QUELLES FORMALITÉS POUR LE TRAITEMENT DE DONNÉES DE SANTÉ ?

Vous souhaitez proposer un service contenant des données de santé et vous vous interrogez sur les démarches à suivre? Voici quelques informations utiles :

Qu'est ce qu'une donnée de santé à caractère personnel ?

On entend par "donnée de santé", les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne. (**Art 4 du RGPD**).

Les données de santé font partie des " **catégories particulières** " de données personnelle dont le traitement est, par principe, interdit (Art 9 RGPD).

Quelles formalités ?

Deux régimes de formalités à accomplir auprès de la CNIL demeurent :

- **Le régime d'autorisation** pour les traitements présentant un intérêt public, les traitements automatisés dont la finalité est l'étude ou la recherche dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention.
  En matière de recherche, le responsable de traitement peut toutefois être exonéré de ce régime d'autorisation dés lors que le traitement est en parfaite conformité avec un référentiel établi par la CNIL. www.cnil.fr/fr/les-referentiels-et-methodologie-de-reference-sante

- **Le régime de la demande d'avis** sur un projet d'acte réglementaire autorisant un traitement de données de santé. A titre d'exemple, les traitements de données de santé comportant le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (NIR) doivent être prévus par un décret cadre, pris après avis motivé et publié de la CNIL. Décret n° 2019-341 du 19 avril 2019

Hormis les cas visés ci-dessus, les traitements de données de santé reposant sur une des bases légales prévues à l'art 9 du RGPD (notamment consentement, intérêt public, etc) peuvent être mis en œuvre, sans accomplir de formalité auprès de la CNIL, sous réserve de respecter les conditions suivantes :

① Réaliser une documentation sur les traitements de données

Renseignez le registre des traitements : vous pouvez utiliser le modèle de registre établi par la CNIL (registre-traitement-simplifie.ods)

Menez une analyse d'impact : pour les traitements présentant un "risque élevé pour les droits et libertés des personnes concernées". Vous pouvez utiliser le logiciel proposé par la CNIL :
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

② Encadrer l'information des personnes concernées

Prenez les mesures appropriées pour informer les personnes dont les données seront traitées par votre société (patients, étudiants, fournisseurs, usagers etc).

Le contenu des informations varie selon deux types de données :

- Les données qui sont collectées directement auprès de la personne concernée (Art 3 RGPD).
- Les données qui ne sont pas collectées directement auprès de la personne concernée (Art 14 RGPD).

③ Formaliser les roles et responsabilités des acteurs

Désignez un délégué à la protection des données : (i) si votre activité fait partie du secteur public, (ii) si votre activité principale amène un suivi régulier et systématique de personnes à grande échelle ou (iii) si votre activité principale amène le traitement à grande échelle de données sensibles

Assurez vous que vos sous-traitants respectent le RGPD : les traitements de données par un sous-traitant doivent être encadrés par un contrat avec le responsable de traitement fondé sur des clauses contractuelles types (CCT) conforme à l'article 28 du RGPD.

Veiller à bien sécuriser le traitement des données de santé

L'exonération d'autorisation préalable suppose également que vous respectiez la sécurisation des données de santé contre toute destruction ou usurpation. Vous devez donc mettre en place des mesures de sécurité adaptées (ex : mot de passe personnel, utilisation d'un système de chiffrement fort en cas d'utilisation d'internet, etc).

Pour vous aider à identifier les mesures de sécurité à mettre en place, vous pouvez consulter le Guide sur la sécurité des données personnelles publié par la CNIL (www.cnil.fr/fr/securité-des-données)

Veiller à héberger vos données de santé dans un environnement HDS

Les données de santé doivent être traitées et sauvegardées par des organismes possédant la certification d'hébergeur de données de santé. L'hébergement des données de santé étant un hébergement spécifique strictement encadré par la loi,, la procédure de certification et le référentiel applicable sont détaillés dans le cadre juridique et règlementaire HDS (https://data.ird.fr/wp-content/uploods/2021/01/HDS cadre-juridique-1.pdf) .

Pour en discuter : Coralline MANIER-GALAS, WOOG & Associés
Avocat au Barreau de Paris
cmanier@woogassocies.com