15/05/2018

LE RGPD ET L'OFFICINE

UNE NOUVELLE REGLEMENTATION

A la date du 25 Mai 2018, le Règlement Général sur la Protection des Données (RGPD) entrera en vigueur et créera de nouvelles obligations pour l'officine ainsi qu'un arsenal de sanctions pouvant monter jusqu'à 20 millions ou 4% du chiffre d'affaire.

Ce règlement repose sur deux principes fondamentaux : Responsabiliser les entreprises sur le traitement des données personnelles, et garantir un panel de droit aux personnes concernées par ces traitements.

Nous contacter
privacy@caduciel.com

LE PHARMACIEN, RESPONSABLE DE TRAITEMENT

Le RGPD responsabilise les entreprises en les nommant **responsable de traitement** dès lors qu'une entreprise effectue un traitement (collecte, transfert, conservation, utilisation…) de données personnelles (Nom, prénom, adresse mail, numéro de sécurité sociale…).

Au sein de l'officine, le responsable de traitement est le pharmacien. Il manipule des données personnelles, et plus particulièrement des données de santé qui représentent une catégorie de données particulièrement sensible.

Le pharmacien est responsable de la sécurité et de la conformité des traitements.

LES NOUVELLES OBLIGATIONS DU RGPD

Dans l'ordre de créer une véritable réflexion et sécurité des données le RGPD impose plusieurs outils de conformité aux officines:

- **Nomination d'un Data Protection Officer** qui aura pour rôle de contrôler ces activités et la sécurité des données. Ce DPO devra être qualifié et sans conflit d'intérêt avec le responsable de traitement. Il ne devra donc pas être le pharmacien ou une personne mettant en œuvre les traitements.
- La création d'un **registre des traitements** dans lequel figure tous les traitements en fonction de leurs finalités et contenant leurs principales caractéristiques (Données collectées, type de traitement, information, transfert, catégorie de destinataire, sécurité, fondement du traitement…).
- La **réalisation d'analyse d'impact** pour tout traitement sensible, et/ou nouveau (contenant le contexte, les principes fondamentaux, les risques de sécurité et les avis d'un DPO)
- **Informer les personnes** faisant l'objet d'un traitement des caractéristiques et des raisons justifiant ce traitement.
- Permettre aux personnes faisant l'objet d'un traitement d'**exercer leurs droits** à l'accès, à la rectification, à la portabilité et à l'opposabilité des traitements de données.
- **Notifier les violations de sécurité** à la CNIL et aux personnes dans les 72 heures.

DEFINITION D'UNE DONNEE DE SANTE (ARTICLE 4.1 RGPD)

*« Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des **données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée** (…) Sont des données de santé : un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques ; et toute information concernant, par exemple, une maladie, 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, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro. »*

15/05/2018

Responsabiliser les entreprises et offrir des droits aux particuliers.

LE TRAITEMENT DES DONNEES

Le RGPD vient clarifier les grands principes qui doivent régir chaque traitement de données.

Ainsi, la collecte de données personnelles devra dès à présent être :

- ✓ **Loyale :** *Pas de collecte à l'insu de la personne*
- ✓ **Licite :** *Pas de collecte illégale*
- ✓ **Transparente :** *Pas de collecte sans information*

Les finalités/buts de ces traitements devront être :

- ✓ **Explicites :** *Pas de traitement sans but*
- ✓ **Légitimes :** *Pas de traitement sans motifs valables*
- ✓ **Déterminées :** *Pas de traitement sans un usage précis et déterminé*

Le responsable devra veiller à ce que les données soient :

- ✓ **Adéquates :** *Pas de données collectées en masse*
- ✓ **Pertinentes :** *Pas de données collectées sans utilité*
- ✓ **Limitées :** *Pas de données collectées sans nécessité absolue*

De même, la conservation de ces données sera réglementée et devra :

- ✓ **Limitée :** *Pas de conservation illimitée*
- ✓ **Déterminée :** *Pas de conservation sans délai défini*
- ✓ **Sécurisé :** *Pas de conservation en dehors des espaces sécurisés*

DECLARATIONS

Le RGPD vient **supprimer** la majeure partie des **déclarations obligatoires à la CNIL**. Actuellement, les officines avaient à réaliser une déclaration de conformité à la **norme NS-052** concernant la gestion informatique de la pharmacie. La CNIL va dans les mois ou années à venir, définir de nouvelles normes et déclarations obligatoires. Toutefois, toute déclaration faite sous l'égide de la législation antérieure au RGPD seront valides pour une **durée de 4 ans**. Une fois ce délai dépassé, il sera de la responsabilité du pharmacien de faire une **analyse d'impact** pour les traitements sensibles. Il devra toutefois recourir immédiatement aux analyses d'impact pour tous les **traitements nouveaux et sensibles**. L'analyse d'impact permettra de déterminer la dangerosité du traitement et devra en cas de doute, être transmise à la CNIL pour avis. Si le responsable néglige de demander l'avis de la CNIL sur un traitement qui se révélera dangereux, alors une sanction pourra être prononcée.

SECURITE

Aucune sécurité de système informatique n'est infaillible. Cependant, il est possible de réduire les risques de violation de sécurité et c'est sur ce point que le RGPD insiste. Le responsable de traitement est le **garant de la sécurité** des données de son officine. Il doit donc veiller à ce qu'un système **le plus efficace, et le plus adéquate possible** soit mis en œuvre. Pour cela un ensemble de mesures permettent d'assurer une sécurité minimale du système informatique :

- Avoir un **système informatique à jour** (Pas de système d'exploitation obsolète (Windows XP...))
- Avoir un **système anti-intrusion** (Routeur ; pare-feu) et anti-virus à jour (solution complète)
- Avoir un **système de sauvegarde automatique et sécurisé** (solution NAS)
- Avoir un **système de cryptage les données** sortantes de l'officine (télétransmissions, statistiques, etc...)

En savoir plus : https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf