Governance Princples Guide for Spotify

1. Principle of Accountability

a. Data Stewards: manages and ensures the quality, integrity and proper use of data within domains.

He also monitors and improves data accuracy, completeness, consistency and timeliness. He documents data definitions, source, transformations and usage.

b. Data Protection Officers (DPOs): he ensures that personal data is handled properly. He ensures Sportify complies with data protection laws GDPR for Europe and CCPA for USA.

The DPO trains employees on data protection best practices and raises awareness across Spotify.

He ensures that personal data is protected and that the company respects all privacy regulations.

c. Developer/data analytics: respect governance standards while developing, write technical documentation of the dataflows. Alert in case of an anomaly.

d. Data Owner: take strategic decisions, define access and security of the data, give the right to the users to delete their information.

2. Principle of Transparency

All data processing activities must be transparent to both internal stakeholders and users. Documentation of data lineage, processing logic, and usage must be maintained and accessible.

Implementation guidelines:

- Maintain comprehensive data cataloging with clear lineage tracking
- Provide detailed privacy notices to users in plain language
- Develop a consent management system that allows each user to:
  - give explicit consent (opt-in),
  - view or modify their preferences,
  - withdraw their consent at any time.

Ensure that product, legal, and technical teams collaborate to integrate these elements from the design stage (privacy by design approach).

3. Principle of Data Security

Data security controls must be implemented proportionate to data sensitivity and regulatory requirements. User trust is paramount to our business model.

Implementation guidelines:

- Implement role-based access controls for all data systems
- Encrypt sensitive data both at rest and in transit
- Conduct regular security audits and penetration testing
- Maintain a robust incident response plan for data breaches
- Raise employee awareness of good safety practices and integrate safety by design into the product and service development cycle.

4. Principle of Data Quality

Data must be accurate, complete, consistent, and timely to support reliable analytics and personalized user experiences.

Implementation guidelines:

- Establish data quality metrics for critical datasets such as completeness, accuracy, consistency, freshness and traceability.
- Implement automated quality monitoring and alerting
- Conduct regular data quality audits
- Establish data cleansing procedures for identified quality issues
- Make teams aware of the importance of data quality and integrate automated controls into processing pipelines.

5. Principle of Compliance

All data handling practices must comply with applicable regulations, including GDPR, CCPA, and local laws in our operating regions.

Implementation Guidelines:

- Maintain records of processing activities as required by GDPR
- Implement mechanisms for users to exercise their rights (access, deletion, portability)
- Conduct Data Protection Impact Assessments (DPIAs) for high-risk processing
- Ensure lawful bases for all data processing activities
- Set up a legal watch system to monitor developments in data protection laws worldwide.
- Train teams in regulatory requirements and involve DPOs in projects from the earliest phases.

6. Principle of Data Minimization

Only necessary data should be collected and retained for clearly defined business purposes.

Implementation Guidelines:

- Justify all data collection with a legitimate business purpose

- Implement data retention policies with automated enforcement
- Regularly review and purge unnecessary data
- Design systems with privacy by design principles

7. Principle of User Rights

Data must be used ethically, respecting user privacy and preventing biased outcomes, particularly in algorithmic systems.

Implementation Guidelines:

- Provide a clear interface that allows users to view, correct, or delete their personal data.
- Offer a simple process for submitting data access or deletion requests (Data Subject Access Requests - DSAR).
- Enable users to manage their privacy preferences, including consent and opt-out options for data collection or sale.
- Ensure rigorous tracking of user requests and guarantee their processing within legal timeframes (e.g., one month under the GDPR).
- Promote enhanced transparency on how data is used, particularly through accessible and easy-to-understand privacy policies.

8. Principle of Continuous Improvement

Data governance practices must evolve over time to reflect changes in regulations, technology, and Spotify's operational needs. Regular assessments should be conducted to ensure the governance framework remains effective.

Implementation Guidelines:

- Schedule periodic reviews of the data governance framework (e.g., every 6 to 12 months)
- Incorporate feedback from stakeholders (business teams, IT, legal, etc.) into policy and procedure updates
- Monitor regulatory developments and adapt practices accordingly
- Document all framework updates to ensure traceability and long-term consistency

9. Principle of Ethical Use

Spotify is committed to using data in an ethical manner, ensuring that the use of AI and other data-driven technologies is transparent and respectful of user privacy. Automated decision-making systems must be monitored to prevent and mitigate potential biases.

Implementation Guidelines:

- Include ethical guidelines in all data processing and AI development projects from the outset
- Conduct regular audits of automated systems to detect and address algorithmic bias
- Ensure transparency in how AI-driven decisions are made, especially when they impact users
- Provide clear documentation and explanations for AI models used in user-facing features
- Involve multidisciplinary teams (data scientists, legal, ethics experts) in the validation of high-impact data initiatives