breaches within 72 hours.	45% <div style="width: 45%;"></div>	PARTIAL	<ul style="list-style-type: none"> Processus de gestion des incidents de sécurité probablement en place Équipes sécurité et DPO disponibles aux obligations RGPD Infrastructure de détection des incidents de base existante Procédures existantes mal ou non testées
GDPR - Data Protection Officer	Appoint a Data Protection Officer for monitoring compliance.	100% <div style="width: 100%;"></div>	YES	<ul style="list-style-type: none"> Rôle DPO formellement établi et reconnu dans l'organisation Point de contact opérationnel avec les autorités de contrôle Impliquer dans la stratégie de protection de données
CCPA - Data Sale Opt-out	Provide a clear opt-out mechanism for the sale of personal data.	50% <div style="width: 50%;"></div>	PARTIAL	<ul style="list-style-type: none"> Absence de lien "Do Not Sell My Personal Information" visible et accessible Procédure d'opt-out CCPA non remplie correctement Transfert des données vers des tiers non encodé ou inexistant Formation insuffisante des équipes sur la définition CCPA étendue (ex: vente) Communication insuffisante publique sur la problématique non conformes CCPA
CCPA - User Access and Deletion Requests	Allow users to request access to or deletion of their data.	55% <div style="width: 55%;"></div>	PARTIAL	<ul style="list-style-type: none"> Système CCPA actif et probablement fonctionnel (sauf module CCPA opt-out) Format d'export des données non nécessaire "portable" au format JSON Procédures de vérification d'identité peut-être trop lâches ou trop strictes Création et suivi de tracking des métriques CCPA existante Page dédiée CCPA sur le site web probablement absente ou obsolète Politique de non-révélation des données dans les Term & Conditions et Privacy Policy
CCPA - Non-discrimination for Exercising Rights	Ensure no discrimination against users for exercising their CCPA rights.	100% <div style="width: 100%;"></div>	YES	<ul style="list-style-type: none"> Politique de non-discrimination dans les Term & Conditions et Privacy Policy
PCI-DSS - Secure Network and Systems	Ensure a secure network infrastructure and firewall protection.	100% <div style="width: 100%;"></div>	YES	<ul style="list-style-type: none"> Infrastructure cloud sophistiquée mentionnée dans le business case Sécurité réseau probablement gérée par des équipes dédiées (Security Infrastructure) Standards de l'industrie cloud appliqués... - Vérifier la conformité complète PCI DSS v4.0 à la fin de la période prévue
PCI-DSS - Protect Cardholder Data	Protect stored cardholder data using encryption and secure storage.	100% <div style="width: 100%;"></div>	YES	<ul style="list-style-type: none"> Archétype de plateau dédié à la protection des données (best practice) Accès direct et sans détour de données cardholder sensibles (PCI DSS v4.0) Conformité PCI DSS obligatoire principalement aux processus contrôlés Utilisation manuelle du risque en cas de bris de l'infrastructure
PCI-DSS - Maintain Vulnerability Management Program	Maintain systems for protection against malware and vulnerabilities.	65% <div style="width: 65%;"></div>	PARTIAL	<ul style="list-style-type: none"> Scanning de vulnérabilités périodiquement (hors et en cours systématique) Actifs vulnérables peut être non déployé pour tous les systèmes (scanning) Patch management Plan de classification des vulnérabilités avec remédiation planifiée Reporting externe annuel probablement non validé par PCI DSS approprié
PCI-DSS - Implement Strong	Limit access to cardholder data to authorized personnel.	50% <div style="width: 50%;"></div>		<ul style="list-style-type: none"> Classification des données absence... offre de l'identifiant unique et de l'autorisation pour accéder aux données Contrôle d'accès non standardisé aux systèmes et départements Nombreux utilisateurs privilégiés probablement pas appliqués systématiquement Multi Factor Authentication absent (MFA) possiblemement non déployé



Compliance Checklist (en bref)



5 Forces (conformité maîtrisée)

01 Présence d'un DPO structuré et identifié

Le Data Protection Officer est en place, actif dans la gouvernance et en lien avec les autorités de régulation

02 Infrastructure de sécurité conforme PCI-DSS

Architecture cloud et prestataires de paiement certifiés (Stripe/Adyen)

03 Procédure de notification des failles opérationnelle

Chaîne d'escalade en cas de violation de données existante (procédure < 72 h), DPO & Legal coordonnés.

