Recommandations de conformité au RGPD

1.1 // MINIMISATION DES DONNEES

Il ne faut collecter que les données vraiment nécessaires pour atteindre votre objectif. Les données sont collectées pour un but bien déterminé (contrat d'assurance) et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.
Le principe de finalité limite la manière dont vous pourrez utiliser ou réutiliser ces données dans le futur et évite la collecte de données « au cas où ».
Le principe de minimisation limite la collecte aux seules données strictement nécessaires à la réalisation de votre objectif. Les données sensibles non strictement nécessaire à l'atteinte de l'objectif sont donc à ne pas collecter.

1.2 // POLITIQUE DE CONSERVATION DES DONNEES

Les données personnelles ne peuvent être conservées indéfiniment : une durée de conservation doit être déterminée par le responsable de traitement en fonction de l'objectif ayant conduit à la collecte de ces données.

- **en l'absence de conclusion du contrat d'assurance**, dans le cadre de la gestion de la prospection, le responsable de traitement ne peut conserver les données du prospect au-delà de **3 ans à compter de leur collecte ou du dernier contact émanant du prospect.**
- **Pour les données pouvant permettre la constatation, la défense ou l'exercice de droit en justice,** elles peuvent être conservées pendant une durée maximale de **5 ans à compter de leur collecte ou du dernier contact émanant du prospect**

  Il faudra bien également ne conserver les données sur la base active que le temps de traitement des données. Puis, tant qu'elles conservent un intérêt administratif, les garder en archivage intermédiaire. Puis on choisira soit de supprimer les données, soit de les archiver définitivement.

1.3 // TRANSPARENCE AUX UTILISATEURS

Le règlement général sur la protection des données (RGPD) impose une information concise, transparente, compréhensible et aisément accessible des personnes concernées.
Pour cela il conviendra de mettre à disposition, sur une page d'information accessible lors de la collecte de donnée par exemple, l'ensemble des informations de collecte, *en des termes clairs et simples.*

Les informations suivantes devront être apportées :

- Identité de la société, responsable du traitement des données
- Identité du DPO
- Le cadre légal qui amène à la récupération des données (finalité)
- Caractère obligatoire ou facultatif du recueil des données
- Destinataires ou catégories de destinataires des données
- Les droits des personnes sur leur données (acces,rectification suppression)
- La durée légale de conservation des données
- Droit d'introduire une réclamation auprès de la CNIL

1.4 // PSEUDONYMISATION DES DONNEES

Dans le cadre de l'archivage des données, il est recommandé de procéder à une pseudonymisation des données. La pseudonymisation est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans information supplémentaire.
En pratique, la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) d'un jeu de données par des données indirectement identifiantes (alias, numéro séquentiel, etc.).
La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe. En pratique, il est toutefois bien souvent possible de retrouver l'identité de ceux-ci grâce à des données tierces : les données concernées conservent donc un caractère personnel. L'opération de pseudonymisation est également réversible, contrairement à l'anonymisation.
La pseudonymisation constitue une des mesures recommandées par le RGPD pour limiter les risques liés au traitement de données personnelles.

1.5 // ACCES ET SECURISATION DES DONNEES

Il faut prendre toutes les mesures utiles pour garantir la sécurité des données : sécurité physique ou sécurité informatique, sécurisation des locaux, armoires et postes de travail, gestion stricte des habilitations et droits d'accès informatiques. Cela consiste aussi à s'assurer que seuls les tiers autorisés par des textes ont accès aux données. Ces mesures sont adaptées en fonction de la sensibilité des données ou des risques qui peuvent peser sur les personnes en cas d'incident de sécurité.