Compliance Area	Requirement Description	Compliance %	Notes	Action Plan
GDPR - Data Processing Principles	Ensure data is processed lawfully, fairly, and transparently.	50% PARTIAL	Documentation des traitements insuffisante (registre article 30 RGPD absent) • Processus non standardisés entre pays et départements • Silos organisationnels créant des incohérences dans le traitement • Transparence variable selon les marchés géographiques • Absence de Privacy Impact Assessments (PIA) systématiques	1. Créer et maintenir le registre des activités de traitement conforme article 30 2. Documenter les bases légales pour chaque finalité de traitement 3. Standardiser les privacy notices sur l'ensemble des 180+ marchés 4. Implémenter des PIA obligatoires pour tout nouveau traitement à risque 5. Programme de formation RGPD pour tous les collaborateurs traitant des données
GDPR - User Rights	Users must be able to access, modify, or delete their data upon request.	55% PARTIAL	Systèmes de traitement des demandes DSAR (Data Subject Access Request) manuels et inefficaces • Fragmentation des données (silos) rendant difficile l'exhaustivité des réponses • Délais de traitement non garantis (obligation RGPD : 1 mois maximum) • Absence de portail self-service pour l'exercice des droits • Processus de vérification d'identité non standardisé • Pas de workflow automatisé pour la portabilité des données	1. Déployer une plateforme DSAR automatisée de bout en bout 2. Cartographier exhaustivement toutes les sources de données personnelles 3. Créer un portail utilisateur dédié accessible depuis le compte Spotify 4. Définir des SLA internes stricts (cible : 15 jours, max : 30 jours) 5. Implémenter un workflow de validation cross-départements 6. Former les équipes support au traitement des demandes
GDPR - Consent Management	Obtain explicit, informed consent before processing personal data.	80% YES	• Absence de Consent Management Platform (CMP) unifiée globalement • Variabilité des mécanismes de consentement entre les 180+ marchés • Granularité insuffisante (pas de consentement séparé par finalité) • Tracking et archivage des preuves de consentement incomplets • Pas de mécanisme simple et accessible pour retirer le consentement	1. Sélectionner et déployer une CMP enterprise globale 2. Standardiser les bannières de consentement conformes RGPD/ePrivacy 3. Implémenter une granularité par finalité (marketing, analytics, personnalisation, partage tiers) 4. Système d'archivage avec audit trail complet du consentement 5. Révision complète des Privacy Policies et Terms & Conditions 6. Formation intensive des équipes Product, Marketing et Engineering
GDPR - Data Breach Notification	Notify supervisory authority of data breaches within 72 hours.	45% PARTIAL	Processus de gestion des incidents de sécurité probablement en place • Équipes sécurité et DPO sensibilisées aux obligations RGPD • Infrastructure de détection des incidents de base existante Procédures existantes mais non testées	1. Formaliser et documenter le Data Breach Response Plan complet 2. Identifier et former la cellule de crise permanente (DPO, Legal, CISO, Communications, IT) 3. Renforcer les outils de détection automatique (SIEM, DLP, anomaly detection) 4. Préparer et pré-approuver des templates de notification (CNIL, ICO, autres autorités EU + utilisateurs) 5. Organiser des simulations trimestrielles obligatoires (tabletop exercises + technical drills) 6. Établir une hotline d'escalation 24/7 avec procédure claire et testée 7. Cartographier les scénarios de breach par type de données et impact
GDPR - Data Protection Officer	Appoint a Data Protection Officer for monitoring compliance.	100% YES	Rôle DPO formellement établi et reconnu dans l'organisation • Point de contact opérationnel avec les autorités de contrôle • Implication dans la stratégie de protection des données	Évaluer si les ressources de l'équipe DPO sont suffisantes pour 180+ pays • Clarifier l'indépendance organisationnelle et le reporting direct au COMEX • Étendre l'équipe avec des Privacy Managers régionaux • Augmenter le budget et les outils à disposition du DPO
