Recommandations

Nous vous proposons les 5 recommandations suivantes à mettre en place sur les données du CRM afin d'être en conformité avec le RGPD.

Recommandation 1

Supprimer et ne plus collecter les données de santé des clients. Sauf cas d'usages spécifiques, le traitement de ces données est interdit (art. 9 du RGPD).
Données concernées dans la base clients :

- groupe_sanguin
- num_ss

Article 9 - Traitement portant sur des catégories particulières de données à caractère personnel

1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

Recommandation 2

Supprimer et ne plus collecter les données qui ne sont pas strictement nécessaires à atteindre la finalité du traitement des données (art. 5 du RGPD).
Données concernées dans la base de données :

- lat (latitude de la résidence du client)
- lon (longitude de la résidence du client)
- valeur_residence_prin (valeur résidence principale)

Article 5 - Principes relatifs au traitement des données à caractère personnel

1. Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);
b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

Recommandation 3

Limiter la durée de conservation des données.

Il s'agit d'un principe général énoncé à l'article 5 du RGPD qui impose à chaque responsable de traitement de déterminer une durée de conservation des données personnelles cohérente et justifiée au regard de l'objectif de leur traitement.

Un organisme ne peut donc conserver des données personnelles de manière illimitée, sauf dans certains cas spécifiques et limités à ce qui est strictement nécessaire.

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

Recommandation 4

Documenter la conformité de l'entreprise en matière de conservation de données.

La documentation constitue un élément clé de conformité aux règles relatives à la protection des données personnelles : les actions entreprises, les analyses menées et les documents réalisés à chaque étape doivent être regroupés et centralisés pour la prouver.

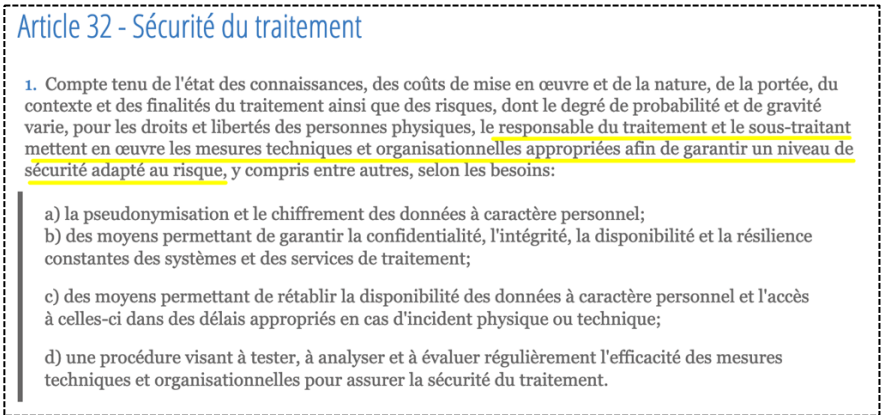
Source : https://www.cnil.fr/sites/cnil/files/atoms/files/guide_durees_de_conservation.pdf

Recommandation 5

Sécuriser les données et leur traitement (art 32 du RGPD).

S'assurer de la mise en place des mesures de sécurité techniques nécessaires à préserver l'intégrité, la disponibilité et la confidentialité des données.

Pour le traitement, compiler dans un document SI de référence « Politique de sécurité des systèmes d'informations (PSSI) », les procédures, contrôles et sensibilisations misent en place pour garantir la sécurité des données.



Article 32 - Sécurité du traitement

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.