6ÈME ÉDITION

JOURNÉES NATIONALES DES CPTS

Les 9 et 10 octobre 2024

6ème édition des Journées Nationales des CPTS

Fédération Nationale

Contact: coordination@fcpts.org

6ÈME ÉDITION

JOURNÉES NATIONALES DES CPTS

Atelier 3

Le RGPD au cœur des préoccupations des CPTS

Fédération Nationale

Contact: coordination@fcpts.org

RAPPELS

Le Règlement Général sur la Protection des Données – RGPD est un règlement européen entrée en vigueur en mai 2018 qui s'inscrit dans la continuité de la Loi française « Informatique et Libertés » de 1978.

Le RGPD renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.

Le RGPD concerne :

Qui ?

Tout organisme quels que soient sa taille, son pays d'implantation et son activité, peut être concerné.

En effet, le RGPD s'applique à toute organisation, **publique et privée**, **qui traite des données personnelles pour son compte ou non, dès lors** :
- qu'elle **est établie sur le territoire de l'Union européenne**,
- ou que son activité cible directement des **résidents européens**.

QUOI ? Le traitement de données personnelles

Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne peut être identifiée :

• directement (exemple : nom, prénom) ;

• indirectement (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

• à partir d'une seule donnée (exemple : numéro de sécurité sociale, ADN) ;

• à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association).

