

Tableau 1

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".(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)		
GDPR - 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	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	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)		