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 : des 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 dès mai 2018

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 accroit 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 :

N
- la **mise en œuvre de processus** permettant d'assurer la sécurité et la 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…)
- 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.

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* »).

Préparer son organisme dès à présent

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.

Pour plus d'informations :

- ***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***
- ***CNIL : Comprendre le règlement européen*** ***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***
- ***CNIL : Se préparer en 6 étapes*** ***www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes***

R Obligation renforcée

N Nouvelle exigence