https://ressources.anap.fr/numerique/publication/2623-memento-rgpd

(DGOS)

Mémento RGPD

Sommaire

1. Notions clés

Qu'est-ce qu'une donnée à caractère personnel ?

Le RGPD définit comme une donnée à caractère personnel toute information relative à une personne physique identifiée ou pouvant être identifiée, directement ou indirectement.

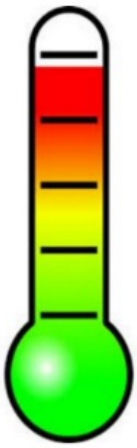
Les données à caractère personnel sont des données qui permettent d'**identifier directement une personne** (le nom, le prénom, une photo, une vidéo, une adresse mail nominative), des données **indirectement identifiantes** (numéro de sécurité sociale, numéro d'employé, identifiant national de compte bancaire, données biométriques, empreinte digitale, image de la rétine, réseau veineux de la main...) ou un **recoupement d'informations** (le fils du notaire hospitalisé dans notre établissement habitant au 11, bd Raspail à Paris).

La définition de donnée à caractère personnel ne vise **que les personnes physiques**, elle ne s'applique pas aux personnes morales.

Exemple : consultantexterne@etablissement.fr n'est pas une donnée à caractère personnel car c'est une adresse mail non nominative, ne rentrant pas dans le champ du RGPD, pour autant que cette adresse fonctionnelle ne puisse être associée à une seule personne ; dans le cas contraire, elle deviendrait alors indirectement nominative.

Qu'est-ce qu'une donnée à caractère personnel ?

Les données de santé font partie des données à caractère personnel dites « sensibles » au sens du RGPD.



DCP sensibles

Données de santé, données génétiques ou biométriques, opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle ou orientation, origine raciale ou ethnique,

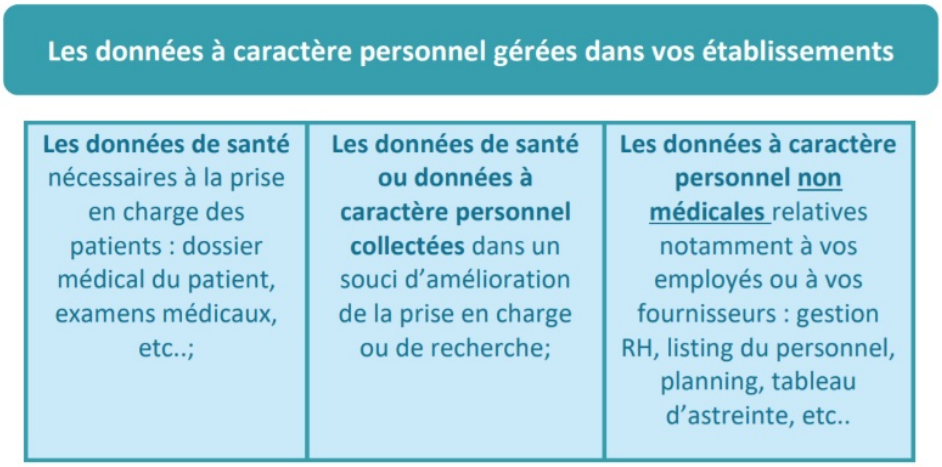
DCP présentant une sensibilité particulière

Numéro de sécurité sociale

DCP courantes

Etat civil (date de naissance, adresse...), données de connexion (adresse IP, journaux, cookies), données de localisation

Vos établissements traitent des données de santé mais pas seulement : le RGPD s'applique également à toutes les DCP que vous traitez, notamment, celles concernant vos employés.

