

Plan de Gouvernance des Données

MoviesForYou

AMIN ELFAQUIRI

December 13, 2023

Introduction

Bienvenue dans le Plan de Gouvernance des Données de MoviesForYou. Ce document énonce les politiques, les procédures et les mesures de sécurité mises en place pour garantir la qualité, la sécurité, l'intégrité des données, ainsi que la conformité au RGPD dans le cadre du projet MoviesForYou.

1. Politiques de Gouvernance des Données

1.1 Qualité des Données

1.1.1 Normes de Qualité

MoviesForYou a défini une norme de qualité exigeant des critiques de films des notations précises sur une échelle de 1 à 5 étoiles, une attribution cohérente de genres, et des informations complètes sur la distribution et la date de sortie.

1.1.2 Processus de Vérification

Pour maintenir la qualité des données, l'équipe de MoviesForYou instaure un processus de vérification mensuelle, combinant des examens manuels des critiques de films et l'utilisation d'outils automatisés pour une vérification plus approfondie.

1.2 Sécurité des Données

1.2.1 Politiques de Sécurité

MoviesForYou établit des politiques de sécurité robustes couvrant le chiffrement des données, la gestion des accès, et la surveillance continue.

1.2.2 Chiffrement des Données

Toutes les données liées aux critiques de films, y compris les notations, les commentaires et les informations associées, sont stockées de manière chiffrée, assurant une protection complète.

1.2.3 Gestion des Accès

Un système rigoureux de gestion des accès est mis en place, attribuant des rôles spécifiques aux employés et aux utilisateurs. L'accès est accordé en fonction de ces rôles, assurant une sécurité optimale.

1.2.4 Tests de Pénétration

Des tests de pénétration réguliers évaluent la résistance du système aux tentatives d'intrusion, renforçant ainsi les mesures de sécurité.

1.2.5 Gestion des Identités et des Accès (IAM)

MoviesForYou implémente une solution de gestion des identités et des accès pour une gestion centralisée des autorisations.

1.2.6 Plan de Continuité des Activités (PCA)

Un plan de continuité des activités garantit la disponibilité continue du système, même en cas d'incident majeur, grâce à des sauvegardes régulières et des procédures de récupération d'urgence.

1.3 Intégrité des Données

Des contrôles sont définis pour garantir l'intégrité des données à chaque étape du traitement, avec un focus sur la détection et la correction rapide des erreurs.

1.4 Conformité au RGPD

Des procédures sont élaborées pour assurer la conformité au RGPD, incluant des mécanismes de consentement utilisateur, des politiques de confidentialité transparentes, et des processus pour répondre aux demandes d'accès aux données.

2. Parties prenantes et Responsabilités

2.1 Officier de Gouvernance des Données

AMIN EL FAQUIRI

2.2 Délégué à la Protection des Données (DPO)

AMIN EL FAQUIRI

2.3 Conseil des Données

Représentants des équipes de conformité, juridique, IT et produit.

3. Mesure de la Qualité et de l'Intégrité des Données

3.1 Audits réguliers

Pour assurer l'intégrité et la qualité des systèmes de traitement des données.

3.2 Surveillance continue

Des protocoles de sécurité sont surveillés régulièrement pour détecter les vulnérabilités potentielles.

4. Sécurité des Données et Conformité Réglementaire

4.1 Chiffrement robuste

Pour les données en transit et au repos.

4.2 Respect strict du RGPD

Et d'autres réglementations pertinentes en matière de protection des données.

4.3 Protocoles d'authentification

Incluant l'authentification biométrique pour les appareils compatibles.

5. Usage et Accès aux Données

5.1 Protection rigoureuse des IPI

Par des mesures de contrôle d'accès.

5.2 Politiques claires

Sur l'usage et le partage des données, explicitement communiquées aux utilisateurs.

6. Traçabilité des Données et Suppression des Données

6.1 Traçabilité des Données

Identification des sources et cartographie des étapes de traitement, stockage sécurisé dans le cloud et local crypté.

6.2 Processus de Suppression des Données

Adhérence à une politique de minimisation, suppression automatisée après utilisation, audits réguliers pour vérifier l'exécution précise.

7. Conformité au RGPD

7.1 Consentement explicite

Obtenu lors de la collecte des données.

7.2 Politiques de confidentialité transparentes

Accessibles aux utilisateurs lors de l'inscription et via les paramètres de l'application.

7.3 Procédures robustes

Pour l'accès, la rectification, la suppression, la portabilité et l'opposition aux données.

8. DPA et Traitement des Données

8.1 Accords détaillés de traitement des données (DPA)

Avec les sous-traitants, définissant les rôles et exigences de conformité.

8.2 Conservation du droit d'auditer

Les pratiques de données des sous-traitants.

9. Évaluation d'Impact sur la Protection des Données (EIPD)

9.1 Évaluations nécessaires

Réalisées pour gérer les données personnelles.

9.2 Stratégies pour l'évaluation et l'atténuation des risques

Incluant l'anonymisation des données et des systèmes de surveillance renforcés.

10. Réponse aux Incidents et Protocole de Violation

10.1 Outils de surveillance

Pour détecter et répondre rapidement aux violations de données.

10.2 Protocoles internes

Établis pour signaler immédiatement les violations au DPO et aux autorités compétentes.

10.3 Notification immédiate

Par email aux utilisateurs en cas de violation de données affectant leurs informations.

11. Surveillance de la Conformité et Audit

11.1 Vérifications internes régulières

Pour garantir la conformité.

11.2 Audits annuels externes

Pour le respect du RGPD par une société indépendante.

11.3 Procédures d'escalade

Pour traiter les constatations de non-conformité.

12. Documentation et Tenue des Registres

12.1 Journaux détaillés

Des activités de traitement des données conservés dans des logiciels conformes.

12.2 Stockage sécurisé

De la documentation sur la protection des données aux côtés des données du compte utilisateur.

12.3 Documentation des sessions de formation

Du personnel et des registres de présence.

13. Délégué à la Protection des Données (DPD)

AMIN EL FAQUIRI nommé en tant que DPO avec une indépendance claire dans son rôle.

14. Formation et Sensibilisation

14.1 Programmes de formation réguliers

Couvrant les fondamentaux du RGPD, la manipulation spécifique des données, et les protocoles de sécurité.

14.2 Formation supplémentaire

Lors des changements de rôles liés au traitement des données.

14.3 Newsletters mensuelles

Sur les meilleures pratiques de protection des données pour sensibiliser les employés.

15. Mécanisme de Révision et de Mise à Jour

15.1 Révisions bi-annuelles

Du plan de conformité au RGPD.

15.2 Processus de gestion des changements

Documentés et approuvés par le DPO et l'équipe juridique pour une mise en œuvre organisationnelle.