Spotify's Data Governance Framework

In this document we provide a unified approach to managing data across all functions, regions, and systems. This policy applies to all data collected, stored, processed, or shared by Spotify globally, and all Spotify teams, including engineering, marketing, content, legal, and product. Non-compliance with this policy will trigger review by the CDO office and may lead to data access restrictions or operational escalation. This policy will be reviewed bi-annually and updated to reflect legal changes, system upgrades, and business expansion.

Objectives and scope

The data governance framework aims to:

- Improve data quality in accordance with ISO 8000. Enhance interoperability across departments.
- Ensure ongoing compliance with GDPR, CCPA, and emerging privacy regulations.
- Build user trust through privacy protection and transparency.
- Improve data accessibility ad integration. Enable consistent, data-driven decisions company-wide.

Data Governance Principles

The following principles serve as the foundation of Spotify's Data Governance Framework. They are designed to ensure that data across the organization is managed ethically, securely, and in compliance with global regulations, while also supporting business innovation and operational excellence. These principles guide all data-related decisions, from collection and processing to quality control and user privacy.

- **Accountability**. Spotify assigns clear data ownership and stewardship across teams. The Chief Data Officer and Data Protection Officer oversee compliance and governance implementation.
- **Transparency**. Users must understand how their data is collected and used. Spotify ensures clear privacy notices and visible consent options in line with GDPR and CCPA.
- **Data Security**. Sensitive data is protected using strong encryption, access controls, and PCI-DSS-aligned practices to safeguard against breaches.
- **Data Quality**. Spotify ensures data is accurate, consistent, and complete, using ISO 8000-aligned standards, audits, and automated validation.
- **Compliance**. All data practices comply with GDPR, CCPA, and other global regulations. Spotify monitors legal changes and updates processes accordingly.
- **Data Minimization**. Only necessary data is collected and retained. Unused or excess data is regularly purged to reduce risk.
- **User Rights**. Spotify provides tools for users to access, correct, or delete their data and opt out of data sharing or sale.
- **Continuous Improvement**. Governance practices are reviewed regularly to adapt to regulatory updates, technology changes, and business needs.
- **Ethical Use**. Spotify commits to responsible data use, including bias-aware AI, ethical automation, and privacy-first product design.

Regulatory Compliance

Spotify's compliance framework integrates legal and ethical requirements using the Compliance Checklist. The key mechanisms are presented in table 1

Table 1: Compliance checklist

Requirement	Regulation	Implementation
Data processing principles	GDPR	Transparent, user-friendly notices in every market
User Rights	GDPR	Portal for access, deletion, and correction requests
Consent Management	GDPR	Consent banners, opt-in/opt-out options for cookies and analytics
Data Breach Notification	GDPR	Incident response procedure and breach dashboard overseen by DPO
Data Protection Officer	GDPR	Appoint a Data Protection Officer for monitoring compliance.
Data Sale Opt-out	CCPA	"Do Not Sell or Share My Info" link available globally
User Access and Deletion Requests	CCPA	Portal for access, deletion, and correction requests
Non-discrimination for Exercising Rights	CCPA	Ensure no discrimination against users for exercising their rights
Secure Network and Systems	PCI-DSS	Implement security measures such as firewalls
Protect Cardholder Data	PCI-DSS	Setup encryption and secure storage
Maintain Vulnerability Management Program	PCI-DSS	Perform regular security audits, ensure systems are up-to-date
Access Control Measures	PCI-DSS	Define access rules for the different data domains and limit access authorized personel
Networks Monitoring and Testing	PCI-DSS	Assess security through pentesting, ensure proper logging
Information Security Policy	PCI-DSS	Create and maintain a definite information security policy, ensure regular training of the teams

Roles and Responsibilities

Effective data governance at Spotify requires clearly defined roles and responsibilities to ensure accountability, compliance, and operational efficiency. This section outlines the key stakeholders involved in managing data across the organization, from strategic oversight to day-to-day data stewardship. Each role plays a critical part in maintaining data quality, protecting user privacy, and supporting informed, data-driven decision-making.

The framework is governed by Spotify's Data Governance Committee, reviewed regularly, and updated to reflect new regulatory changes and updates, along with change in Spotify platform.

Table 2: Roles and Responsibilities summary.

Role	Key Responsibilities
Chief Data Officer (CDO)	Leads data governance strategy, policies, and KPIs.
Data Protection Officer (DPO)	Ensures compliance with GDPR/CCPA, handles breaches, data subject access requests (DSARs).
Head of Engineering	Builds systems to support secure, governed data access.
Marketting Director	Uses the data to drive marketting campaigns or get insight about the platform usage.
Data Stewards	Manage data definitions, quality, access control, and metadata within domains.
Legal Counsel	Advises on compliance risks and regulatory interpretation.
Product & Marketing Leads	Ensure responsible use of user data and accurate analytics.