Gestion des Données CRM Conformément au RGPD

Le Règlement Général sur la Protection des Données (RGPD) impose des règles strictes en matière de gestion des données personnelles, y compris pour les données collectées via les systèmes de CRM (Customer Relationship Management).

1- Collecte et Traitement des Données :

Obtenir un consentement clair pour collecter et traiter les données client. Collecter uniquement les données nécessaires à votre activité.

Les actions à mettre en place pour définir clairement les objectifs du traitement des données dans votre CRM (trier les données pour ne garder que les informations sur la prospection commerciale afin de faire des marges sur les ventes et anonymisées et pseudonymies les données restant).

Il faut garder que les informations nécessaires à ces objectifs.

2- Obtenir et Gérer le Consentement de Façon Claire et Documentée :

Il est nécessaire d'obtenir le consentement explicite des personnes concernées pour le traitement de leurs données, conformément aux exigences du RGPD. Il convient également de conserver une trace de ce consentement et de permettre aux individus de le retirer aisément. Enfin, il est important de documenter ce consentement afin de démontrer la conformité avec la réglementation.

Pour obtenir ce consentement, vous pouvez envoyer un e-mail dans lequel vous confirmez les informations que vous détenez et incluez une case à cocher permettant à la personne de consentir à la conservation de ses données personnelles pour le traitement.

Mais également pour les nouveaux contrats, en ajoutant une clause spécifique relative à la collecte et au traitement des données personnelles, précisant les finalités, la durée de conservation, et les droits des individus concernant leurs données.

3- Garantir la Sécurisation des Données et la Confidentialité :

Il est essentiel de mettre en place des mesures techniques et organisationnelles adéquates pour garantir la sécurité des données CRM, afin de les protéger contre toute fuite, perte ou accès non autorisé.

Il est important de sensibiliser les salariés à la sécurité des données, notamment par le biais de formations internes, et d'implémenter des contrôles d'accès stricts. Il convient

également de désigner des responsables spécifiques, tels que le DPO, le RSSI et les équipes juridiques, pour assurer la gestion et la sécurité des données.

Il est crucial de limiter l'accès aux bases de données CRM aux seules personnes autorisées et d'appliquer des politiques de mot de passe strictes afin de prévenir tout accès non autorisé.

4- Respecter les Droits des Personnes Concernées :

Assurez-vous que les clients puissent facilement exercer leurs droits d'accès, de rectification, d'effacement et de portabilité de leurs données.

Vous pouvez mettre en place des mécanismes simples pour permettre aux utilisateurs de demander l'accès, la modification, ou la suppression de leurs données personnelles (formulaire ou sur l'espace client en ligne).

5- Limiter la Conservation des Données et Mettre en Place une Gestion des Risques :

Il est essentiel de limiter la durée de conservation des données CRM aux périodes strictement nécessaires à la réalisation des finalités du traitement, et d'assurer une gestion proactive des risques associés aux violations de données.

Il convient de définir des périodes de conservation des données et de veiller à leur respect. Lorsque les données ne sont plus nécessaires, elles doivent être supprimées ou anonymisées afin de garantir le respect du principe de minimisation des données.

En cas de violation de données, il est impératif d'informer les autorités compétentes et les personnes concernées dans un délai de 72 heures. Il convient également de mettre en place un plan d'action pour gérer efficacement les violations de données.

Conclusion :

Ces cinq recommandations permettent de mettre en place une gestion rigoureuse et conforme des données CRM, assurant ainsi la protection de la vie privée des clients et le respect des obligations légales imposées par le RGPD. Il est essentiel d'adopter une approche proactive et systématique pour garantir la sécurité et la confidentialité des informations personnelles.