04 Politique de confidentialité publique et transparente

Information claire sur la collecte et l'usage des données ; base solide pour le principe de transparence RGPD/CCPA.

05 Cadre technique de protection robuste (Zero Trust)

Authentification multi-facteur, segmentation réseau, surveillance "Security by design" bien intégrée.



5 Faiblesses (risques et écarts de conformité)

01 Gestion des droits utilisateurs partiellement automatisée

Les demandes RGPD (DSAR) sont traitées manuellement

02 Consentement utilisateur peu granulaire et non centralisé

Le système actuel ne permet pas un choix fin par type de traitement (cookies, publicité, analytics) ; pas de CMP global.

03 Traçabilité incomplète des traitements de données

Absence de registre central uniifié, documentation disparate entre entités régionales.

04 Visibilité insuffisante de l'opt-out CCPA aux États-Unis

Le lien "Do Not Sell My Info" est peu accessible sur les applications mobiles et sites US

05 Audit PCI-DSS irrégulier et reporting non consolidé

Contrôles techniques réalisés, mais manque de plan d'audit annuel et de reporting transverse au Comité Data.



Data Policy (en bref)

- 
- 01 **Vision stratégique** : Faire de la donnée un actif gouverné, conforme et éthique, au service de la personnalisation, de l'innovation IA et de la conformité internationale.
 - 02 **Cadre de gouvernance** : Modèle fédéré de type **Center of Excellence (CoE)**, combinant **Data Mesh** (responsabilisation des domaines) et **standards centralisés** pilotés par le **CDO**.
 - 03 **Principes clés** : Accountability, Transparence, Sécurité, Qualité, Conformité, Minimisation, Droits Utilisateurs, Amélioration Continue et Utilisation Éthique.
 - 04 **Organisation** : Gouvernance structurée autour du **CDO**, du **Comité de Gouvernance des Données**, du **DPO**, du **CoE**, des **Data Stewards** métiers et du **Comité d'Éthique IA**.
 - 05 **Conformité & Sécurité** : Alignement sur **RGPD**, **CCPA** et **PCI-DSS**. Score actuel ≈ **64/100** : cible **80+** via automatisation DSAR, gestion granulaire du consentement et audits réguliers.
 - 06 **Gouvernance de l'IA** : Mise en place d'un **AI Governance Framework** : traçabilité des modèles (Model Cards), audit de biais, monitoring de dérive et conformité anticipée à l'**AI Act**.
 -  [Document détaillé](#)
 - 07 **Feuille de route 2025–2027** : 3 phases : **Fondations** (standardisation & compliance) : **Industrialisation** (outils, CoE, DSAR automatisé) : **Excellence** (gouvernance éthique et IA responsable).



Comparaison des modèles organisationnels

Critères	Centralisé	Embedded (Décentralisé)	Center of Excellence (CoE)
Structure	Une équipe data unique et centrale	Data analysts / scientists directement intégrés dans les départements	Un hub expert central + ressources dans les équipes métiers
Connaissance métier	Faible → éloignement des besoins réels	Excellente car proximité avec les équipes	Bonne car hybridation central/métier
Homogénéité & standards	Forte cohérence, règles unifiées	Standards hétérogènes, fragmentation	Standards centralisés + adoption via relais locaux
Réactivité	Lente : dépend d'une équipe centrale	Très rapide : intégration directe aux projets	Bonne : priorisation au CoE + exécution locale
Coordination globale	Facile	Difficile (silos, duplication)	Bonne : gouvernance fédérée
Innovation / IA / ML	Peut devenir un frein (goulot)	Forte localement mais incohérente globalement	Excellente : mutualisation + autonomie
Scalabilité organisationnelle	Difficile lorsque l'entreprise grandit	Très difficile → escalade du chaos	Meilleure : modèle conçu pour scale
Conformité & Sécurité	Maîtrisée (cadre unique)	Risques élevés (pratiques différentes)	Cadre commun + contrôle fédéré
Coût & efficacité	Rationalisé mais risque de surcharge	Coûts dispersés, doublons	Coût optimisé, mutualisation
Adaptation aux organisations Agile / Squads	Peu adapté	Très adapté	

