RGPD

# Recommandations RGPD – Gestion des données CRM

## Limitation de la collecte aux données strictement nécessaires (principe de minimisation)

Avant toute collecte de données, il est essentiel d’identifier clairement la finalité du traitement. Seules les données pertinentes, adéquates et limitées à ce qui est strictement nécessaire doivent être collectées.

Actions à mettre en œuvre :

* Réaliser un audit des données collectées pour vérifier leur pertinence par rapport aux objectifs définis.
* Supprimer ou éviter la collecte de données sensibles inutiles comme le numéro de sécurité sociale, les coordonnées GPS précises, ou encore les informations de santé.
* Préférer des champs de saisie généraux ou catégoriels (ex : tranche d’âge plutôt que date de naissance exacte) lorsque le niveau de précision n’est pas requis.

## Mise en place de processus d’anonymisation ou de pseudonymisation des données personnelles

L’anonymisation permet de supprimer tout lien identifiable avec une personne. À défaut, la pseudonymisation, qui rend les données indirectement identifiables, peut être utilisée avec des mesures de protection supplémentaires.

Actions à mettre en œuvre :

* Remplacer les identifiants directs (noms, prénoms, emails, numéros clients) par des identifiants aléatoires ou des pseudonymes.
* Regrouper ou convertir certaines données numériques en tranches (ex : tranches de revenus, tranches d’âge, zones géographiques larges).
* Appliquer des techniques d’anonymisation statistique (agrégation, suppression, permutation) pour les analyses.

## Restriction des accès aux données sensibles (principe de confidentialité)

La sécurité des données passe par une gestion fine des droits d’accès. Les collaborateurs ne doivent avoir accès qu’aux données strictement nécessaires à leurs missions.

Actions à mettre en œuvre :

* Définir des profils d’accès par rôle ou service, et appliquer une politique de contrôle d’accès (ex : RBAC – Role-Based Access Control).
* Protéger les fichiers contenant des données sensibles par mot de passe, chiffrement ou restriction sur les serveurs internes.
* Assurer une traçabilité des accès et des modifications (logs) afin de garantir l’audibilité des traitements.

1. **Documentation complète des traitements de données personnelles (obligation de traçabilité)**

La tenue d’un registre des traitements est obligatoire pour les organismes traitant des données personnelles. Ce registre permet de démontrer la conformité à tout moment.

Actions à mettre en œuvre :

* Élaborer un registre interne mentionnant :

o Les finalités de chaque traitement  
 o Les catégories de données concernées  
 o Les destinataires internes ou externes  
 o Les durées de conservation  
 o Les mesures de sécurité associées

* Mettre à jour régulièrement ce registre en cas d’évolution des traitements ou de la structure organisationnelle.

## Transparence et information des personnes concernées sur leurs droits

Le RGPD impose une communication claire et accessible sur l’usage des données personnelles. Chaque individu doit pouvoir exercer ses droits facilement.

Actions à mettre en œuvre :

* Rédiger une politique de confidentialité claire, concise et facilement accessible (site web, contrat, email).
* Informer les utilisateurs des droits suivants :

o Droit d’accès  
 o Droit de rectification  
 o Droit à l’effacement (droit à l’oubli)  
 o Droit à la portabilité  
 o Droit d’opposition et à la limitation du traitement

* Mettre en place des canaux simples pour l’exercice de ces droits (formulaire de contact, adresse email dédiée, interface utilisateur).