

# Recommandations RGPD

## 1. Consentement client/prospect (opt-in/opt-out)

**L'opt-in**, c'est obtenir l'accord préalable du destinataire de la publicité : s'il n'a pas dit « oui », c'est « non ». C'est le cas pour envoyer de la publicité « *B2C* » (du professionnel au consommateur) par email, SMS, MMS, automate d'appels ou fax.

**L'opt-out**, c'est le contraire, lorsque le destinataire de la publicité ne s'est pas opposé : s'il n'a pas dit « non », c'est « oui ». C'est le cas pour la publicité « *B2B* » (de professionnel à professionnel) adressée par email et « *B2C* » adressée par voie postale ou par téléphone.

Il faut donc que le client/prospect soit au fait de l'utilisation que vous ferez de ses données lorsqu'elles sont récoltées et lui permettre de demander la suppression de celles-ci à tout moment.

## 2. Stocker les données strictement utiles uniquement

En fonction de votre secteur d'activité, certaines données sont superflues, il faut alors les identifier et éviter de les stocker.

Par exemple, stocker des données médicales pour une assurance de téléphone est superflu.

À l'inverse, l'assurance maladie n'a pas besoin de savoir si vous avez une assurance pour votre téléphone, votre voiture ou votre maison, ces données leur sont superflues également.

## 3. Suppression auto en cas d'inactivité (3 ans selon la CNIL)

Effectuer une purge automatique des données après 3 ans pour les données non essentielles. (les données marketing par exemple).

Attention, certaines données nécessitent d'être gardées plus longtemps comme :

- Les contrats
- Les factures
- Les contentieux
- Les documents comptables

(liste non exhaustive)

Il faudra, pour ces données, les archiver dans une base de données dont l'accès sera plus restreint.

## 4. Pseudonymisation des données

La pseudonymisation de vos données permet de protéger efficacement les données de vos clients tout en permettant à vos équipes commerciales et techniques de travailler sur le jeu de données.

Cela consiste à une « anonymisation » des données pour ces équipes tout en ayant la possibilité de retrouver les données d'un client si nécessaire.

Pour ce faire il faudra randomisés « identité des clients sur une nouvelle base de données qui sera celle transmise aux équipes pour leur permettre d'effectuer leur travail, tout en conservant le données non modifié sur la base de données principale en y limitant l'accès au personnel essentiel uniquement.

## 5. Stratégie data gouvernance pour identifier les rôles avec un data Stewart et un DPO.

La data gouvernance, permettra aux différentes équipes d'accéder à la base de données tout en limitant leur action et le visu pour qu'ils n'aient accès qu'aux données nécessaires à leur travail.

Ainsi l'équipe qui s'occupe du scoring n'aura pas les mêmes besoins que l'équipe commerciale, qui n'aura pas les mêmes besoins que l'équipe sinistre, etc.

Aucune équipe n'aura un accès total sur toutes les données afin de protéger celles-ci et d'éviter une éventuelle fuite des données.