

# Le règlement européen sur la protection des données personnelles (RGPD) vous concerne

## EN BREF

- ▶ 25 mai 2018 : le règlement européen sur la protection des données personnelles (RGPD) s'applique à tous les organismes et dans tous les secteurs d'activité.
- ▶ Son objectif : renforcer les droits des citoyens européens vis-à-vis de la protection de leurs données personnelles, dans un environnement numérique croissant et mondialisé.
- ▶ Ses impacts : les formalités auprès de la CNIL sont remplacées par une responsabilisation accrue des organismes (et de leurs sous-traitants) qui doivent assurer une protection optimale des données à chaque instant, et être en mesure de la démontrer en documentant leur conformité. Les contrôles et les sanctions sont renforcés.

## Un nouveau cadre juridique qui s'applique à tous

Les données personnelles sont protégées en France par le **cadre juridique** de la loi n°78-17 du 6 janvier 1978 dite « loi Informatique et Libertés », qui **évolue** avec l'entrée en vigueur **en mai 2018** du règlement européen n°2016/679 du 27 avril 2016 sur la protection des données personnelles (RGPD).

Le RGPD est un texte européen, commun à tous les pays membres de l'Union européenne, **qui concerne tous les organismes**, tant publics que privés, **et tous les secteurs d'activité**.

Il renforce les droits des personnes et accroît les obligations des **responsables de traitement** et des **sous-traitants**.

Il s'applique aux **traitements de données personnelles**, réalisés sur **support informatique** (logiciels, applications, bases de données, sites web...), mais également sur **support papier**.

**Le secteur de la santé** est d'autant plus impacté par ce texte que les données de santé bénéficient d'un régime de protection renforcé, les données de santé étant considérées comme des données sensibles. A cela s'ajoutent les obligations additionnelles prévues par le code de la santé publique, relatives aux données de santé couvertes par le secret médical (règles relatives à l'hébergement externalisé des données de santé, télémédecine, identifiant national de santé, etc.).

Le RGPD instaure pour la première fois une définition des données 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* ». Il précise que les données de santé peuvent se rapporter à l'état de santé (passé, présent ou futur) d'une personne, par exemple les données collectées dans un contexte médical (prestation de soins de santé, résultats de tests,...), ainsi que les données permettant d'identifier une maladie ou un risque de maladie, un handicap, des antécédents médicaux, un traitement clinique, un état physiologique ou biomédical.

Les données génétiques et les données biométriques sont également définies par le RGPD.

## Des obligations majeures renforcées et nouvelles

Le RGPD impose à tous les acteurs traitant des données personnelles, qu'ils soient responsables de traitement ou sous-traitants, **certaines obligations majeures**, dont ils doivent pouvoir **démontrer le respect à tout moment** :

R

**La tenue d'un registre interne**, qui décrit les traitements mis en œuvre au sein de l'organisme. Les formalités déclaratives auprès de la CNIL étant supprimées, la mise en conformité d'un traitement de données personnelles passe principalement par la tenue de cette documentation interne (registre, analyse d'impact, audits réguliers...).

Dans certains cas, la mise en œuvre du traitement reste toujours soumise à l'autorisation préalable de la CNIL.

La tenue du registre devient **obligatoire pour tous**. Auparavant, seuls les organismes disposant d'un correspondant informatique et libertés (CIL) devaient tenir cette documentation des traitements.

R

**La désignation d'un délégué à la protection des données (DPD ou DPO)**, désormais obligatoire pour les organismes publics ainsi que pour tout organisme mettant en œuvre des traitements créant des risques particuliers pour les personnes (par exemple le suivi des personnes ou le traitement de données sensibles - telles des données de santé - à grande échelle). Le DPD est chargé d'informer et de conseiller son organisme sur ses obligations, de contrôler le respect du RGPD et du droit national et de coopérer avec l'autorité de contrôle. La mutualisation d'un DPD pour plusieurs organismes est possible.

La désignation d'un DPD, qui remplace le CIL dont la désignation était facultative, **devient obligatoire pour de nombreux organismes** (tous les organismes publics et autres organismes dont l'activité est décrite à l'article 47 du RGPD).

