DEV'IMMEDIAT

RECOMMANDATIONS POUR ASSURER LA CONFORMITE AU REGLEMENT GENERAL DE PROTECTION DES DONNEES (RGPD).

Projet : Collecter des données en respectant les normes RGPD.

Rédigé par : Milaine GUIAGAING

Date : 10/08/2023

CONTEXTE ET RECOMMANDATIONS

DEV'IMMEDIAT est une filiale de l'assurance automobile dont le métier est de faire de la prospection commerciale et de la marge sur la vente des contrats. A cet effet ,elle collecte et manipule beaucoup de données au quotidien. Elle fait face à un problème de conformité au RGPD. Notons qu'à ce jour aucun système de gouvernance de données n'est implanté dans cette société.

Notre rôle consiste donc à les accompagner vers une solution de gestion de la conformité au RGPD. Pour ce faire, nous nous référerons à la CNIL et proposerons cinq (05) recommandations à mettre en place immédiatement.

Après avoir pris connaissance de la base de données, des règles de conformité du RGPD ainsi que des attentes de la société, il en ressort les éléments suivants :

1 La minimisation des données

« Seules les données strictement nécessaires pour atteindre la finalité peuvent être collectées et traitées ».

Les données d'identification, les données relatives à la gestion du contrat, à la situation familiale, à la situation économique, patrimoniale et financière, etc. doivent être traitées uniquement lorsqu'elles sont pertinentes et strictement nécessaires au regard de l'objectif poursuivi par le traitement. C'est par exemple le cas du nom du client, du nombre d'enfants, de la valeur de la résidence principale du client.

Le traitement de certaines catégories de données telles que le Numéro de sécurité sociale est soumis à des restrictions particulières, son utilisation est strictement interdite en dehors des cas d'usage visés par décret .

2 La protection particulière des données sensibles

« Les données sensibles concernant la santé, les opinions politiques ou religieuses… ne peuvent être collectées et traitées que dans certaines conditions ». Le RGPD liste ces conditions et interdit de recueillir ou d'utiliser ces données en dehors de celles-ci.

Pour appliquer donc ce principe, les données de santé telles que le groupe sanguin ne doivent plus être collectées et utilisées.

3 La conservation limitée des données

« Dès que la finalité pour laquelle elles ont été collectées est atteinte, les données selon les cas peuvent être : archivées, supprimées, anonymisées. Dans tous les cas, une durée de conservation doit être définie et appliquée ».

Dans la base de données actuelle certains devis sont anciens et remontent en 2019 . Il faudrait fixer un délai de conservation selon l'utilisation des données en 03 phases :

- Conservation en base active : pour les données collectées pour la réalisation de l'objectif fixé ;
- L'archivage intermédiaire : pour les données qui ne répondent plus à l'objectif fixé mais qui présentent encore un intérêt administratif pour l'organisme ou doivent être conservées pour répondre à une obligation légale ;
- L'archivage définitif : pour les données qui peuvent être archivées sans limitation de durée.

4 L' Obligation de sécurité

« Des mesures doivent être mises en œuvre pour prévenir les risques d'atteinte à la sécurité des données, assurer la sécurité des données traitées ».

Quelques précautions élémentaires qui devraient être mises en œuvre de façon systématique sont :

- Sensibiliser et authentifier les utilisateurs : chaque utilisateur doit être doté d'un identifiant qui lui est propre;
- Gérer les habilitations : définir les profils d'habilitation et faire valider chaque demande d'habilitation par un responsable, supprimer les permissions d'accès dés qu'un utilisateur n'est plus habilité ;
- Sécuriser les postes de travail, l'informatique mobile, les serveurs, les sites web ;
- Archiver de manière sécurisée,
- Protéger les locaux .

5 Les droits des personnes

« Les personnes bénéficient de nombreux droits qui leur permettent de garder la maitrise de leurs données : Droit d'accès, Droit de rectification, Droit de suppression, Droit d'opposition, Droit à la portabilité, Droit à la limitation du traitement».

L'entreprise doit donc mettre à leur disposition des moyens pour exercer leurs droits et prévoir dans ses systèmes informatiques les outils techniques qui permettront la bonne prise en compte de leurs droits. Préparer en amont la façon dont ils la contacteront et dont elle traitera leurs demandes lui permettra de gérer efficacement l'exercice de ces droits.