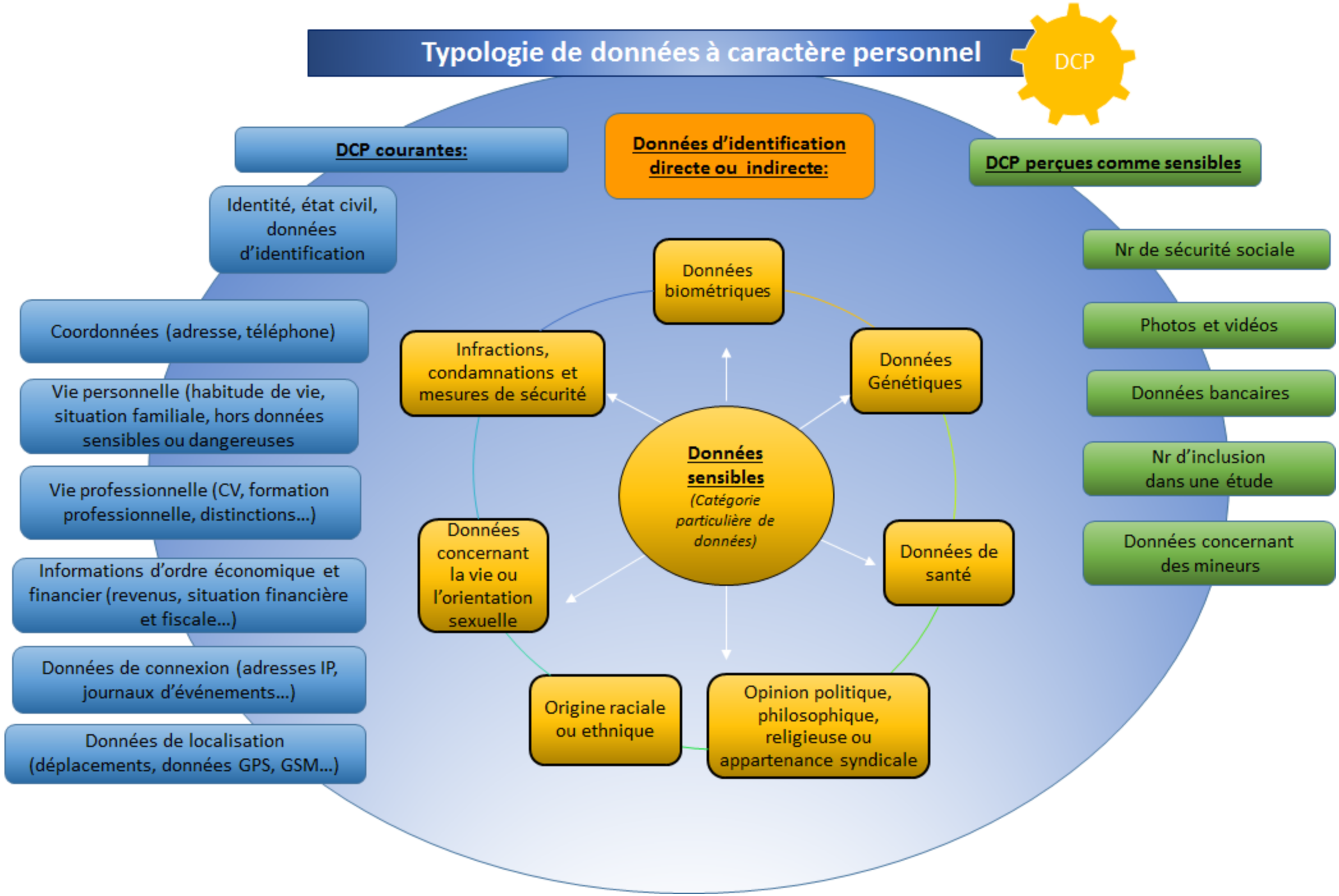
Les données dites sensibles

Les données concernant la santé, les données génétiques et biométriques sont qualifiées par le RGPD de données dites sensibles et en vertu du 1er alinéa de son Article 9, leur traitement est interdit.

L'alinéa 2 liste cependant les exceptions à cette interdiction, notamment :

« **a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques**, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne c
concernée; »

h) **le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale** sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3;


Typologie de données à caractère personnel
DCP
DCP courantes:
Identité, état civil, données d'identification
Coordonnées (adresse, téléphone)
Vie personnelle (habitude de vie, situation familiale, hors données sensibles ou dangereuses
Vie professionnelle (CV, formation professionnelle, distinctions…)
Informations d'ordre économique et financier (revenus, situation financière et fiscale…)
Données de connexion (adresses IP, journaux d'événements…)
Données de localisation (déplacements, données GPS, GSM…)
Données d'identification directe ou indirecte:
Données sensibles
(Catégorie particulière de données)
Données biométriques
Données Génétiques
Données de santé
Opinion politique, philosophique, religieuse ou appartenance syndicale
Origine raciale ou ethnique
Données concernant la vie ou l'orientation sexuelle
Infractions, condamnations et mesures de sécurité
DCP perçues comme sensibles
Nr de sécurité sociale
Photos et vidéos
Données bancaires
Nr d'inclusion dans une étude
Données concernant des mineurs

Un « **traitement** » de données personnelles » : c'est-à-dire ?

Un **« traitement de données personnelles** » est une **opération, ou ensemble d'opérations**, portant sur des données personnelles, **quel que soit le procédé utilisé** (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Un traitement de données doit avoir un objectif, une finalité, c'est-à-dire que vous ne pouvez pas collecter ou traiter des données personnelles simplement au cas où cela vous serait utile un jour. À chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de votre activité professionnelle.

COMMENT ?

Respecter le RGPD suppose de l'organisation et du bon sens !

Il vous faut :

- **Recenser les données collectées** (tenir le registre de traitement des données : cf. https://www.cnil.fr/fr/RGPD-le-registre-des-activites-de-traitement
- **Préciser leur finalité** (le principe est de minimiser les données collectées pour ne stocker que les données indispensables à la finalité poursuivie)
- **Apprécier leur durée de stockage** (en classant les données, certaines sontimpérativement à conserver pendant telle durée : par ex/ en interne : bulletin de salaire: à conserver 50 ans ou jusqu'à l'âge de la retraite du salairé + 6 ans – ref.utile : https://entreprendre.service-public.fr/vosdroits/F10029?profil=societe
- **Organiser leur protection**

Et faire en sorte que toutes vos données soient mises à jour.

N'oubliez pas : en cas de contrôle, vous devez être à même de fournir tous les éléments précités !!!

Les sanctions

En cas de manquements à la règlementation, les sanctions financières pourront s'élever jusqu'à 20 millions d'euros ou jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent – le montant le plus élevé étant retenu,

Étant précisé que le RGPD appréhende, dans sa définition de l'entreprise, les associations qui exercent régulièrement une activité économique (ART.4 RGPD).