Légende

Faible

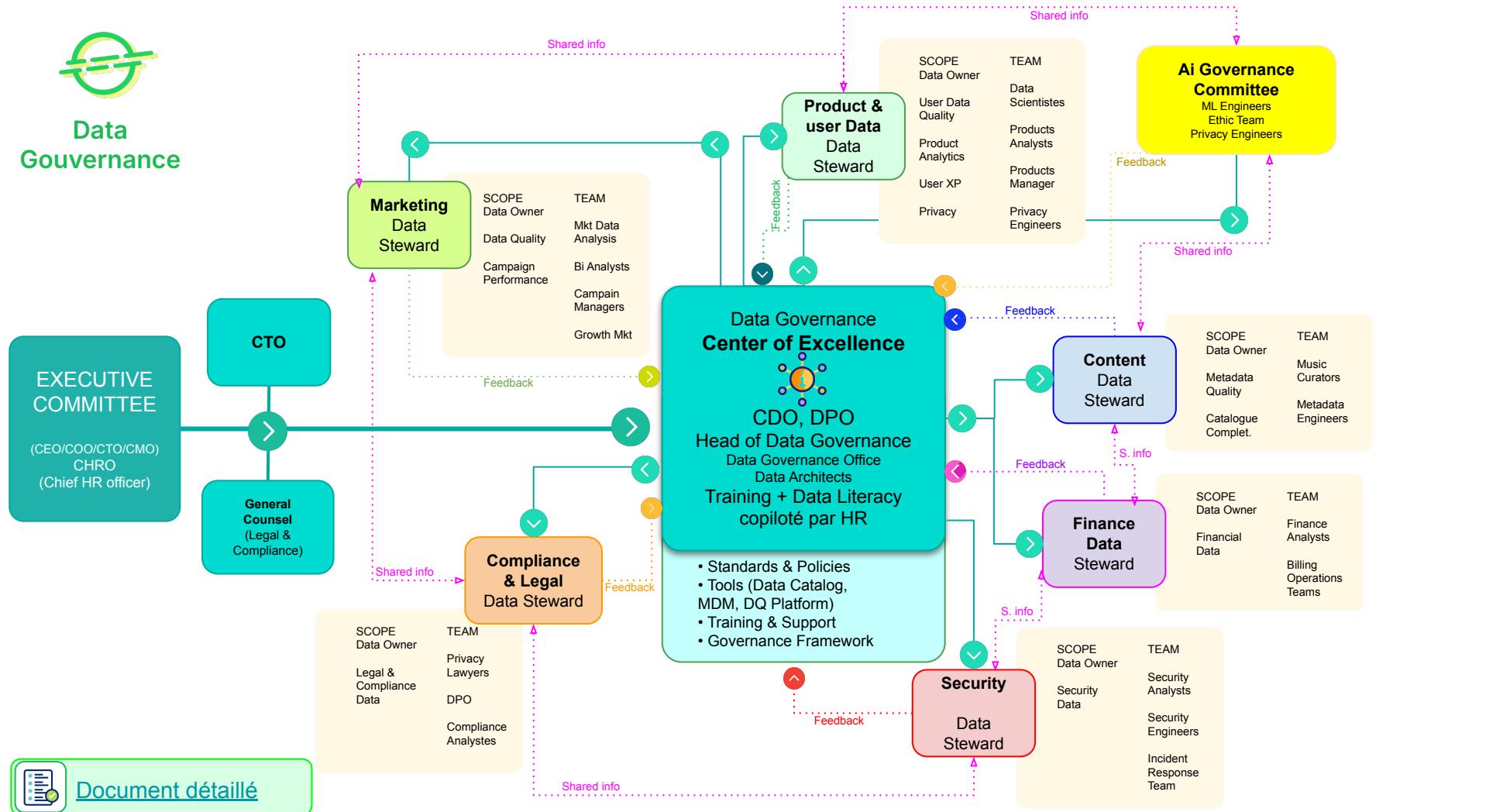
Fort

Idéal

Le modèle CoE est parfaitement adapté à Spotify.