CCPA - Data Sale Opt-out	Provide a clear opt-out mechanism for the sale of personal data.	50% PARTIAL	Absence de lien "Do Not Sell My Personal Information" visible et accessible • Processus d'opt-out CCPA non implémenté techniquement • Tracking des préférences opt-out incomplet ou inexistant • Formation insuffisante des équipes sur la définition CCPA extensive de "sale" • Contrats avec partenaires publicitaires probablement non conformes CCPA	1. Audit juridique approfondi : Spotify "vend"-il des données au sens CCPA ? (définition large) 2. Implémenter un lien "Do Not Sell My Personal Information" visible sur homepage et footer : toutes interfaces US 3. Créer un système centralisé de gestion des préférences opt-out utilisateurs 4. Réviser tous les contrats avec partenaires ad tech (Google, Facebook, etc.) 5. Former les équipes Marketing, Partnerships et Legal sur obligations CCPA 6. Mettre à jour la Privacy Policy avec section CCPA détaillée 7. Implémenter le respect de Global Privacy Control (GPC)
CCPA - User Access and Deletion Requests	Allow users to request access to or deletion of their data.	55% PARTIAL	Système DSAR actuel probablement focalisé GDPR sans module CCPA spécifique • Format d'export des données pas nécessairement "portable" au sens CCPA • Processus de vérification d'identité peut-être trop léger ou trop lourd • Dashboard de tracking des métriques CCPA inexistant • Page dédiée CCPA sur le site web probablement absente ou	1. Étendre le système DSAR (cf. GDPR) avec module CCPA spécifique 2. Implémenter export de données dans formats portables standards (JSON, CSV structurés) 3. Développer un processus de vérification d'identité équilibré (sécurité vs. friction) 4. Créer un dashboard interne de tracking des demandes et métriques CCPA 5. Publier une page web dédiée CCPA avec formulaires accessibles (lien depuis Privacy Policy)
CCPA - Non-discrimination for Exercising Rights	Ensure no discrimination against users for exercising their CCPA rights.	100% YES	• Politique de non-discrimination incluse dans les Terms & Conditions et Privacy Policy	1. Audit périodique des algorithmes ML : vérifier l'absence d'impact négatif de l'opt-out sur la qualité de service 2. Documenter formellement la politique de non-discrimination dans tous les documents légaux 3. Former Product Managers et Data Scientists sur les obligations CCPA anti-discrimination 4. Monitoring continu : aucune corrélation entre exercice des droits et qualité de service 5. Si création de programmes d'incentives futurs : validation Legal + DPO obligatoire
PCI-DSS - Secure Network and Systems	Ensure a secure network infrastructure and firewall protection.	100% YES	Infrastructure cloud sophistiquée mentionnée dans le business case • Sécurité réseau probablement gérée par des équipes dédiées (Security/Infrastructure) • Standards de l'industrie cloud appliqués. 👉 **Vérifier la conformité complète PCI-DSS v4.0 sur la stack de paiement premium.**	Audit PCI-DSS complet de l'infrastructure réseau par Qualified Security Assessor (QSA) 2. Documenter l'architecture réseau complète et les flux de données de paiement 3. Vérifier la segmentation réseau stricte (isolation CDE si données cardholder stockées) 4. Standardiser les configurations de firewall avec revues semestrielles 5. Implémenter IDS/IPS sur périmètre CDE si applicable
PCI-DSS - Protect Cardholder Data	Protect stored cardholder data using encryption and secure storage.	100% YES	• Architecture de paiement découplée via processeurs tiers (best practice) • Aucun stockage direct de données cardholder sensibles (PAN, CVV, dates d'expiration) • Conformité PCI-DSS déléguée principalement aux processeurs certifiés • Réduction massive du risque en cas de breach (tokens inutilisables)	1. Audit annuel : vérifier qu'aucun PAN n'est stocké dans aucun système Spotify 2. Scanner tous les logs et backups : rechercher des patterns de numéros de carte (regex PAN) 3. Vérifier le masquage systématique dans toutes les UI et rapports internes 4. Confirmer la certification PCI-DSS Level 1 active des processeurs de paiement 5. Audit des transmissions : TLS 1.3 obligatoire pour toute communication paiement