- **La sécurisation juridique, technique et organisationnelle des traitements**, impliquant notamment :

- o la **mise en œuvre de processus** permettant d'assurer la sécurité et la

N

confidentialité des données, ainsi que le respect des droits des personnes (procédures internes, mentions et processus d'information, clauses contractuelles avec les sous-traitants et les partenaires, adhésion à des codes de conduites, réalisation de certifications...);

- o la réalisation d'un **document d'analyse de l'impact du traitement de données sur la vie privée** pour les personnes avant certains traitements sensibles.

N

R

**L'intégration des problématiques liées aux données personnelles dès le début d'un projet** : le RGPD impose de prendre en compte les principes de protection des données personnelles dès la conception d'un système d'information (« *Privacy by design* »), et dans le paramétrage par défaut de ces systèmes (« *Privacy by default* »).

## S'adapter aux exigences du RGPD

L'entrée en vigueur du RGPD implique ainsi un renforcement des obligations pour tous les organismes, qui s'accompagne d'un rehaussement des sanctions applicables en la matière ainsi que d'une meilleure compréhension pour les personnes des droits dont elles disposent concernant leurs données personnelles.

Les impacts du RGPD s'étudient dans la continuité des actions d'ores et déjà portées par l'organisme pour gérer sa conformité juridique et les risques de sécurité de son système d'information.

R

Obligation renforcée

N

Nouvelle exigence

# Établissements de santé : préparez-vous au règlement européen sur la protection des données personnelles (RGPD)

## EN BREF

- ▶ Tous les établissements de santé sont concernés par le RGPD en tant que responsables de traitement de données personnelles dans leur organisme, et parfois également comme sous-traitants (dans le cadre d'un groupement par exemple).
- ▶ Le RGPD porte sur toutes les données personnelles issues des activités de l'établissement de santé, et pas uniquement sur les données de santé générées par la prise en charge des personnes.
- ▶ De nombreuses actions sont à mener dès à présent, y compris pour les établissements qui disposent déjà d'un correspondant informatique et libertés (CIL). En effet, le règlement entre en application en mai 2018. Ces actions s'inscrivent dans la démarche globale de gestion des risques portée par l'établissement pour améliorer la qualité et la sécurité des soins, et s'intègrent notamment aux procédures de conformité de l'établissement, ainsi qu'à la gestion des risques de sécurité des systèmes d'information de l'établissement.

## Identifiez la portée du RGPD dans votre établissement

La démarche de mise en conformité au RGPD concerne tous les établissements de santé.

Les obligations à prendre en compte varient en fonction de la qualification du rôle de l'établissement et de la nature des traitements et des données utilisées.

2 qualifications  
juridiques

D'une manière générale, l'établissement est **responsable de multiples traitements de données personnelles**, impliquant ou non des données de santé.

Dans certains cas, l'établissement peut être considéré comme un **sous-traitant**, lorsqu'il agit pour le compte d'un tiers, notamment dans le cadre de certains groupements.

Nature des données  
traitées par  
l'établissement

L'établissement traite des **données personnelles qui ne sont pas des données de santé** (les données de ressources humaines par exemple) pour lesquelles le RGPD s'applique.

L'établissement de santé collecte, génère et traite également des **données de santé**. De façon identique au régime actuel, le RGPD fixe un principe d'interdiction de collecte de ces données en raison de leur sensibilité. Toutefois, ce principe est assorti de plusieurs exceptions, comme dans la loi Informatique et Libertés. A titre d'exemple, il est possible de créer un traitement de données de santé à caractère personnel lorsque la personne concernée donne son consentement exprès. Autre fondement possible utilisé dans le cadre de l'activité quotidienne des établissements de santé, les traitements créés pour une finalité relative :

- aux diagnostics médicaux, à la prise en charge sanitaire ou sociale, ou à la gestion des systèmes et des services de soins de santé ;
- à l'intérêt public dans le domaine de la santé publique, aux fins de recherche, de la médecine préventive ou de la médecine du travail.

## Vos obligations relatives à la protection des données de santé de vos patients

---

L'établissement de santé est soumis à plusieurs obligations en ce qui concerne les modalités de mise en œuvre de ses traitements de données de santé.

De façon générale, il doit respecter les principes de protection des données de santé (finalité, pertinence et proportionnalité, conservation limitée, sécurité et confidentialité et respect des droits des personnes).

