| Tableau de conformité réglementaire – Spotify (basé sur le business case) | | | |
|---|---|---|---|
| **Réglementation – Principe** | **Description (FR)** | **Compliance Status (Y/N)** | **Action Plan** |
| GDPR – Principes de traitement des données | Assurer un traitement des données légal, équitable et transparent. | Y | Renforcer la traçabilité et la gouvernance des données. |
| GDPR – Droits des utilisateurs | Permettre aux utilisateurs d'accéder, modifier ou supprimer leurs données. | Y | Automatiser la gestion des demandes d'accès et de suppression. |
| GDPR – Gestion du consentement | Obtenir un consentement clair avant tout traitement de données personnelles. | Y (partiel) | Centraliser la gestion du consentement utilisateur. |
| GDPR – Notification de violation de données | Signaler toute violation de données sous 72 heures à l'autorité compétente. | Y | Tester régulièrement les procédures de notification d'incident. |
| GDPR – Délégué à la protection des données (DPO) | Désigner un DPO pour superviser la conformité. | Y | Assurer le pilotage de la conformité par le DPO. |
| CCPA – Option de refus de vente de données | Offrir un moyen simple de refuser la vente de données personnelles. | Y (partiel) | Clarifier les mécanismes d'opt-out des données personnelles. |
| CCPA – Demandes d'accès ou de suppression des données | Autoriser la demande d'accès ou de suppression des données. | Y | Harmoniser les processus RGPD et CCPA. |
| CCPA – Non-discrimination liée à l'exercice des droits | Éviter toute discrimination liée à l'exercice des droits CCPA. | Y | Formaliser la protection contre la discrimination des utilisateurs. |
| PCI-DSS – Réseau et systèmes sécurisés | Garantir une infrastructure réseau sécurisée avec pare-feu. | Y | Maintenir une infrastructure cloud sécurisée. |
| PCI-DSS – Protection des données de carte | Chiffrer et stocker de manière sécurisée les données de cartes. | Y (implicite) | Protéger les données de paiement par chiffrement et audits PCI-DSS. |
| PCI-DSS – Programme de gestion des vulnérabilités | Maintenir une protection contre malwares et vulnérabilités. | Y | Renforcer la surveillance continue des systèmes de sécurité. |
| PCI-DSS – Contrôles d'accès stricts | Restreindre l'accès aux données de carte aux personnes autorisées. | Y | Mettre en place une gestion des accès basée sur les rôles (RBAC). |
| PCI-DSS – Surveillance et tests réguliers des réseaux | Tester régulièrement les mesures de sécurité. | Y (partiel) | Formaliser un programme de tests de sécurité. |
| PCI-DSS – Politique de sécurité de l'information | Maintenir une politique de sécurité de l'information à jour. | Y (partiel) | Déployer des formations régulières en sécurité informatique. |