DEV'IMMEDIAT

5 recommandations sur les règles de gestion à mettre en place sur les données du CRM pour être conforme au RGPD

1) Constituez un registre de vos traitements de données

Le RGPD impose au responsable de traitement de tenir un registre listant les traitements de données.

La tenue du registre est l'occasion de sensibiliser les services aux enjeux de la protection des données. Dans les faits, ce registre est souvent tenu par le DPO (Data Protection Officer ou Délégué à la Protection des Données) qui est un responsable désigné au sein d'une organisation pour veiller à la conformité avec le RGPD, conseiller sur les questions de protection des données et servir de point de contact pour les autorités de contrôle et les individus concernés.

Dans votre registre, créez une fiche par activité recensée, en précisant :

1) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données.
2) le ou les objectifs poursuivis par chaque traitement.
3) les catégories de personnes concernées et de données utilisées.
4) les destinataires des données.
5) les durées de conservation de ces données.
6) les mesures de sécurité envisagées.
7) le cas échéant, les transferts de données à caractère personnel en dehors de l'UE ou à une organisation internationale.

Pour avoir un registre exhaustif et à jour, il est nécessaire d'être en contact régulier avec toutes les personnes de la collectivité susceptibles de traiter des données personnelles.

2) Faites le tri dans vos données

Chaque fiche du registre vous permet de vérifier :

1) la pertinence des données traitées et qu'elles sont nécessaires à l'objectif poursuivi (principes de pertinence et de minimisation).
2) la nature des données traitées afin d'adopter des mesures de sécurité adaptées aux risques spécifiques associés aux données.
3) la garantie que seuls les agents habilités ont accès aux données dont ils ont besoin.
4) que les données ne sont pas conservées au-delà de ce qui est nécessaire en fixant précisément la durée de conservation et d'archivage des données.

Il ne faut collecter les données vraiment nécessaires pour un but bien déterminé et légitime et qu'elles ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.

3) Respectez les droits des administrés

Les individus doivent conserver la maîtrise des données qui les concernent.

Cela suppose qu'ils soient clairement informés de l'utilisation qui sera faite de leurs données dès leur collecte. Les données ne peuvent en aucun cas être collectées à leur insu. Les personnes doivent également être informées de leurs droits et des modalités d'exercice de ces droits.

Vous devez organiser des modalités permettant aux personnes d'exercer leurs droits et répondre dans les meilleurs délais à ces demandes de consultation ou d'accès, de rectification ou de suppression des données, voire d'opposition, sauf si le traitement répond à une obligation légale. Ces droits doivent pouvoir s'exercer par voie électronique à partir d'une adresse dédiée.

Remarque : le consentement n'est pas nécessaire lorsque ces données sont collectées pour l'exécution d'un contrat ou de mesures précontractuelles (ex : un devis).

4) Fixez des durées de conservation

Vous ne pouvez pas conserver les données indéfiniment.

Elles ne sont conservées en « base active », c'est-à-dire la gestion courante, que le temps strictement nécessaire à la réalisation de l'objectif poursuivi et elles doivent être par la suite détruites, anonymisées ou archivées dans le respect des obligations légales applicables en matière de conservation des archives publiques.

5) Sécurisez les données

Vous devez prendre toutes les mesures utiles pour garantir la sécurité des données : sécurité physique ou sécurité informatique, sécurisation des locaux, armoires et postes de travail, gestion stricte des habilitations et droits d'accès informatiques.

Cela consiste aussi à s'assurer que seuls les tiers autorisés par des textes ont accès aux données.

Ces mesures sont adaptées en fonction de la sensibilité des données ou des risques qui peuvent peser sur les personnes en cas d'incident de sécurité.

Pour conclure, la conformité n'est pas gravée dans le marbre et figée : il faut l'inscrire dans une démarche continue. Elle dépend du bon respect au quotidien par les agents, à tous les niveaux, des principes et mesures mis en oeuvre.

Vérifiez régulièrement que les traitements n'ont pas évolué, que les procédures et les mesures de sécurité mises en place sont bien respectées et adaptez-les si besoin.