RECOMMANDATIONS SUR LES REGLES DE GESTION CONFORMES AU RGPD

Le traitement et la sécurisation des données sont des éléments essentiels pour garantir la conformité au RGPD et protéger la vie privée des individus.

Une fois que le consentement a été obtenu, il est crucial de mettre en place des mesures de sécurité adéquates pour prévenir les violations de données et assurer la confidentialité des informations personnelles.

Voici des recommandations clés pour sécuriser le traitement des données conformément au RGPD :

1. **CRYPTAGE DES DONNEES** : le cryptage est une méthode efficace pour protéger les données en transit et au repos. Toutes les données sensibles, telles que les informations d'identification, les numéros de sécurité sociale et les coordonnées bancaires, doivent être stockées sous forme cryptée. Utilisez des algorithmes de cryptage robustes et assurez-vous que les clés de cryptage sont gérées de manière sécurisée.

2. **GESTION DES ACCES ET DES HABILITATIONS** : limitez l'accès aux données personnelles aux seules personnes qui en ont besoin pour effectuer leur travail. Mettez en place des politiques d'habilitation strictes pour contrôler qui peut accéder aux informations sensibles. Suivez les principes du moindre privilège en accordant uniquement les droits d'accès nécessaires à chaque utilisateur.

3. **AUDIT ET TRAÇABILITE** : mettez en place des journaux d'audit pour enregistrer toutes les activités liées aux données personnelles. Cela permet de suivre qui a accédé aux données, quand et pourquoi. Surveillez régulièrement les journaux d'audit pour détecter toute activité suspecte ou non autorisée.

4. **FORMATION ET SENSIBILISATION DES UTILISATEURS** : sensibilisez tous les employés à l'importance de la sécurité des données. Organisez des sessions de formation régulières pour les informer des meilleures pratiques et des risques potentiels. Encouragez les utilisateurs à signaler immédiatement toute violation de sécurité ou tout comportement suspect.

5. **GESTION DES INCIDENTS** : élaborez un plan de gestion des incidents pour réagir rapidement en cas de violation de données. Ce plan doit inclure des procédures pour informer les autorités de protection des données et les personnes concernées. Testez régulièrement votre plan de gestion des incidents pour vous assurer qu'il est opérationnel et que les équipes savent comment réagir en cas d'urgence.

En mettant en œuvre ces recommandations, votre entreprise renforcera la sécurité de ses données et se conformera aux exigences du RGPD tout en protégeant la vie privée des individus.

A l'analyse des données collectées par le CRM, un certain nombre de mesures sont à prendre sans tarder, voici nos recommandations.

TABLEAU DE SYNTHESE RECAPITULATIF DE RECOMMANDATIONS POUR LA SECURISATION DES DONNEES COLLECTEES PAR LE CRM

Nom du champ ou de la variable collectée	Mesure à mettre en place rapidement pour la sécurisation des données
num_ss	Cryptage de la donnée
groupe_sanguin*	Données médicales / sensibles | Ne pas collecter la donnée !
email	Cryptage de la donnée
date_naissance	Cryptage de la donnée
revenus	Accès limité / habilitation contrôlée
valeur_residuelle_prin	Accès limité / habilitation contrôlée
tarif_devis	Accès limité / habilitation contrôlée
adresse	Accès limité / habilitation contrôlée

* Cette donnée médicale n'a aucun intérêt pour l'activité et sa collecte et son usage peuvent valoir à l'entreprise de lourdes sanctions administratives et financières. Il faut cesser sa collecte de tout urgence et la supprimer de toute base de données.