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

- **Consentement :**

Le consentement des utilisateurs aux traitements de leurs données à caractère personnel est la première règle de l'RGPD à respecter. Bien que le consentement ne soit pas nécessaire dans le cas de collecte des données pour conclure des contrats ou des devis mais dans notre cas ces données vont être aussi utilisées pour une autre finalité. C'est le pilotage de la performance commerciale. Pour cela il faut avoir le consentement de l'utilisateur avant de les utiliser pour cette fin.

- **Respecter le principe de minimisation**

Le principe de minimisation impose que les données à caractère personnel soient adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Il s'agit d'un principe majeur à respecter lors de collectes des données sur les clients.

Donc, il ne faut collecter que les données strictement nécessaires aux: contrats, devis ou pilotage de la performance commerciale.

Noter bien : Il ne faut jamais collecter des données sensibles sur les clients tels que des données concernant la santé (exemple : le groupe sanguin) et les opinions politiques ou religieuses, etc. Ça induit aux non respects du principe de « protection particulière des données sensibles ».

- **Mettre en place et appliquer des durées de conservations**

Les données personnelles ne peuvent pas être conservées de façon indéfinie par l'organisme qui les traite mais doivent avoir une durée de conservation bien définie. Cette **durée de conservation** doit être déterminée en fonction de l'objectif ayant déterminé la collecte de ces données. Et à l'expiration de cette durée, les données doivent être archivées ou anonymisées ou supprimées.

On pourrait donc sauvegarder les données dans une base de données active pendant une durée bien définie et limitée et à l'expiration on pourrait archiver ces données et/ou les anonymiser et le sauvegarder pour des plus longues durées selon le besoin.

Pour nos données on peut identifier deux types des données:

1. Les données personnelles des clients qui ont finalisé le processus et ont concluent des contrats d'assurance : leurs données peuvent être sauvegardées sans archivage ou anonymisation tout au long de la durée de leur contrats. Et à la fin de cette durée, ces données peuvent être anonymisées pour qu'on puisse continuer à les utiliser dans le pilotage de la performance commerciale. Et tout document (contrat d'assurance, facture, ...) contient des informations personnelles des anciens clients

doit être archivé et sauvegardé et y limiter l'accès sauf en cas de besoin extrême (exemple: conflit juridique avec le client).

2. Données issues des devis: ces données peuvent être sauvegardées pendant une durée spécifique et bien déterminée à l'avance (je recommande 2 ans) et il faut informer l'utilisateur de cette durée de conservation lors de son consentement. Après l'expiration de cette durée, les données peuvent avoir le même sort que les données précédentes. Sauvegardées sous forme des données anonymes.

Sécuriser les données

Les données à caractère personnel des utilisateurs doivent être sauvegardées d'une manière sécurisée. Pour cela des mesures de sécurité doivent être mises en œuvre comme par exemple :

- Sauvegarde périodique des données;
- Utiliser des mots de passes forts pour y accéder. Et mettre un mécanisme d'expiration des mots de passe pour que ces soient changés après une période limitée (6 mois par exemple);
- Mettre en place un antivirus et le mettre à jour périodiquement;
- Bien organiser ces données et surtout organiser l'accès à ces données. Utiliser des permissions différentes pour données à nombre restreint des personnes l'accès à ces données.
- Sécurisé les données lors de collectes (sécuriser l'échange des données entre le navigateur de l'utilisateur et le serveur de l'application);
- Sécurisé l'accès aux serveurs qui hébergent ces données.

Transparence et droits des personnes

Les utilisateurs doivent être informés de l'utilisation de leurs données dans le pilotage de la performance commerciale pendant une durée bien déminée. Et qu'ils ont des droits qui leur permettent de garder la main sur leurs données.

Donc, on devrait mettre en place un mécanisme qui permet aux utilisateurs de pratiquer sur leurs données les droits suivants:

- Modifier;
- Supprimer;
- s'opposer à l'utilisation
- Récupérer;
- limiter le traitement;
- définir le sort des données après la mort;
- ne pas faire l'objet d'une décision automatisée.