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.