Data Gouvernance





Budget VS Risques

Dépenses

Poste	Montant (€)
Budget Technique	5,05-7,8M
Budget Humain	9,47-13,055M
Formation & Développement	0,55-0,935M
Conseil externe & Audit	1,02-1,58M
Réserve (10%)	1,6-2,3M
TOTAL PROJET (36 mois)	17,69-25,67M€

Humain : Équipe Core - Data Governance Office (10); Équipe Fraud Detection (8), Support & Intégration(8), Consultants...

Risques juridiques directs

Risque	Probabilité	Impact (€)	Espérance (€)
Amendes GDPR (données artistes)	0,4	20-50M	8-20M
Class actions artistes (USA/EU)	0,6	50-200M	30-120M
Amendes régulateurs nationaux (CNC France, etc.)	0,3	10-30M	3-9M
Litiges labels majors	0,5	30-80M	15-40M
TOTAL Risque juridique (3 ans)	-	-	56-189M€

Impact	Estimation basse	Estimation haute
Churn artistes (perte top 1000 artistes → exclusivités concurrents)	-2% revenus = 200M€/an	-5% = 500M€/an
Churn utilisateurs (scandales répétés => -3% MAU)	-150M€/an	-400M€/an
Dépréciation valeur boursière (multiples baisses)	-2Mds€	-8Mds€
Coûts PR & gestion crise	50M€/an	100M€/an
Surcoûts juridiques défensifs	30M€/an	80M€/an
TOTAL Impact business (3 ans)	1,29Mds€	3,54Mds€

