Recommandations RGPD pour la gestion des données CRM chez Dev'Immediat

1. Minimisation et pertinence des données

Principe : Collecter uniquement les données strictement nécessaires pour répondre aux objectifs définis.

- Établir un audit des données collectées pour évaluer leur pertinence **(Equipe commercial)**.
- Supprimer ou anonymiser les informations sensibles non essentielles (exemple : numéros de sécurité sociale, revenus précis).
- Documenter les finalités de traitement dans un registre clair et accessible.

2. Gestion du consentement et des droits des personnes

Principe : Garantir la transparence et le contrôle des utilisateurs sur leurs données personnelles.

- Mettre en place un système pour obtenir un consentement explicite et traçable.
- Intégrer des outils dans le CRM permettant aux utilisateurs d'exercer leurs droits (accès, rectification, suppression, portabilité).
- Communiquer clairement les durées de conservation et les modalités d'exercice des droits via les politiques de confidentialité (exemple : Inclure dans les contrats une section intitulée "Vos droits et durées de conservation").

3. Sécurité des données et contrôle d'accès

Principe : Protéger les données contre les accès non autorisés ou les cyberattaques.

- Définir des rôles et permissions utilisateur précis dans le CRM.
- Activer l'authentification à deux facteurs pour l'accès au système.
- Chiffrage des données au repos et en transit.
- Mettre en place un journal de suivi des actions effectuées sur les données **(Transparence pour organisme tiers comme CNIL)**.
- Réaliser des audits réguliers pour vérifier la conformité et les niveaux de sécurité **(DPO)**.

4. Durée de conservation et suppression des données

Principe : Conserver les données uniquement pour la durée nécessaire à leur finalité.

- Définir des durées de conservation pour chaque type de données (exemple : 3 ans pour les prospects sans contrat, 7 ans pour les données contractuelles ; source : **CNIL**).
- Implémenter des processus automatisés pour l'archivage et la suppression des données obsolètes.
- Créer un registre des activités de traitement incluant les durées de conservation **(transparence sur l'historique de la data)**.

5. Anonymisation et protection des données sensibles

Principe : Réduire les risques liés à la réidentification des personnes tout en préservant l'utilité des données.

- Mettre en place des techniques d'anonymisation pour les données.
- Adopter des pratiques telles que la randomisation ou la généralisation pour rendre les données non identifiables tout en garantissant leur pertinence pour les analyses.
- Effectuer une veille régulière sur les techniques d'anonymisation pour maintenir leur efficacité face à l'évolution technologique.

Ces recommandations visent à assurer une gestion conforme des données tout en renforçant la confiance des clients et en préservant leur vie privée.