L'établissement doit également adapter ses procédures à l'entrée en vigueur du RGPD, et notamment :

- **Tenir une documentation interne**, décrivant les traitements mis en œuvre et les mesures de mise en conformité de ces traitements. Dans certains cas (notamment les traitements de recherche), il doit solliciter l'autorisation de la CNIL avant de mettre en œuvre son traitement de données personnelles.
- **Désigner un délégué à la protection des données (DPD ou DPO) dans une majorité de cas** : les établissements publics de santé sont tous concernés par cette obligation, tandis que les établissements privés de santé sont potentiellement concernés, selon qu'ils mettent ou non en œuvre un traitement de données sensibles « à grande échelle ». La mutualisation d'un DPD entre plusieurs établissements est possible.
- **Assurer le respect des droits des personnes** : le RGPD renforce les droits traditionnels des personnes concernées par un traitement (droit à l'information sur le traitement, droit d'accès, de rectification, de suppression, ou encore droit d'opposition pour motif légitime) qui sont spécifiquement adaptés au secteur de la santé par le code de santé publique. **De nouveaux droits sont prévus**, notamment le droit à la portabilité des données et le droit à l'oubli, qui nécessitent parfois des fonctionnalités spécifiques à prévoir dans les systèmes d'information de l'établissement.
- **Réaliser une analyse de l'impact du traitement de données** portant tant sur les risques sécurité et technique que sur les risques juridiques pour les personnes, avant de mettre en œuvre certains traitements, notamment ceux portant sur des données de santé à grande échelle.
- **Porter une attention particulière à l'encadrement contractuel des prestations des tiers fournisseurs de service** :
  - o dès que l'établissement de santé a recours à un prestataire de service dont la prestation implique le traitement des données de santé, il doit signer avec le prestataire un contrat (ou, le cas échéant, passer un marché public) décrivant précisément le contenu des prestations (obligations de sécurité et respect des clauses obligatoires prévues par l'article 28 du règlement) ;
  - o dans le cas où l'établissement de santé n'est pas maître des moyens de travail mis à sa disposition (solutions de type progiciel ou Saas, fournies « telles quelles » par le prestataire), il doit autant que possible inclure dans le contrat avec son prestataire des clauses garantissant que celui-ci respecte les principes de la loi Informatique et Libertés.
- **Mettre en place des procédures** permettant de garantir **la sécurité et la confidentialité des données**, dans le respect de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S), et de respecter les obligations liées à la **conservation des données** (fixer une durée de conservation, organiser les modalités d'archivage, assurer la capacité de restitution des données de santé).
- **Signaler auprès de la CNIL des incidents de sécurité** impliquant des données personnelles (obligation qui s'ajoute à l'obligation actuelle de signalement des incidents de sécurité des systèmes d'information de santé prévue à l'article L.1111-8-2 du code de la santé publique).

# Se préparer en 6 étapes

La CNIL propose et outille une démarche en 6 étapes :

[www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes](http://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes)

- 1 **Désigner un pilote** : une personne disposant de relais internes et chargée de s'assurer de la mise en conformité au règlement européen ;
- 2 **Cartographier vos traitements de données personnelles** ;
- 3 **Prioriser les actions à mener** au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées ;
- 4 **Gérer les risques**, en menant une étude d'impact sur la protection des données pour chacun de vos traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées ;
- 5 **Organiser les processus internes** qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement ;
- 6 **Documenter la conformité au règlement** et la tenir à jour.

Ces actions s'inscrivent dans la démarche globale de gestion des risques portée par l'établissement pour améliorer la qualité et la sécurité des soins, et tout particulièrement dans le cadre de la gestion des risques de sécurité de système d'information de l'établissement.

## Pour en savoir plus

- CNIL : Le règlement européen n°2016/679 du 27 avril 2016 sur la protection des données personnelles (RGPD) [www.cnil.fr/fr/reglement-europeen-protection-donnees](http://www.cnil.fr/fr/reglement-europeen-protection-donnees)
- CNIL : Comprendre le règlement européen [www.cnil.fr/fr/comprendre-le-reglement-europeen](http://www.cnil.fr/fr/comprendre-le-reglement-europeen)
- CNIL : Ce qui change pour les professionnels [www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels](http://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels)
- CNIL : Se préparer en 6 étapes [www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes](http://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes)