Plan de Gouvernance des Données pour FraudDetectioMaster

1. Politiques de Gouvernance des Données

1.1 Qualité des Données

1.1.2 Normes de Qualité

Supposons que FraudDetectioMaster ait défini une norme de qualité stipulant que les transactions doivent être conformes aux règlement propre de l'entreprise.

1.1.3 Processus de Vérification

Pour maintenir la qualité des données, l'équipe de FraudDetectioMaster peut mettre en place un processus de vérification mensuelle où les transactions sont examinées manuellement pour s'assurer qu'elles respectent les normes établies. Ils pourraient également utiliser des outils automatisés pour identifier les transactions qui pourraient nécessiter une vérification plus approfondie.

1.2 Sécurité des Données

1.2.1 Politiques de Sécurité

FraudDetectioMaster établit des politiques de sécurité robustes pour garantir la protection des données relatives aux transctions. Ces politiques incluent des directives spécifiques sur le chiffrement des données, la gestion des accès et la surveillance continue.

1.2.2 Chiffrement des Données

Toutes les données liées aux clients sont stockées de manière chiffrée. Cela s'applique à la fois aux données en transit et aux données au repos, assurant une protection complète contre les accès non autorisés.

1.2.3 Gestion des Accès

FraudDetectioMaster met en place un système rigoureux de gestion des accès pour contrôler qui peut accéder aux données. Les employés et les utilisateurs sont attribués à des rôles spécifiques, et l'accès est accordé en fonction de ces rôles. Par exemple, seuls les administrateurs système ont un accès complet, tandis que les transactions ont un accès limité aux données nécessaires à leurs activités.

1.2.4 Tests de Pénétration

Des tests de pénétration réguliers sont effectués pour évaluer la résistance du système aux tentatives d'intrusion. Les résultats de ces tests sont utilisés pour renforcer les mesures de sécurité existantes et remédier aux vulnérabilités identifiées.

1.2.5 Gestion des Identités et des Accès (IAM)

FraudDetectioMaster implémente une solution de gestion des identités et des accès pour gérer de manière centralisée les identités des utilisateurs, les autorisations et les accès. Cela garantit que seules les personnes autorisées ont accès aux ressources nécessaires.

1.2.6 Plan de Continuité des Activités (PCA)

Un plan de continuité des activités est élaboré pour assurer la disponibilité continue du système même en cas d'incident majeur. Des sauvegardes régulières des données critiques sont effectuées, et des procédures de récupération d'urgence sont établies.

En mettant en œuvre ces mesures de sécurité, FraudDetectioMaster renforce la protection de ses données liées aux transactions, garantissant la confidentialité, l'intégrité et la disponibilité des informations tout en réduisant les risques liés à la sécurité.

1.3 Intégrité des Données:

Définir des contrôles 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 :

Élaborer des procédures 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(Référence doc de RGPD).

2. Parties prenantes et Responsabilités

Officier de Gouvernance des Données : **John Doe**
Délégué à la Protection des Données (DPO) : **SEFDINE Nassuf**
Conseil des Données : Représentants des équipes de conformité, juridique, IT et produit.

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

Audits réguliers pour assurer l'intégrité et la qualité des systèmes de traitement des données.

Surveillance continue des protocoles de sécurité pour détecter les vulnérabilités potentielles.

4. Sécurité des Données et Conformité Réglementaire

Chiffrement robuste pour les données en transit et au repos.

Respect strict du RGPD et d'autres réglementations pertinentes en matière de protection des données.

Mise en place de protocoles d'authentification, y compris l'authentification biométrique pour les appareils compatibles.

5. Usage et Accès aux Données

Protection rigoureuse des Informations Personnelles Identifiables (IPI) par des mesures de contrôle d'accès.

Politiques claires et transparentes sur l'usage et le partage des données, explicitement communiquées aux utilisateurs.

6. Traçabilité des Données et Suppression des Données

Traçabilité des Données

Identification des données sources à partir des API.

Cartographie des étapes de traitement des données, de la collecte à la détection des fraudes.

Stockage sécurisé dans le cloud FraudDetectioMaster et stockage local crypté sur les appareils des utilisateurs.

Processus de Suppression des Données

Adhérence à une politique de minimisation - conservation des données uniquement tant que le compte utilisateur est actif, plus une année supplémentaire pour les sauvegardes.

Suppression automatisée des données après utilisation dans la détection des fraudes.

Audits réguliers pour vérifier l'exécution précise des processus de suppression des données.

7. Conformité au RGPD

Consentement explicite de l'utilisateur obtenu lors de la collecte des données.

Politiques de confidentialité transparentes accessibles aux utilisateurs lors de l'inscription et via les paramètres de l'application.

Procédures robustes pour l'accès, la rectification, la suppression, la portabilité et l'opposition aux données.

8. DPA et Traitement des Données

Accords détaillés de traitement des données (DPA) avec les sous-traitants, définissant les rôles et exigences de conformité.

Conservation du droit d'auditer les pratiques de données des sous-traitants.

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

Évaluations nécessaires réalisées pour gérer les données personnelles.

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

Outils de surveillance pour détecter et répondre rapidement aux violations de données.

Protocoles internes établis pour signaler immédiatement les violations au DPO et aux autorités compétentes.

Notification immédiate par email aux utilisateurs en cas de violation de données affectant leurs informations.

11. Surveillance de la Conformité et Audit

Vérifications internes régulières pour garantir la conformité.

Audits annuels externes pour le respect du RGPD par une société indépendante.

Procédures d'escalade pour traiter les constatations de non-conformité.

12. Documentation et Tenue des Registres

Journaux détaillés des activités de traitement des données conservés dans des logiciels conformes.

Stockage sécurisé de la documentation sur la protection des données aux côtés des données du compte utilisateur.

Documentation des sessions de formation du personnel et des registres de présence.

13. Délégué à la Protection des Données (DPD)

SEFDINE Nassuf nommé en tant que DPO avec une indépendance claire dans son rôle.

14. Formation et Sensibilisation

Programmes de formation réguliers couvrant les fondamentaux du RGPD, la manipulation spécifique des données, et les protocoles de sécurité.

Formation supplémentaire lors des changements de rôles liés au traitement des données.

Newsletters mensuelles sur les meilleures pratiques de protection des données pour sensibiliser les employés.

15. Mécanisme de Révision et de Mise à Jour

Révisions bi-annuelles du plan de conformité au RGPD.

Processus de gestion des changements documentés et approuvés par le DPO et l'équipe juridique pour une mise en œuvre organisationnelle.