Coût total de l'inaction
en 3 ans : 1 à 4 Mds €



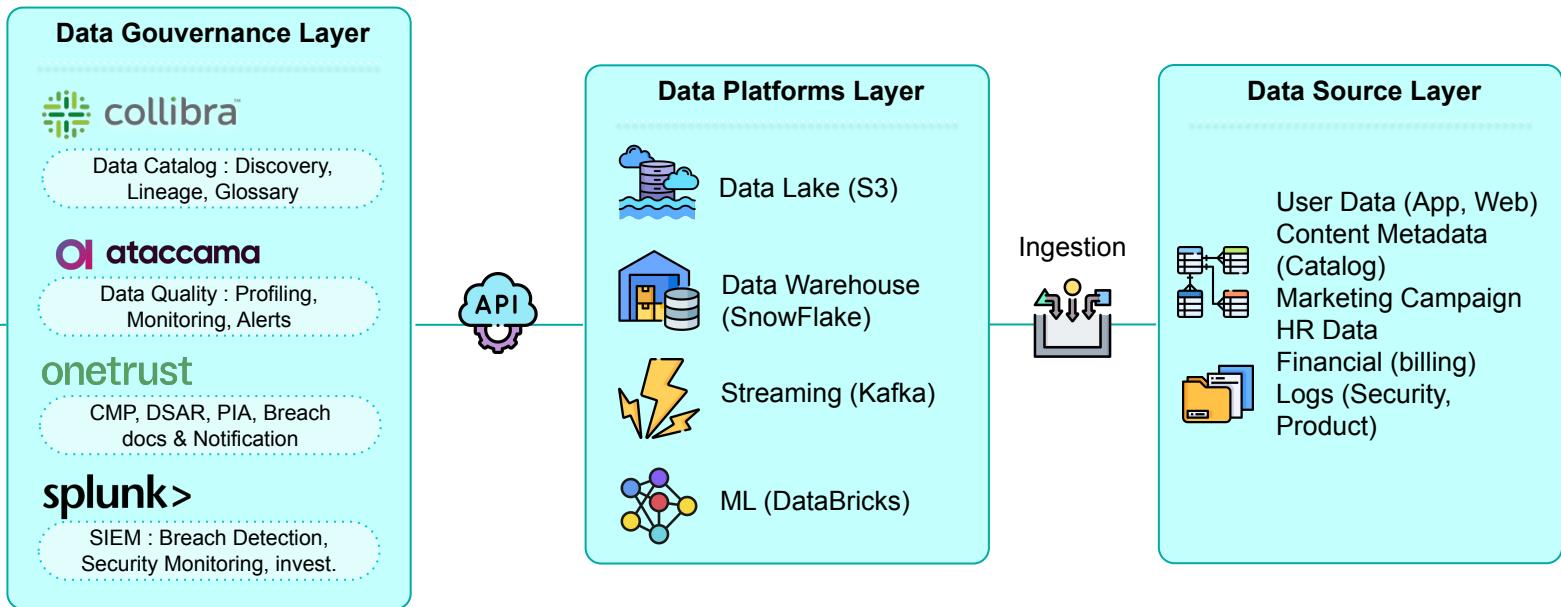
Document détaillé



Stack technologique

USERS

(External Users & Internal Users)



[Document détaillé](#)



Timeline implémentation Data Governance



Phase 1
M1 - M6 : Pilote

collibra
Data Catalog, Data Discovery
Configuration, Connectors, Datasets
Formation Data Stewards
Optimisation Feedback
Data Quality
Configuration DQ, Profiling
Cleansing pipelines + monitoring
Formation Data Steward
Dashboards DQ + alerting
Data Quality
CMP Configuration, DSAR automation,
Formation DPO + Privacy
Security
Configuration
Ingestion logs
Alerting security
Formation SOC Team
Dashboards + incident response testing



Phase 2
M7-M12 : Scale Domain

collibra
ataccama
onetrust
splunk>
Informatica

Data Quality
DQ rules Product/User, DQ rules Content,
DQ rules Financial, Automated,
Compliance
DSAR automation
PIA workflows
Breach incident
Optimisation temps
50-70 users supplémentaires
Security
PCI-DSS monitoring, SOC 24/7 setup
Full coverage, Automated incident
Threat hunting, forensics capabilities
Master Data Management
Configuration MDM, Data matching rules,
Pilot User Master Data (450M users)
Golden records creation
Formation Data Stewards MDM workflows



Phase 2
M13-M18 : Full Deployment

collibra
ataccama
onetrust
splunk>
Informatica

HR & People Data Domain
Compliance & Legal Data domain
Security Data domain
Consolidation, 80-100 catalogues
Data lineage end-to-end
ML Deployment DQ
ML for Data Quality (prédition issues)
DQ rules Security logs (SIEM quality)
Automated remediation (AI-powered)
Compliance
DQ rules HR Data, (employee privacy)
HR systems monitoring (access logs)
Legal systems monitoring
Security
Full Security domain integration
Enterprise-wide coverage (all systems)
Advanced threat detection (ML)
(proactive hunting)
Content
Scale User + Content + Artist Master Data
tracks, albums dedup



Phase 4
M19-M24 :
Optimisation

Data Governance Active
Amélioration continue
Automation avancée
(ML for Data Quality, automated lineage)
Certifications externes
(ISO 27001, SOC 2 Type II)



Phase 5
M25-M36 :
Leadership Industrie

Data Governance Active
Benchmark vs. Netflix, Amazon (peers)
Leadership industrie
publications, conférences
Participation conférences (Data Council, CDO Summit)
Positionnement Spotify comme référence
Data Governance streaming



Conclusion



Gouvernance des données : impératif stratégique



Scandale “**vues simulées**” : accentuer la **Détection de Fraude Amende** : La cour de Stockholm a confirmé **une amende de 5 Mi €** (données personnelles)



EU Music Streaming Act 2026 pourrait être un atout, et donc renforcer la Data Governance permettra la place de Leader (vs Apple)



Any questions ?



Spotify®