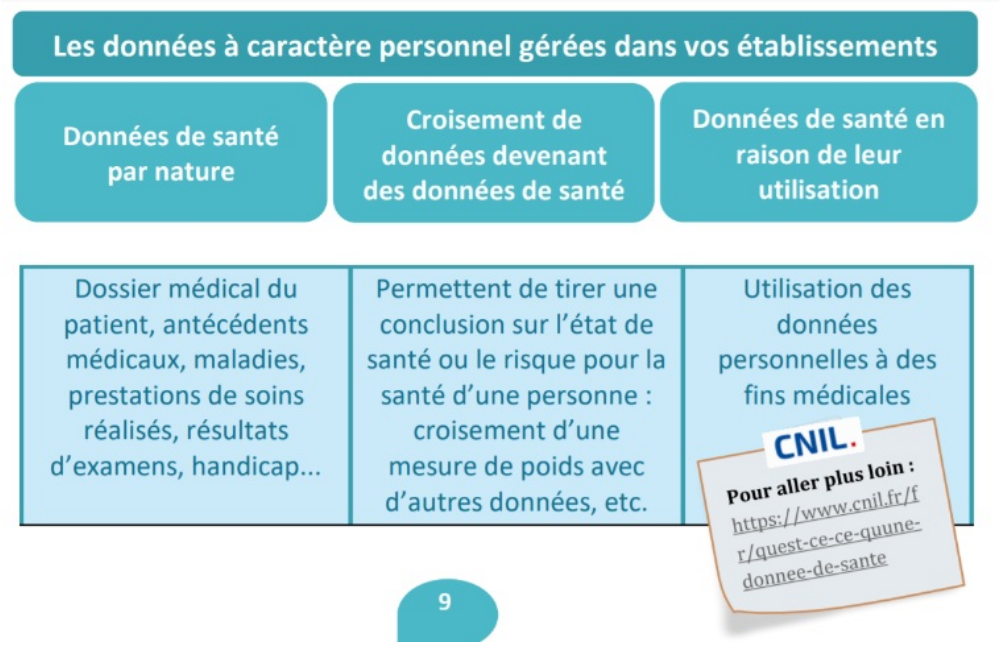


Zoom sur les données de santé

Les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, 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.

Cette définition comprend donc les informations relatives à une personne physique ou identifiable :

- **Collectées** lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services : un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé.
- **Obtenues** lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle y compris à partir des données génétiques et d'échantillons biologiques.
- **Concernant** par exemple, une maladie, un traitement médicamenteux, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source (médecin, autre professionnel de santé, d'un hôpital)



Qui est responsable de traitement au sein d'un établissement de santé ?

Le responsable de traitement est une personne physique ou morale, autorité publique, service ou autre organisme, juridiquement responsable, qui détermine la finalité et les moyens du traitement : cette qualification implique des responsabilités et des sanctions en cas de non-respect de ses engagements.

- La **finalité** est l'objectif principal pour lequel le traitement est réalisé : elle doit être déterminée, explicite et légitime.
- Les **moyens** du traitement désignent les mesures mises en œuvre pour atteindre cette finalité : équipement, matériel informatique, logiciels, services associés, le budget, le personnel…
- Un **co-responsable** du traitement peut intervenir lorsque les finalités et les moyens du traitement sont propres à deux entités ou plus. Un contrat est alors passé pour définir les droits et les obligations réciproques de chaque responsable de traitement. Le responsable de traitement est amené à interagir avec les fournisseurs, les tiers et autres acteurs intervenant dans la mise en œuvre du traitement.

Par exemple, le responsable de traitement pour la gestion des effectifs non médicaux est l'établissement de santé même si la Direction des Ressources Humaines reste en charge de la mise en œuvre du traitement.

Chaque traitement de données à caractère personnel est mis en œuvre sous la responsabilité d'un responsable de traitement.

Le cas des GHT : qui est le responsable de traitement

Selon la nature des traitements, leurs finalités, l'organisation retenue au sein du GHT et dès lors qu'ils déterminent conjointement les finalités et les moyens du traitement, l'établissement support et établissements parties au GHT sont responsables conjoints de traitement (ex : dossier médical partagé, traitement utilisé pour le laboratoire commun de biologie médicale, traitement utilisé pour la pharmacie commune, etc.). Dans ce cas, il est nécessaire de formaliser la coresponsabilité par voie d'accord.

L'accord de coresponsabilité peut prendre la forme d'une convention ad hoc. Il peut également être formalisé dans les documents constitutifs supports du GHT (convention constitutive, règlement intérieur du GHT) ou encore au niveau du registre des traitements.

La coresponsabilité de traitement entre les établissements parties au GHT, selon la nature du traitement et sa finalité, peut donner lieu à l'accomplissement de nouvelles formalités auprès de la CNIL.

Glossaire

CNIL
DCP
GHT
laboratoire
personne
RGPD
risque

Date de parution : 25/06/2019

Télécharger la production