5 RECOMMANDATIONS INDISPENSABLES DE CONFORMITÉ AU RGPD

RECOMMANDATION N°1 : construire un registre de traitement des données.

Nous recommandons à l'assureur Dev'immédiat de tenir un **registre des activités de traitement** contenant le **recensement** et la **description des données à caractère personnel** dont il dispose. C'est un document central qui lui permettra d'avoir une bonne visibilité sur sa situation afin d'organiser sa conformité au RGPD. Celui-ci impose les rubriques suivantes, qui devront être remplies pour chaque activité de traitement :

- Le **nom** et les **coordonnées du DPO** (data protection officer) ;
- Les **finalités du traitement** (quel est le but du traitement) ;
- Une description des **catégories de personnes concernées** et des **catégories de données personnelles collectées** ;
- Les **catégories de destinataires** (en particulier les sous-traitants) auxquelles les données ont été ou seront communiquées.

RECOMMANDATION N°2 : s'assurer de la liceité du traitement des données à caractère personnel recensées dans le registre (article 6 RGPD).

Dev'immédiat doit s'assurer que son client a **consenti** au traitement de ses données à caractère personnel dans le cadre d'une **finalité spécifique, explicite et légitime.**
Ici, les données stockées dans le CRM servent à manipuler la performance commerciale des équipes de l'assureur. Certaines d'entre elles sont considérées comme étant des **données sensibles**. Il peut s'agir par exemple du **groupe sanguin**, du **numéro de sécurité sociale**, du **nom**, du **revenu**, de la **date de naissance**, de **l'adresse** ou de **l'identifiant client** etc. C'est la raison pour laquelle il est impératif de les **anonymiser** ou bien de **limiter leur conservation**, c'est-à-dire soit les **stocker selon une durée déterminée**, soit les **supprimer définitivement**.
A noter que le consentement n'est pas nécessaire lorsque ces données sont collectées pour l'exécution d'un contrat (ex : contrat de vente, de location, de travail etc.) ou de **mesures précontractuelles** comme un **devis**.

RECOMMANDATION N°3 : collecter les données strictement nécessaires et respecter le droit des personnes.

Il est vivement conseillé à l'assureur de ne traiter uniquement les données **strictement nécessaires** pour atteindre la finalité qu'il s'est fixé. C'est la raison pour laquelle nous ne sélectionnerons exclusivement les champs strictement utiles au futur traitement qui en sera fait. A savoir les champs suivants : **Id_client** sous forme d'index, **usage_vehicule**, **type_vehicule**, **points_perdus**, **age_vehicule**, **type_conduite**, **formule**, **date_demande**, **etat_dossier**, **date_naissance**, **tarif_devis**, **revenus**, **nombre_enfants**, **enfant_conduite_accompagnee**, **est_rouge.**

Dev'immédiat devrait également rappeler à ses clients leur droit concernant la maîtrise de leurs données. C'est-à-dire que l'assureur doit faire preuve de **transparence** en informant ses clients de l'utilisation des données les concernant ainsi que de la manière dont ils peuvent exercer leur droit. A savoir qu'ils ont entre autres un **droit d'accès**, de **rectification**, de **suppression** ou **d'opposition**.

RECOMMANDATION N°4 : limiter la conservation des données.

Les anciennes données de prospection commerciale, **stockées depuis 7 années**, ne doivent pas être conservées aussi longtemps par l'assureur. C'est la raison pour laquelle il est important de mettre en place un **processus de suppression ou d'archivage limité dans le temps** des données du CRM.

RECOMMANDATION N°5 : sécuriser les données traitées.

Des mesures doivent être mises en œuvre par l'assureur pour prévenir les risques d'atteintes à la sécurité des données. De quelle manière ? Nous pouvons nous appuyer sur le **guide de la sécurité des données personnelles** rédigé par la **CNIL**. Celui-ci se fixe les objectifs suivants : **sensibiliser** et **authentifier** les utilisateurs, gérer les **habilitations**, **tracer les opérations** et gérer les incidents, **sécuriser les postes de travail**, **protéger le réseau informatique interne**, **sécuriser les serveurs** et les **sites WEB**, effectuer des **sauvegardes**, **encadrer la maintenance des logiciels**, **chiffrer les informations**, **anonymiser les données**.