

Recommandations sur les règles de gestion à mettre en place sur les données du CRM de Dev'Immediat pour être conforme au RGPD

Dans le cadre de ma mission de conseil, voici cinq recommandations essentielles pour garantir la sécurité et la conformité des données clients de Dev'Immediat avec le Règlement Général sur la Protection des Données (RGPD) :

1. Minimisation des Données Collectées :

- **Description :** Conserver uniquement les données strictement nécessaires à l'activité (principe de minimisation).
- **Action :** J'ai réalisé un audit pour identifier et éliminer les données inutiles, telles que les informations sensibles inutilisées (par exemple, le numéro de sécurité sociale, le groupe sanguin) ou des données personnelles non requises.

2. Anonymisation et Pseudonymisation :

- **Description :** Transformer les données personnelles pour qu'elles ne permettent plus d'identifier une personne.
- **Action :**
 - L'identifiant unique a été remplacé par des identifiants Random unique.
 - Les adresses précises ont été remplacées par des zones géographiques approximatives (ex. : ville uniquement).
 - Les emails et le nombre d'enfant est remplacé par la présence ou non des enfants en charges.

3. Contrôle des Accès :

- **Description :** Limiter l'accès aux données en fonction des rôles et des responsabilités de chaque équipe.
- **Action :**
 - Gestion des accès basé sur le principe du moindre privilège.
 - L'accès aux données sensibles est désormais limité aux seules personnes autorisées.
 - Un journal des connexions est maintenu pour tracer les accès.

4. Limitation de la Conservation des Données :

- **Description :** Définir une durée de conservation appropriée des données.
- **Action :**

- Mettre en place une politique de suppression automatique des données à l'expiration de leur durée de conservation.
- Les clients sont informés sur la durée de conservation via des mentions légales claires.

5. Contrôles Réguliers et Documentation :

- **Description** : Effectuer des contrôles réalistes et réguliers pour maintenir la conformité au RGPD.
- **Action** :
 - Mettre en place un processus d'audit trimestriel pour vérifier l'application des politiques RGPD.
 - Documenter les actions clés liées à la gestion des données pour assurer leur traçabilité.
 - Sensibiliser régulièrement les équipes sur les bonnes pratiques liées à la protection des données.