PCI-DSS - Maintain Vulnerability Management Program	Maintain systems for protection against malware and vulnerabilities.	65% PARTIAL	• Scanning de vulnérabilités probablement ad-hoc et non systématique trimestriel • Anti-malware peut-être non déployé sur tous les systèmes touchant CDE • Patch management process probablement non formalisé avec SLA • Pas de classification des vulnérabilités avec remédiation priorisée • Pen testing externe annuel possiblement non réalisé par PCI-SSC approved vendor	1. Implémenter scanning de vulnérabilités automatisé trimestriel (minimum) par Approved Scanning Vendor (ASV) 2. Déployer anti-virus/anti-malware sur TOUS les systèmes (serveurs, workstations, containers) 3. Mettre à jour anti-malware automatiquement et scanner régulièrement 4. Créer un patch management process formel avec SLA par criticité (critical : 30j max) 5. Conduire penetration testing annuel par QSA ou PCI-SSC approved vendor 6. Implémenter Web Application Firewall (WAF) sur toutes les applications publiques 7. Scanner les applications custom avec SAST/DAST tools
PCI-DSS - Implement Strong Access Control Measures	Limit access to cardholder data to authorized personnel only.	50% PARTIAL	Classification des données absente : difficile d'identifier précisément le CDE (Cardholder Data Environment) • Contrôles d'accès non standardisés entre systèmes et départements • Principe de moindre privilège probablement pas appliqué systématiquement • Multi-Factor Authentication (MFA) possiblement non déployé universellement pour accès CDE • Revues d'accès périodiques probablement absentes ou non systématiques • Logging des accès au CDE potentiellement incomplet	1. Implémenter classification des données avec identification claire du CDE 2. Inventorier tous les accès actuels au CDE et appliquer principe need-to-know strict 3. Déployer Role-Based Access Control (RBAC) standardisé avec rôles PCI-DSS définis 4. Implémenter MFA obligatoire pour TOUT accès au CDE (personnel interne et remote) 5. Créer des comptes uniques par utilisateur (éliminer comptes partagés ou génériques) 6. Implémenter logging complet de tous les accès au CDE avec alerting 7. Établir revues d'accès trimestrielles obligatoires avec attestation formelle 8. Automatiser la révocation des accès lors des départs (intégration HR)
PCI-DSS - Regularly Monitor and Test Networks	Implement systems to regularly test security measures and procedures.	60% PARTIAL	Absence probable de SIEM centralisé pour monitoring temps réel • Logs probablement non centralisés et pas conservés 1 an (requirement PCI-DSS) • File Integrity Monitoring (FIM) probablement absent sur systèmes critiques CDE • Alerting automatique sur événements suspects probablement limité • Pen testing annuel et quarterly network scans possiblement non réalisés • Incident response testing probablement absent	1. Implémenter un SIEM enterprise (Splunk, QRadar, Sentinel) avec monitoring 24/7 2. Centraliser TOUS les logs des systèmes CDE avec rétention 1 an minimum 3. Déployer File Integrity Monitoring (FIM) sur systèmes CDE critiques 4. Configurer alerting automatique sur 20+ événements de sécurité PCI-DSS 5. Réaliser quarterly vulnerability scans par Approved Scanning Vendor (ASV) 6. Conduire penetration testing annuel (externe et interne) par QSA 7. Implémenter change detection sur configurations critiques 8. Créer un SOC (Security Operations Center) ou externaliser (MSSP)
PCI-DSS - Information Security Policy	Maintain an updated information security policy for all personnel.	30% NO	Aucune Information Security Policy formelle et documentée • Pas de politique spécifique PCI-DSS publiée et communiquée • Absence de programme de sensibilisation sécurité pour tous les employés • Formation PCI-DSS probablement pas dispensée aux personnel ayant accès CDE • Processus d'onboarding sécurité probablement incomplet • Revue annuelle de la politique de sécurité absente	1. Rédiger une Information Security Policy enterprise complète 2. Créer une PCI-DSS Security Policy spécifique (Requirement 12 détaillé) 3. Faire approuver les politiques par le COMEX et publier largement 4. Implémenter programme de sensibilisation sécurité annuel obligatoire (all staff) 5. Former spécifiquement tout personnel ayant accès CDE (formation PCI-DSS dédiée) 6. Intégrer formation sécurité dans onboarding de tous nouveaux employés 7. Faire signer des acknowledgments formels (acceptation des politiques) 8. Réviser et mettre à jour les politiques annuellement 9. Créer des politiques spécifiques : Acceptable Use, Remote Access, Incident Response