

Plan de Conformité au RGPD pour FraudDetectioMaster

Vue d'Ensemble du Projet

- **Nom du Projet** : FraudDetection
- **Description** : Ce projet a pour but de détecter des fraudes de transaction en temps réel.
- **Responsable** : SEFDINE Nassuf, John Doe
- **Sous-traitant(s)** : Aucune
- **Délégué à la Protection des Données (Contact)** : SEFDINE Nassuf : sefnassuf@FraudDetectioMaster.com;

1. Inventaire des Données et Spécification de l'Objectif

- **Types de Données Collectées** :
 - Informations Personnelles (IP) : Age, location, moyenne de transaction
 - Information des transactions : Montant, numéro de transaction, location, date, marchand, numéro client, type de transaction
 - Données externes : fraude par client, score par client, liste noire de marchands
- **Points de Collecte des Données** : API avec trois endpoints, /api/transactions, /api/customers, /api/externalData
- **Objectif de la collecte et du traitement des Données** : Détecter les transactions frauduleuses en temps réel.
- **Base Juridique du Traitement** : Consentement explicite des utilisateurs et exécution du contrat.

2. Cartographie des Flux de Données

- **Source des Données** : L'API de FraudDetectioMaster.
- **Activités de Traitement des Données** : Création de l'API, Collecte, analyse, détection de fraude.
- **Lieux de Stockage des Données** : Cloud Sécurisé FraudDetectioMaster (basé dans l'UE), stockage local de l'appareil (crypté).
- **Destinataires des Données** : Équipe de support et d'analyse.
- **Transferts de Données Transfrontaliers** : Les données des utilisateurs ne sont pas transférées hors de l'UE

3. Transparence et Avis de Confidentialité

- **Détails de la Politique de Confidentialité** :
 - Utilisation des données, partage avec des tiers, et droits de l'utilisateur clairement expliqués.
 - Coordonnées du DPD pour toute préoccupation concernant la confidentialité.

- **Méthode de Distribution de l'Avis de Confidentialité** : Notification lors de l'inscription de l'utilisateur et accessible dans les paramètres de l'application.

4. Gestion du Consentement

- **Mécanisme de Consentement** :
 - Opt-in actif lors de l'inscription et consentement séparé pour les données sensibles
 - Option facilement accessible pour modifier le consentement à tout moment dans le profil utilisateur.
- **Documentation du Consentement** : Consentement enregistré avec horodatage et version de la politique de confidentialité acceptée.

5. Droits des Sujets de Données

- **Demandes d'Accès** : Les utilisateurs peuvent voir toutes leurs données dans l'application sous 'Mon Profil' -> 'Mes Données'.
- **Demandes de Rectification** : Modifiable via les paramètres du profil utilisateur; l'équipe de support est notifiée pour assistance si nécessaire
- **Demandes d'Effacement** : Fonction 'Supprimer Mon Compte' pour initier l'effacement complet des données.
- **Demandes de Portabilité des Données** : Fonctionnalité pour exporter les données dans un format lisible par machine disponible dans les paramètres.
- **Demandes d'Opposition au Traitement** : Informations de contact pour le DPD fournies pour les objections au traitement.

6. Mesures de Sécurité des Données

- **Mesures Techniques** :
 - Cryptage de bout en bout pour les données en transit et au repos
 - Authentification biométrique pour l'accès à l'application sur les appareils compatibles
- **Mesures Organisationnelles** :
 - Formation régulière sur la protection des données et la sécurité pour tous les membres du personnel.
 - Contrôles d'accès aux données limitant l'accès aux informations en fonction des rôles professionnels.

7. Minimisation des Données et Politique de Conservation

- **Stratégies de Minimisation** : Seules les données nécessaires pour fournir les services sont collectées.
- **Calendrier de Conservation** : Les données sont conservées tant que le compte utilisateur est actif, plus un an pour des fins de sauvegarde
- **Procédures d'Élimination des Données** : Effacement sécurisé des données de tous les systèmes et sauvegardes après la période de conservation.

8. Accords de Traitement des Données (DPA)

- **Détails des DPA avec les Sous-traitants** : Rôles, responsabilités et exigences de conformité au RGPD clairement définis.
- **Droits d'Audit** : FraudDetectionMasters conserve le droit d'auditer les pratiques de données de l'API.

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

- **Analyse de l'Exigence d'EIPD** : Nécessaire pour gérer les données personnelles.

- **Procédure d'EIPD** : Évaluation des risques associés au traitement des données et décisions sur les stratégies d'atténuation.
 - **Mesures d'Atténuation des Risques** : Anonymisation des données si possible, systèmes de surveillance améliorés.
10. Réponse aux Incidents et Protocole de Violation des Données
- **Méthodes de Détection des Incidents** : Outils de surveillance pour détecter les violations de données.
 - **Procédures de Rapport de Violation** : Processus interne établi pour un rapport immédiat au DPD et aux autorités compétentes.
 - **Format et Calendrier de Notification de Violation** : Notification par email aux utilisateurs si leurs données sont affectées, sans retard indu
11. Surveillance de la Conformité et Audit
- **Calendrier de Surveillance** : Vérifications régulières par l'équipe de conformité interne.
 - **Calendrier d'Audit Interne** : Audit de conformité au RGPD réalisé annuellement par une entreprise externe.
 - **Plan d'Action pour les Constatations de Non-conformité** : Plan de remédiation en place, avec des procédures d'escalade à la direction
12. Documentation et Tenue des Registres
- **Registres d'Activité de Traitement** : Journaux détaillés maintenus dans le logiciel de conformité.
 - **Documentation sur la Protection des Données** : Stockée en toute sécurité avec les données du compte utilisateur.
 - **Registres de Formation** : Journaux de toutes les sessions de formation du personnel et présence.
13. Délégué à la Protection des Données (DPD)
- **Nomination du DPD** : SEFDINE Nassuf, avec une claire indépendance dans son rôle.
 - **Responsabilités du DPD** : Superviser la conformité, être un point de contact pour les sujets de données et les autorités de surveillance.
 - **Structure de Rapport du DPD** : Ligne directe avec le CTO et le conseil d'administration.
14. Formation et Sensibilisation
- **Plan de Programme de Formation** : Bases du RGPD, manipulation spécifique des données de l'application, protocoles de sécurité.
 - **Fréquence de Formation** : Annuellement pour tout le personnel, avec formation supplémentaire lors de changements dans les rôles de traitement des données.
 - **Campagnes de Sensibilisation** : Newsletter mensuelle sur les meilleures pratiques de protection des données.
15. Mécanisme de Révision et de Mise à Jour
- **Fréquence de Révision** : Révision bi-annuelle du plan de conformité au RGPD.
 - **Procédures de Mise à Jour** : Les changements sont approuvés par le DPD et l'équipe juridique.

- **Processus de Gestion des Changements** : Procédure documentée pour mettre en œuvre les changements dans toute l'organisation.

Validation

- Préparé par : SEFDINE Nassuf,