Le RGPD ne prévoit donc pas de dérogation particulière pour le monde associatif.

PASSEZ À L'ACTION

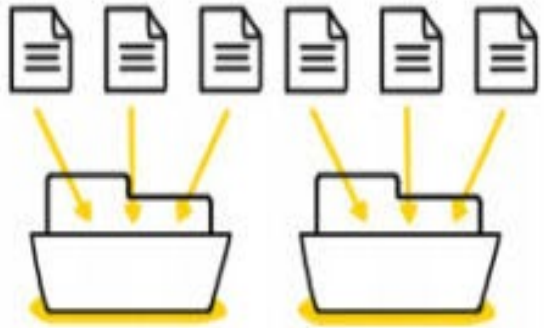
en 4 étapes

1

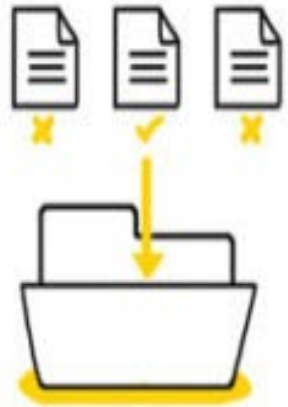
Constituez un registre de vos traitements de données

Je m'assure que les données collectées servent bien l'objectif prévu

2



Faites le tri dans vos données



Je ne collecte que les données dont j'ai vraiment besoin

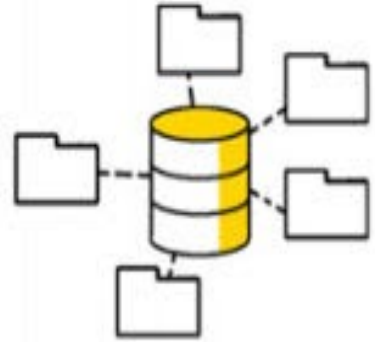
3

Respectez les droits des personnes

Je donne les moyens aux personnes d'exercer leurs droits sur leurs données

4

Sécurisez vos données



Je tiens à jour la liste de mes fichiers

Source : la lettre culturelle

Les CPTS doivent-elles désigner un DPO ?

Les règles impératives diffèrent si les structures ont plus ou moins de 250 salariés et s'il s'agit de structures privées ou publiques.

En effet, toutes n'ont pas l'obligation de désigner en leur sein un DPO :
Le Délégué à la Protection des données (*Data Protection Officer*)

Les responsables de traitement et les sous-traitants devront obligatoirement désigner un délégué :

- s'ils appartiennent au secteur public,
- si leurs activités principales les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
- si leurs activités principales les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

En dehors de ces cas, la désignation d'un délégué à la protection des données sera bien sûr possible.

Les responsables de traitement peuvent opter pour un délégué à la protection des données mutualisé ou externe.

Le délégué devient le véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Il est ainsi chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
- de contrôler le respect du règlement européen et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA) et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Les structures de droit privé de plus de 250 salariés doivent désigner un DPO. **Celles de moins de 250 salariés doivent s'organiser en interne**. La personne morale reste responsable du traitement des données des personnes concernées. La procédure suggérée de mise en oeuvre du RGPD est la même pour tous.

Il n'y a donc pas, en l'état, d'obligation de désignation d'un DPO pour les CPTS, associations de droit privé.

Cas pratique 1 : La CPAM demande la transmission de la liste des adhérents d'une CPTS : ?

Dans sa publication concernant la transmission de données à des tiers dits autorisés, la CNIL précise :

« *Au regard du RGPD, l'enjeu principal pour un responsable de traitement recevant une telle demande est double :* ***veiller à se conformer aux demandes prévues par les dispositions légales et garantir la sécurité des données à caractère personnel traitées.***

En application des articles 5-1-f et 32 du RGPD, ***tout responsable de traitement doit en effet assurer la confidentialité des données en veillant à limiter les accès et transmissions aux seuls acteurs habilités ou autorisés*** *(dont font partie les tiers autorisés lorsqu'une disposition législative ou réglementaire le prévoit).*

Ces exigences doivent conduire le responsable de traitement interrogé à impérativement suivre trois étapes :

1. Vérification de l'existence d'un fondement légal autorisant la demande et la communication de données ;

2. Vérification de la qualité de l'organisme à l'origine de la demande et du périmètre des informations ciblées ;

3. Sécurisation de la communication des données ou des modalités d'accès par le tiers autorisé. »

La CPAM est-elle un « tiers autorisé » ?

