Recommandations sur les règles de gestion des données personnelles selon le Règlement Général de la Protection des Données (RGPD)

# Recommandation n°1 : Informations aux clients

Bien que les données soient collectées dans le cadre d’un contrat de prestation de service, il est essentiel d’informer les clients du traitement des données.

Pour ce faire, une politique RGPD ainsi qu’un registre des traitements de données doivent être facilement accessibles à toutes les parties prenantes et doivent être rédigées de manières claires et compréhensibles de tous.

* Pour des raisons de transparence Il est nécessaire de fournir les informations suivantes :
* Identité du responsable du traitement des données
* Identité du DPO
* Finalités des traitements
* Bases juridiques des traitements ou preuves des consentements
* Liste des droits des personnes concernées
* Durée de conservation des données
* Liste des mesures de sécurité
* Information sur les éventuels transferts de données
* Explication de la procédure de plainte

# Recommandation n°2 : Sélection des données

Nous n’avons plus le droit de sélectionner un maximum de données « au cas où ». Le RGPD nous oblige à prendre uniquement le nécessaire par rapport au traitement prévu.

Les données sensibles ne doivent pas être collectées, sauf dans certains cadres très déterminées. Les données sensibles sont les données suivantes :

* Origine raciale ou ethnique
* Opinions politiques
* Convictions religieuses ou philosophiques
* Appartenance syndicale
* Données génétiques ou biométriques
* Données de santé
* Vie sexuelle ou l'orientation sexuelle
* Condamnations pénales ou infractions

# Recommandation n°3 : Fin de vie des donnees

Elles ne doivent être gardées que pour la durée prévue pour le traitement des données ou une durée fixée par la loi. Le traitement terminé, les données doivent soit être détruites, soit être archivées et anonymisées.

* En l’absence de conclusion du contrat d’assurance : 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 : 5 ans à compter de leur collecte ou du dernier contact émanant du prospect

S’agissant de l’archivage, il existe plusieurs niveaux. Les données doivent être conservées sur la base active uniquement le temps du traitement. Ensuite elles doivent être stockées en archivage intermédiaire, le temps d’un éventuel recours. A la fin de ce délai elles doivent être définitivement archivées ou supprimées. Ces trois niveaux d’archivage doivent être attachées à des espaces de stockage physiques distincts.

# Recommandation n°4 : Sécurité des données

Une fois en possession de données personnelles, il est obligatoire mettre en place des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque.

Une analyse d’impact (PIA) est parfois même obligatoire en cas de traitements sensibles (ex : profilage) ou d’utilisation de données sensibles (ex : données de santé).

Une gestion particulière de la sécurité des données doit également avoir lieu en cas de transfert de données, selon si elles sont transférées dans l’Union Européenne ou hors Union Européenne. Un contrat avec les sous-traitants doit généralement être régularisés en cas de traitement hors Union Européenne.

En dehors de ces cas, les mesures techniques et organisationnelle peuvent être les suivantes : chiffrement, politique de gestion des accès, sensibilisation du personnel, stockage physique en dehors des locaux, etc.

En cas de violation de ces mesures de sécurité, il est nécessaire d’informer les victimes de cet incident, éventuellement en informer la CNIL et l’ANSSI, et dans tous les cas, mettre en place des mesures correctives et préventives.

Il faut en également veiller au respect des fondamentaux de la sécurité du système d’information : Intégrité, Confidentialité, Disponibilité. L’intégrité afin que les données soient fiables, justes et ne puissent pas être modifiées sans suivre un procédé défini. Confidentialité, afin que les données ne soient accessibles qu’aux personnes autorisées. Disponibilité, afin que les données soient accessibles aux destinataire le temps défini.

# Recommandation n°5 : Anonymisation et pseudonymisation

Parfois il est nécessaire de traiter des données nominatives et précises, par exemple pour un devis.

Suite à ce traitement les données et après un délai prévu sur la politique RGPD, si les données ne sont pas détruites, elles doivent être anonymisées ou pseudonymisées.

* Une anonymisation consiste à supprimer définitivement tout caractère identifiant à un ensemble de données
* La pseudonymisation implique la modification des données de manière à ce qu'elles ne puissent plus être attribuées à une personne sans l'utilisation d'informations supplémentaires

En l’espèce, une anonymisation consisterait à supprimer une colonne dans une base de données. La pseudonymisation consisterait quant à elle de modifier les données, par exemple, via l’utilisation d’ID, de fourchettes de données ou d’information binaire (oui/non, vrai/faux, etc.)

Si les données sont pseudonymisées, par le biais d’ID, il ne faut cependant pas conserver de règles de correspondances. Si une table de correspondance ID/identité existe, la pseudonymisation ne peut être considérée comme efficace ou recevable.