Technical Specification Document

Identity Management Compliance for Amazon Music

Document Version: 1.0

Date Created: [Insert Date]

Last Updated: [Insert Date]

Author: Amazon Music Compliance Team

# Document Control

* Authors: [Full Name(s)]
* Reviewers: [Full Name(s) from Legal, IT Security, and Compliance Teams]
* Approval: [Approver’s Full Name]

# Reference Documents

1. GDPR Compliance Guidelines
2. CCPA Implementation Standards
3. ISO/IEC 27001 Security Management Standards
4. NIST Cybersecurity Framework

# Introduction

This document outlines the system requirements and configurations necessary to ensure Amazon Music’s identity management system complies with GDPR, CCPA, COPPA, and future anticipated privacy regulations through 2025.

# System Overview

## Purpose

Upgrade the identity management system to ensure robust security and compliance with international data protection laws.

## Scope

Includes all systems handling personal identification information (PII) of Amazon Music users across all operational regions.

# Requirements

## Functional Requirements

* Implement AES-256 encryption for all stored PII.
* Support adaptive multi-factor authentication (MFA) for user logins, incorporating contextual factors.
* Allow users to manage their PII (view, update, delete) in compliance with GDPR’s 'Right to be Forgotten' and similar CCPA provisions.

## Non-Functional Requirements

* Achieve 99.999% uptime outside scheduled maintenance.
* Log all PII access and modifications with immutable timestamps.
* Ensure critical operations (e.g., authentication) meet stringent latency requirements (≤ 1 second).

## Compliance Requirements

* All data handling processes must comply with GDPR, particularly Articles on security of processing.
* Facilitate handling of CCPA user requests within the stipulated 45-day period.

# System Architecture

## High-Level Architecture

High-level diagram illustrating data flows, API interactions, and major components. [Insert Diagram: High-Level System Architecture]

## Detailed System Components

Component 1: Biometric Authentication System

* Function: Validates user identity using biometric data (facial recognition, fingerprint).
* Specifications: Handle at least 200,000 transactions per day with failover capability.

Component 2: Encryption Service

* Function: Ensures data encryption both at rest and in transit.
* Specifications: Use TLS 1.3 for transit and AES-256 for data at rest.

# Data Management

## Data Model

Entity-Relationship Diagram showing the user table, PII fields, and relationships. Fields: UserID, EncryptedUsername, HashedPassword, EncryptedPII, ConsentTimestamp, DeletionFlag. [Insert Diagram: ER Diagram of User Data Model]

## Data Flow Diagram

Diagram showing how PII is processed during registration, login, and deletion in compliance with GDPR/CCPA. [Insert Diagram: Data Flow Diagram]

# Security Specifications

* Encryption Protocols: AES-256 for data at rest and TLS 1.3 for data in transit.
* Intrusion Detection System: Real-time monitoring and threat response.
* Regular Security Audits: Frequency and scope of audits to ensure compliance and integrity.

# Testing and Validation

## Test Cases

* Validate encryption integrity of PII at rest.
* Verify latency and accuracy of biometric authentication.
* Test compliance of data deletion processes.

## Test Plan

Phases include unit, integration, and system-level testing using automated tools within a CI/CD pipeline.

# Deployment Strategy

## Initial Rollout

Phased rollout prioritizing compliance in the EU.

## Monitoring and Feedback

Cloud-native monitoring tools to ensure performance metrics are met, with systematic user feedback collection.

# Maintenance and Support

* System Updates: Regular update cycles for security patches and feature improvements.
* User Support: End-user support for privacy concerns and data management queries.

# Conclusion

This document defines the requirements and strategy for ensuring Amazon Music’s identity management system complies with global data protection standards while enhancing security and user trust.

# References

1. GDPR Compliance Guidelines
2. CCPA Implementation Standards
3. ISO/IEC 27001 Security Management Standards
4. NIST Cybersecurity Framework

# Glossary

Definitions for all technical terms and acronyms used in this document.

# Approval

Signatures and dates from key stakeholders validating the document.