En l'état, il n'apparait pas qu'un texte de loi ou un règlement habilite la CPAM en tant que « tiers autorisé », lui permettant d'exiger la transmission de données personnelles de la part des CPTS.

Le seul élément légal évoquant cette transmission de la liste des membres de la CPTS figure en **annexe 1 de l'ACI** (paru au JO du 7 avril 2019 avec son avenant 2 paru au JO du 31 mars 2022), soit **le contrat type relatif au CPTS conclu avec le directeur de la CPAM et le directeur de l'ARS, évoquant la liste des pièces à annexer audit contrat** :

- *« La copie du projet de santé validé par l'ARS*
- *Les statuts de la CPTS*
- *Les contours du territoire d'intervention de la CPTS*
- ***La liste des membres de la CPTS avec leurs statuts : professionnels de santé libéraux, MSP, équipes de soins primaires, équipes de sopins spécialisées, centre de santé, établissements (sanitaires et médico-sociaux), services de santé et services sociaux etc..***

- ***La CPTS doit informer l'organisme local d'Assurance Maladie, une fois par an, des modifications intervenues sur ces éléments et notamment, sur la liste des membres de la communauté professionnelle. »***

Les préconisations de la CNIL

« Les formes que peut prendre une demande de communication de données d'un tiers autorisé sont diverses : il n'existe pas de document ou de formulation type que le responsable de traitement pourrait systématiquement exiger (sauf lorsque le texte le prévoit explicitement).

Lorsqu'un responsable de traitement reçoit une demande exigeant la communication de données à caractère personnel, le premier réflexe à avoir est de s'assurer que la requête se fonde sur une disposition légale en vigueur.

Deux scénarios sont possibles :
1./ Si la demande mentionne une référence légale ou réglementaire précise, alors le responsable de traitement doit vérifier (depuis le site web Légifrance, par exemple) la réalité des dispositions mentionnées ;
2./ ***Si la demande ne mentionne aucune disposition particulière, alors le responsable de traitement doit demander à l'organisme s'il agit en application d'un texte et de préciser la référence légale afin que la vérification précitée puisse être menée.***

Le responsable de traitement ne peut en effet se satisfaire d'une demande uniquement fondée sur des éléments contextuels (nature de l'organisme émetteur, habitudes relationnelles, tournures de phrases impératives, etc.). Il doit s'assurer que l'organisme agit effectivement, au moment de la demande, en tant que tiers autorisé. »

« Adresser des données à caractère personnel à un organisme sans qu'une telle vérification n'ait été réalisée expose le responsable de traitement à deux risques susceptibles de conduire aux sanctions précitées :

- *Transmettre des données à caractère personnel à des personnes non autorisées ;*
- *Transmettre des données sans respecter le cadre établi par les dispositions légales relative au droit de communication exercé. »*

Alors, que faire ?

L'élément légal sur lequel se fonde la CPAM pour exiger la transmission de ces données n'apparait pas clairement à ce jour.

L'exigence dans le cadre de l'accord de la transmission d'une liste de membres de la CPTS assortie de leurs statuts aurait pu apparaitre fondée si la CPAM pouvait revendiquer la qualité de « tiers autorisé », ce qu'elle ne semble pas être à ce jour, sachant qu'en tout état de cause, **la finalité de la transmission de ces données n'est pas connue** : la CPAM ne parait pas avoir à ce jour indiqué l'usage qu'elle entend faire de ces données, la durée de conservation de ces données ni la possibilité pour les personnes physiques concernées d'avoir un droit d'accès pour modification, rectification voire suppression, comme d'usage en matière de données personnelles.

Les CPTS se doivent d'être rigoureuses voire exemplaires dans la gestion des données personnelles et ne peuvent prêter le flan à la moindre critique de leurs membres.

Une suggestion ?

L’idée est de clarifier les relations entre les CPTS et tout organisme réclamant la liste de ses membres.

