5 recommandations clés pour mettre en place des règles de gestion conformes au RGPD sur les données CRM

1. Minimisation et pertinence des données

- Collecter uniquement les données strictement nécessaires aux finalités définies : Précisément déterminée, Explicite, Légitime.
- La collecte des données doit avoir un but clair et légitime dès le départ.
  - ➢ Ce but doit être défini avant la collecte des données.
  - ➢ Toute utilisation ultérieure des données doit être compatible avec l'objectif initial.
  - ➢ Il est interdit de traiter les données d'une manière qui s'écarterait de la finalité première de leur collecte.
- Éviter la collecte de données sensibles ou non essentielles : Origine ethnique, opinions politiques, données de santé, n° de ss…
- Documentez clairement les finalités de traitement pour chaque type de donnée collectée dans le CRM.

2. Gestion du consentement et des droits des personnes

- Mettre en place un système pour obtenir et documenter le consentement explicite des clients.
  - ➢ S'assurer du consentement de la personne concernée à propos de ses données personnelles pour une ou plusieurs finalités spécifiques.
  - ➢ Les durées de conservation doivent être communiquées aux personnes concernées via les mentions d'information.
  - ➢ Informations fournies dans la documentation contractuelle, envoyée par courrier postal, brochure, infographie, lien vers notre politique de protection des données…
- Implémentez des fonctionnalités permettant aux utilisateurs d'exercer facilement leurs droits RGPD (accès, rectification, suppression, portabilité).
  - ➢ Assurez-vous que le CRM permet de tracer et d'honorer les demandes liées aux droits des personnes.

3. Sécurité et contrôle d'accès

- https://cyber.gouv.fr/bonnes-pratiques-protegez-vous
- Utiliser les fonctionnalités du CRM pour définir des rôles et permissions adaptés aux différents utilisateurs selon leur usage (ex. marketing, support, gestion commerciale).
  - ➢ Qui est autorisé à voir quoi, à faire quoi (lecture/édition)
- Activer l'authentification à deux facteurs pour protéger l'accès au CRM
  - ➢ Mot de passe défini par un générateur de mot de passe (https://www.keepersecurity.com/fr_FR par ex) avec au moins une majuscule, un chiffre, un caractère spécial et 10 caractères, à modifier tous les 3 mois.
- Mettre en place un système de journalisation des accès et des actions effectuées sur les données.
  - ➢ Tous les 6 mois, revoir les permissions des utilisateurs.
  - ➢ Verrouillage automatique après temps réduit.
- Dans les cas les plus sensibles, interdiction pour certains métiers de :
  - ➢ Utiliser leur téléphone portable personnel, Bloc note/crayon, Répéter à haute voix les infos des clients.
- Effectuer des audits RGPD réguliers pour évaluer la conformité et identifier les améliorations nécessaires. Effectuer des tests d'intrusion.
- Le DPO sera impliqué dans toutes les questions relatives à la protection des données personnelles.
- Mettre en place des formations RGPD régulières pour le personnel utilisant le CRM.
- Créer des guides internes sur les bonnes pratiques de gestion des données dans le CRM (charte de gouvernance).

4. Durée de conservation et suppression des données

https://www.cnil.fr/sites/cnil/files/atoms/files/guide_durees_de_conservation.pdf

Les données personnelles ne peuvent être conservées indéfiniment :

- La loi de modernisation de la justice du XXIème siècle (2016) impose aux assureurs de conserver certaines informations des assurés (nom et adresse du propriétaire ou conducteur habituel du véhicule) pendant 7 ans après la fin du contrat d'assurance.
- Pour les prospects sans contrat conclu, les données peuvent être conservées 3 ans après leur collecte ou le dernier contact.
- Les données utiles à la constatation, défense ou exercice de droits en justice peuvent être gardées jusqu'à 5 ans.
- En l'absence de texte législatif spécifique, le responsable de traitement doit déterminer la durée de conservation en fonction de l'objectif de la collecte des données.

Définir une procédure d'archivage, de suppression et de conservation des données avec des durées spécifiques pour chaque type d'information

- Sous forme de tableau par exemple.
- Rappels automatiques pour supprimer les données après la durée légale définie.
- Mettre en place un processus régulier d'identification et de suppression des données obsolètes ou inutiles.
- Mettre en place un registre des activités de traitement, incluant les bases légales et les mesures de sécurité

Dès que la finalité pour laquelle elles ont été collectées est atteinte, les données selon les cas peuvent être :

Archivées

Archivage intermédiaire

- Permet de conserver des données personnelles qui ne servent plus leur objectif initial mais gardent un intérêt administratif ou légal. L'accès à ces données est limité et contrôlé, réservé à des consultations ponctuelles par du personnel autorisé.

Archivage définitif

- Certaines informations présentant une valeur significative sont archivées de manière définitive et pérenne. Contrairement à la conservation en base active, ces étapes d'archivage ne sont pas systématiques et doivent être évaluées au cas par cas, avec un tri rigoureux des données à chaque phase.

Supprimées

Anonymisées

Elle permet de conserver des données au-delà de leur durée de conservation.

5. Protection des données sensibles : Règles strictes et exceptions limitées

Le RGPD établit une protection renforcée pour certaines catégories de données personnelles considérées comme sensibles. Ces données incluent les informations relatives à la santé, les opinions politiques, les croyances religieuses, l'orientation sexuelle, l'origine ethnique…

Pour établir un processus d'anonymisation efficace, il est recommandé de suivre ces étapes clés :

- Identifier les informations pertinentes à conserver
- Supprimer les identifiants directs et les valeurs rares facilitant la ré-identification
- Identifier les données essentielles en éliminant ce qui est accessoire ou inutile.
- Ajuster le niveau de détail de chaque information pour garantir son utilité tout en minimisant les risques d'identification personnelle.

Cette analyse préliminaire permet de choisir la méthode d'anonymisation appropriée, qui peut relever de deux grandes familles :

- La randomisation : consiste à modifier les attributs dans un jeu de données de telle sorte qu'elles soient moins précises. (ex : Permutation : intervertir les dates de naissance entre individus).
- La généralisation : modifie l'échelle ou l'ordre de grandeur des attributs pour les rendre communs à un groupe de personnes. (ex : remplacer l'âge précis par des tranches d'âge (ex. "30-40 ans"))