DEV'IMMEDIAT

CONTEXTE ET RECOMMANDATIONS

La société Dev'Immediat est une entreprise spécialisée dans le courtage d'assurance automobile. Dans le cadre de son activité elle s'est constituée une base de données regroupant différentes informations sur ses clients pour établir des devis.

La société n'a pas élaboré de processus ou méthodologie pour le traitement et la protection de ses données, ce qui a entraîné une sanction de la CNIL pour non-respect des règles du Règlement Général sur la Protection des Données (ci-après dénommé « RGPD »), portant sur une limitation temporaire de traitement des données durant 6 mois. La société Dev'Immediat a sollicité notre intervention afin de se mettre en conformité avec les règles du « RGPD ».

Le présent document a pour objectif d'identifier dans le fichier « Base_client » les informations susceptibles d'être en violation avec les règles du « RGPD » pour ensuite préconiser des recommandations en vue de mettre le fichier en conformité avec la réglementation actuelle.

Pour ce faire, après avoir pris connaissance des règles du « RGPD » et après avoir pris connaissance des informations contenues dans la base de données,

Il en ressort les recommandations suivantes :

1. Minimisation des données :

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

Pour respecter ce principe, il faudrait ne collecter que les données étroitement liées et strictement nécessaires pour réaliser le but pour lequel elles ont été collectées.

En l'occurrence, certaines informations contenues dans le fichier n'ayant aucune utilité pour une prospection commerciale en vue d'établir des devis pour une assurance automobile, il faudra donc supprimer les informations telles que : nombre d'enfants, revenus, valeur de la résidence principale…etc.

2. Protection particulière des données sensibles :

« Les données sensibles concernant la santé… ne peuvent être collectées et traitées que dans certaines conditions ».

Le RGPD liste précisément les organismes autorisés à collecter ces données ainsi que la finalité et les conditions dans lesquelles ces données sont collectées.

En l'occurrence, il faudrait supprimer l'information de santé relative au groupe sanguin.

3. 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 »

En l'occurrence, il faudrait fixer une date limite de conservation des données collectées à compter de la date de l'enregistrement de la demande du client.

En outre, certaines données datent de 2019, ainsi une fois arrivées à échéance il faudra choisir le sort qu'on souhaite leur réserver en fonction de l'utilité qu'elles auront au cas par cas, soit les archiver, supprimer ou anonymiser.

4. Obligation de sécurité :

« Des mesures doivent être mises en œuvre pour : Prévenir les risques d'atteinte à la sécurité des données et assurer la sécurité des données traitées »

Dans le cas actuel il est préconisé de mettre en place des procédures de sécurité techniques comme : sécuriser les serveurs et site internet, archiver de manière sécurisée. Mais également, des procédures de sécurité organisationnelles comme : authentifier les utilisateurs avant de leur donner accès et gérer les habilitations.

5. Droit des personnes :

« Les personnes bénéficient de nombreux droits qui leur permettent de garder la maîtrise de leurs données : ● Droit d'accès ● Droit de rectification ● Droit de suppression… »

Toute personne dont les informations ont été collectées a des droits qui lui permettent de conserver la maîtrise de ses données. Ainsi il faut lui expliquer comment exercer ces droits, auprès de quel service, par quel moyen, dans quel délai…etc.

Par ailleurs, le délai de réponse concernant l'exercice de ses droits tel qu'une demande de rectification ne doit pas dépasser un mois à compter de la date de la demande de rectification.