Le RGPD et les données de santé : Tout ce qu'il faut retenir !

Selon le RGPD, les données de santé sont des données personnelles sensibles

Parmi les données personnelles, il existe des données dites **sensibles.** Il s'agit des données de religion, d'orientation sexuelle mais aussi des données de santé.

Par données de santé, on entend des données relatives à la **santé physique ou mentale.** Il peut s'agir d'informations relatives à une personne physique collectées lors d'une inscription, d'informations obtenues lors d'un test ou un examen d'une partie du corps ou enfin d'informations concernant une maladie.

Ceci englobe certaines données de mesure à partir desquelles il est possible de déduire **l'état de santé** d'une personne. C'est très courant dans les modèles innovants actuels.

Deux exemples de sociétés traitant des données personnelles dans la santé

Doctolib

Plateforme de mise en relation et prise de rendez-vous entre médecin et patients. Doctolib va de plus en plus loin en permettant de transmettre et stocker des documents de type ordonnance ou résultats d'analyses. La plateforme **traite des données personnelles** des patients comme le nom, l'adresse email et des données de santé via les spécialités des médecins visités, les ordonnances de médicaments…

Diabeloop

Permet de piloter la distribution d'insuline pour les patients diabétiques. C'est une véritable révolution pour les patients atteints de diabète. Le taux de sucre dans le sang est mesuré en permanence et l'application diabeloop définit la quantité d'insuline à délivrer. L'application s'appuie sur un modèle de prédiction qui est enrichi par une base de données patient de grande taille. Les données personnelles sont **au cœur de l'activité** de Diabeloop.

Les sujets RGPD les plus fréquemment rencontrés par les acteurs de santé

1/ Hébergement des données de santé en France et chez un hébergeur de données de santé (HDS)

Les données de santé doivent être stockées en France et sur un **serveur HDS.** C'est un principe qui est décrit au-delà du RGPD, dans la loi informatique et liberté. En effet, le RGPD permet quelques spécificités locales notamment dans la santé.

Il est donc clé de **maîtriser ses outils** stockant les données personnelles de santé pour s'assurer qu'ils sont bien sur des serveurs d'hébergeur de données de santé (HDS).

Il est également clé de **maîtriser ses prestataires.** En effet, notamment sur vos sites web, outils digitaux, des prestataires techniques comme l'authentification, les formulaires… exercent un traitement sur des données personnelles de vos utilisateurs.

Il est donc important de réaliser la liste et de vérifier que les données personnelles sont bien stockées en France sur des serveurs HDS. C'est l'un des **éléments clés** réalisé lors d'une mise en conformité RGPD.

2/ Un consentement préalable est nécessaire pour tout traitement de données de santé d'une personne

A l'exception des hôpitaux ou des instituts de recherche, pour pouvoir traiter une donnée de santé d'une personne, son **consentement** doit être recueilli. Cela peut prendre la forme d'une case à cocher ou d'un document à signer par exemple.

Traiter une donnée personnelle n'est pas uniquement le fait de stocker une donnée. Un simple transfert d'information par vos outils, sans stockage, est reconnu comme un traitement de données personnelles.

3/ La recherche médicale nécessite une déclaration ou une demande d'autorisation auprès de la CNIL

Dans le cadre de la recherche médicale, il existe un cadre légal qui peut varier en fonction de plusieurs critères. Notamment s'il s'agit de **recherche "interne" ou "multicentrique".** Cette

dernière nécessite davantage de démarches puisque les données personnelles des patients vont être exposées à davantage d'acteurs. Il faudra, dans ce cas, réaliser une demande d'autorisation "recherche" **(www.entreprendre.service-public.fr/vosdroits/R18457)** ou réaliser un engagement de conformité à la MR-001, MR-002 ou MR-003 en fonction des cas.

La CNIL a réalisé un guide sur le sujet : **Recherche médicale : quel est le cadre légal ? | CNIL**

4/ Des clauses RGPD doivent être intégrées dans les protocoles de recherche

Un **protocole de recherche** doit être établi pour faire de la recherche médicale. Ce document comporte notamment les accords entre les différentes parties. Ces accords définissent les responsabilités de chacun. Des clauses RGPD doivent être rédigées pour bien définir ce qu'il advient de chacunes des données personnelles traitées lors de l'étude. Cela définit également les responsabilités de chaque acteur quant à ces données et potentiellement les niveaux de sécurité à mettre en place pour les sécuriser.

5/ Les sanctions dans la santé adressée par la CNIL sont très lourdes

La santé est le domaine où les contrôles sont les plus fréquents. Les sanctions y sont également les plus **sévères et coûteuses.** C'est en effet un domaine où les déviances peuvent engendrer des discriminations importantes, avoir un impact négatif très fort en cas de fuite de données ou d'exploitation détournée des données.

Par exemple, DEDALUS BIOLOGIE a été condamné à 1,5 m€ d'amende suite à une fuite de données.

6/ Les partenariats avec les hôpitaux nécessitent d'être conforme au RGPD

La conformité RGPD est à présent un **élément essentiel** du fonctionnement des hôpitaux. Lors de l'étude d'un partenaire potentiel, les hôpitaux vont devoir s'assurer que celui-ci est conforme au RGPD. C'est une obligation de l'hôpital pour qu'il soit lui-même en conformité RGPD. Surtout si vous êtes amené à traiter des données patients ou des données des employés de l'hôpital.

7/ Des obligations particulières si vous traitez des données personnelles pour le compte d'un autre acteur.

Si vous êtes amené à traiter des données personnelles pour le compte d'un hôpital ou un autre organisme alors vous êtes **"sous-traitant"** au sens du RGPD.

Cela implique quelques responsabilités:

- Vous devrez ajouter une **clause** dans vos CGV indiquant que vous traitez des données personnelles et que vous prenez la responsabilité en cas de fuite de données.
- Vous devrez tenir à jour un **registre** des activités de traitement en tant que sous-traitant.
- Vous devrez également vous assurer de la conformité de vos **prestataires techniques**, eux même "sous-traitants" mais de votre structure.

8/ Vous avez une plateforme digitale. Vous devez réaliser un "privacy by design"

Votre **produit digital** traite des données personnelles dans le cadre de l'exercice de votre service (exemple : livraison de médicament, transport de patients, prises de rdv…). Vous devez vérifier dès le design du produit ou à minima lors de votre mise en conformité RGPD, la conformité du produit digital.

C'est-à-dire,

- Est-ce que les durées de conservation sont respectées ?
- Les consentements nécessaires sont-ils en place ?
- L'information des utilisateurs sur les traitements réalisés est-elle suffisante ?
- La sécurité technique des données est-elle suffisante au regard de la sensibilité des données ?
- Les prestataires techniques du produit digital sont-ils conformes ?