Ainsi, en cas de demande de tout organisme, les CPTS pourrait répondre :

« *En application des dispositions du RGPD concernant la transmission de données personnelles à un tiers, nous vous remercions de bien vouloir nous préciser l’élément légal ou règlementaire vous autorisant à formuler une telle demande afin de vérification ainsi que la ou les finalité(s) pour lesquelles vous souhaitez recueillir ces données, leur durée de conservation, et les modalités d’accès, d’opposition, de rectification et d’annulation des données ainsi transmises.* »

CAS PRATIQUE N°2 – Le traitement de données dites sensibles par les CPTS

Certaines CPTS indiquent traiter des données patients, qui sont des données sensibles.

D’autres font en sorte que ce soit les professionnels de santé qui échangent en eux ces données, à l’aide des logiciels cryptés dont ils disposent, pour la sécurisation de la circulation de ces données.

La question est : les CPTS sont-elles habilitées à traiter ces données ?

Que dit la CNIL sur le traitement des données de santé ?

Tout d'abord, vous devez identifier si votre traitement relève d'une des hypothèses excluant l'accomplissement de formalités :
L'article 65 de la loi Informatique et Libertés prévoit des cas ou l'accomplissement de formalités n'est pas nécessaire. **Cela concerne les traitements suivants** :
•la personne concernée a donné son consentement explicite au traitement de ses données personnelles pour une ou plusieurs finalités spécifiques ;

- L'accomplissement d'une formalité n'est pas nécessaire lorsque la personne a donné son consentement au traitement de ses données de santé (article du 9 RGPD) après avoir été correctement informée.
- Il convient de distinguer la base légale (article du 6 RGPD) sur laquelle est fondée le traitement, de la dérogation qui permet de traiter des données sensibles (article du 9 RGPD) qui sont complémentaires et qui doivent toutes deux être justifiées.
- Le consentement au traitement des données doit être distingué du consentement à l'acte de soins ou du consentement à la participation à une étude.

•le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

•le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité prévue par les textes ;

•le traitement porte sur des données personnelles qui sont manifestement rendues publiques par la personne concernée ;

•le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;

•le traitement est nécessaire aux fins de la **médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé**, ou par une autre personne à laquelle s'impose – en raison de ses fonctions – l'obligation de secret professionnel ;
À savoir : il s'agit de l'exception mobilisée dans le cadre de la prise en charge des patients par les professionnels de santé.

•**les études internes, répondant à trois conditions cumulatives**. Il doit s’agir d’une étude réalisée :

- à partir de données recueillies dans le cadre de la prise en charge individuelle des patients concernés ;
- par les personnels assurant ce suivi ;
- et pour leur usage exclusif ;

•les traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale ;

•les traitements mis en œuvre par les organismes chargés de la gestion d'un régime de base d'assurance maladie dans le cadre de leurs missions ainsi que la prise en charge des prestations par les organismes d'assurance maladie complémentaire ;

•les traitements mis en œuvre par l’État ou les agences régionales de santé (ARS) ;

•les traitements mis en œuvre par l’État pour la conception, le suivi ou l’évaluation des politiques publiques ou la collecte, l’exploitation et la diffusion de statistiques en santé.

Pour ces traitements, aucune formalité auprès de la CNIL n'est requise. Cependant, il est nécessaire de les inscrire dans votre registre des activités de traitement et de réaliser une analyse d'impact relative à la protection des données si nécessaire.

En revanche, **si le traitement envisagé n'appartient à aucune de ces catégories et en dehors de cas spécifiques (par exemple, les traitements créés et encadrés par un acte réglementaire)**, le responsable de traitement devra effectuer des formalités préalables auprès de la CNIL.

ANALYSE

Si l'on considère que les CPTS entrent dans l'une des catégories ci-dessus visées, les CPTS n'auront pas d'autorisation préalable à solliciter.

En revanche, le secret professionnel s'impose au personnel des CPTS tout comme la transmission de ces données via un logiciel protégeant les données.

En l'état, il n'apparait pas que le traitement de ces données entrent dans le cadre des autorisations hors recherche dont la procédure est développée sur le site de la CNIL.