Le RGPD et les données de santé

Description

L'essor de la digitalisation a fait du traitement des données de santé un point essentiel traité par le Règlement Général sur la Protection des Données (RGPD).

Ce dernier, entré en vigueur en 2018, est venu poser un cadre réglementaire au traitement de ces données et imposer aux organismes une mise en conformité avec le RGPD et les règles établies par celui-ci.

Obtenir un devis gratuit RGPD

Qu'est-ce qu'une donnée de santé ?

Avant toute chose, il convient de définir ce qu'est **une donnée de santé**, en quoi elles sont particulièrement **sensibles** et les **conséquences** de leur particularité.

Définition

L'article 4-15 du RGPD définit les données concernant la santé comme « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ». Elles peuvent être **passées, présentes ou futures.**

Ainsi, on retrouve parmi les données de santé :

- Les informations relatives à une **personne physique**
- Les informations obtenues lors du **test** ou de **l'examen d'une partie du corps**
- Les informations concernant une **maladie** (handicap, risque de maladie, antécédents médicaux, etc)

L'interdiction de traitement des données sensibles

Les données sensibles font partie d'une catégorie particulière de données personnelles et sont encadrées par l'article 9 du RGPD. Elles correspondent à des informations révélant :

- la prétendue origine raciale ou ethnique
- les convictions religieuses ou philosophiques
- l'appartenance syndicale
- le traitement des données génétiques
- les opinions politiques
- les données biométriques aux fins d'identifier une **personne physique** de manière unique

Les données de santé en font également partie, ce qui rend leur traitement **interdit en principe**. On entend par traitement des données de santé, toute opération impliquant l'utilisation de données de santé.

Toutefois, certaines prestations médicales requièrent impérativement le traitement de ces données, c'est pourquoi le RGPD pose de **nombreuses exceptions** à cette interdiction.

Les exceptions à l'interdiction de traitement des données de santé par le RGPD

Le traitement des données de santé est en principe interdit par le RGPD, néanmoins celui-ci est venu poser **deux exceptions** :

- L'obtention du consentement de la personne
- Les exceptions à l'obligation de consentement

L'obtention du consentement de la personne

Le traitement des données de santé est autorisé dans le cas où la personne physique donne son **accord** au responsable de traitement. Il s'agit d'une **des exceptions** ayant été introduites dans le RGPD.

Le recueil du consentement est cependant soumis au respect de quatre critères cumulatifs. Il doit en effet être :

- Libre : il ne doit pas être contraint ni influencé

- Spécifique : il doit correspondre à un seul traitement, pour une finalité déterminée
- Eclairé : il doit être accompagné d'un certain nombre d'informations communiquées à la personne physique
- Univoque : il doit être donné par une déclaration ou tout autre acte positif clair

Attention : Ne sont pas considérées comme **univoques** les cases pré-cochées ou pré-activées, les consentements « groupés », ou encore l'inaction.

Les exceptions à l'obligation de consentement

Hormis **l'obligation de consentement**, le RGPD prévoit d'autres exceptions permettant le traitement des données de santé, notamment :

- La prévention de la santé publique
- La préservation des intérêts vitaux de la personnes physique concernée
- L'appréciation médicale
- La médecine du travail ou la mise en œuvre du respect du pourcentage légal d'emploi de personnes atteintes d'un handicap
- La gestion des systèmes et services de santé ou de la protection sociale

Comment traiter les données de santé en conformité avec le RGPD ?

Plusieurs **obligations** sont imposées par le RGPD aux responsables de traitement des données de santé. On retrouve notamment le principe d'accountability, consistant à mettre en œuvre les mesures nécessaires pour garantir les principes **posés par le RGPD.**

La désignation d'un DPO

L'entreprise réalisant des traitements de données de santé peut avoir l'obligation de désigner un délégué à la protection des données (DPO). C'est le cas notamment lorsque l'entreprise traite des données de santé **à grande échelle.**

En effet, le DPO a pour fonction d'organiser la **mise en conformité** de l'organisme au RGPD. La personne désignée peut être **interne ou externe** à l'entreprise.

La tenue d'un registre des traitements

Les entreprises traitant des données de santé ont également l'obligation de tenir un **registre des traitements**

devant réunir :

- Les informations sur le responsable du traitement et DPO
- Les informations sur les personnes concernées
- Les finalités du traitement
- Les délais de conservation des données
- La description des mesures mises en place pour optimiser la protection des données

La réalisation d'une analyse d'impact des risques relatifs aux données de santé

Le traitement de données de santé peut conduire à des impacts non négligeables sur **la vie privée** ainsi que sur les **droits et libertés** des individus. C'est pourquoi le RGPD impose la réalisation d'une **analyse d'impact** sur le traitement de ce type de données aux responsables de traitement.

Cette analyse doit notamment comporter :

- Les détails sur les opérations de traitement ainsi que le but poursuivi par le responsable de traitement
- Les mesures de protection mises en œuvre pour assurer la protection des données
- Un rapport entre bénéfices et risques causés par le traitement

Attention : La réalisation d'une analyse d'impact des risques n'est nécessaire que si le traitement des données de santé est susceptible d'avoir un impact significatif sur les **droits et libertés fondamentaux** des individus.

Les droits des utilisateurs

Afin de garantir la **protection de leurs données personnelles**, le RGPD prévoit de nombreux droits aux utilisateurs :

- Un droit d'accès aux données
- Un droit de rectification
- Un droit à la portabilité des données en vertu duquel toute personne dispose du droit de récupérer les données qu'elle a fournies à l'organisme collecteur
- Un droit à la limitation du traitement permettant aux personnes concernées de demander sous certaines conditions le gel de l'utilisation de leurs données

A noter : Les responsables de traitements doivent impérativement veiller au respect de ces droits, au risque de s'exposer à des sanctions imposées par le RGPD.

FAQ

Qu'est-ce qu'une donnée de santé ?

Une donnée de santé est une donnée personnelle concernant la santé physique ou mentale d'une personne qui révèle une information sur l'état de santé de celle-ci. Ces données sont considérées comme sensibles par l'article 9 du RGPD. Elles bénéficient donc d'un encadrement spécifique.

Qui peut traiter des données de santé ?

Le traitement des données de santé est en principe interdit. Toutefois, les organismes ayant recueilli le consentement des personnes concernées sont autorisés à traiter les données de santé. Les organismes répondant également aux exceptions posées par l'article 9 du RGPD ont la possibilité de traiter des données de santé.

Comment traiter les données de santé ?

Le traitement des données de santé est soumis à plusieurs obligations en matière de protection des données personnelles. Ainsi, les responsables de traitement doivent notamment nommer un délégué à la protection des données (DPO) et tenir un registre des traitements.