INFORMATIQUES ET LIBERTÉS - PROJET DE LOI

Règlement Général relatif à la Protection des Données

Le Règlement Général relatif à la Protection des Données (RGPD) est une source juridique européenne d'application directe (c'est-à-dire qu'il ne nécessite pas d'être transposé par une loi), et ce à compter du 25 mai 2018. Un projet de loi vient néanmoins d'être déposé afin d'adapter la loi dite "Informatique et Libertés" au droit européen.

En substance, on rappellera que, dans les suites de la loi n° 78-17 du 6 janvier 1978, dite « Informatique et Libertés », d'autres textes nationaux ont été publiés, notamment la loi n° 2014-344 du 17 mars 2014 étendant les pouvoirs de contrôle de la CNIL. Au plan européen, le Règlement visé en référence fait, lui, écho à la Directive 95/46/CE du 24 octobre 1995 et participe de l'harmonisation souhaitée du cadre juridique en matière de protection des données.

La démarche juridique et pratique posée par ce texte tend à remplacer les déclarations ou autorisations auprès de la CNIL par la démonstration, en cas de contrôle, de la conformité des traitements concernés aux principes de sécurité afférents. C'est une « responsabilisation » des acteurs qui est consacrée *(Principe d'Accountability)*.

Chaque acteur doit envisager de se questionner quant au dispositif contractuel et technique qu'il peut avoir en matière de traitement de données (...)

Ce principe est applicable à tous les responsables de traitement de données à caractère personnel et à leurs sous-traitants.
On précisera que ces traitements sont tout autant ceux dédiés aux données des employés de la structure concernée que ceux relatifs à des données de santé. Les SSTI peuvent donc avoir à s'assurer de la conformité de plusieurs types de traitements.
On indiquera ensuite la définition des deux notions-clés en présence :

▶ ***« données à caractère personnel »***, *toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;*

▶ ***« traitement »***, *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.*

On soulignera, en complément, que le responsable de traitement est la personne physique ou morale qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement et qu'un sous-traitant est la personne physique ou morale qui traite les données à caractère personnel pour le compte du responsable de traitement.

A ce titre, les CIL (Correspondant Informatique et Libertés) vont en conséquence être remplacés par des DPO (Data Protection Officer ou Délégué à la Protection des Données), obligatoirement désignés — en interne ou non — par les responsables précités. De plus, on ajoutera que les droits des personnes concernées par ces traitements de données sont redéfinis par le Règlement.

En résumé, chaque acteur doit envisager de se questionner quant au dispositif contractuel et technique qu'il peut avoir en matière de traitement de données et s'assurer de sa conformité avec les principes posés par le RGPD. En cas de manquement avéré, des amendes administratives peuvent être encourues.

En tout état de cause, Présanse ne manquera pas de vous tenir informés des avancées relatives à ce tout récent projet de loi, visé en référence. ■

CERTIFICATION DES HÉBERGEURS DE DONNÉES DE SANTÉ

Référentiel publié par l'ASIP

L'hébergement de données de santé à caractère personnel : de l'agrément des hébergeurs à la certification des SSTI.

On rappellera que, dans le prolongement de la loi dite « Touraine », (n° 2016-41) du 26 janvier 2016 relative à la modernisation de notre système de santé, une ordonnance (n° 2017-27) en date du 12 janvier 2017 a modifié une obligation juridique qui intéresse les SSTI concernant l'hébergement de données à caractère personnel.

En effet, s'agissant de l'hébergement des données de santé, nombre de SSTI ont contracté avec des structures agréées à cet effet et listées en conséquence par l'ASIP.

Or, le principe et les modalités de l'agrément en la matière sont modifiés et ce sera - à compter du 1er janvier 2019 - un mécanisme de certification qui va être mis en place.

De plus, le libellé du nouvel article L. 1111-8 du Code de la Santé publique permet de conclure que les Services eux-mêmes vont avoir à obtenir une telle certification.

En effet, cet article est ainsi rédigé :
« ***Toute personne*** ***qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention,*** *de diagnostic, de soins ou de suivi social et médico-social,* ***pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, réalise cet hébergement dans les conditions prévues au présent article.*** »

Dit autrement et dans l'attente des précisions réglementaires annoncées, on retiendra donc que la loi ne vise plus, comme précédemment, le dépôt de données de santé auprès d'hébergeurs agréés par la personne concernée, mais oblige toute personne qui héberge de telles données recueillies à l'occasion d'activité de prévention, notamment, dès lors qu'elles le sont pour le compte des personnes physiques à l'origine de la production ou du recueil desdites données.

Le fait qu'un professionnel de santé collige des données de santé au sein d'un Service de santé au travail implique, selon nous, que le Service réponde à l'obligation de certification nouvellement révisée.

En complément de l'article publié dans les *Informations Mensuelles* numéro 58 - Mars 2017 (pages 15-16), explicitant le changement du régime applicable – lequel passe de l'agrément de l'hébergeur concerné à sa certification, on indiquera ici que le certificat de conformité envisagé par les textes doit s'appuyer sur un référentiel.

En attendant sa publication par voie d'arrêté, on indiquera que l'ASIP vient de publier un « référentiel de certification des hébergeurs de données de santé » sur son site.

S'il convient d'attendre sa traduction réglementaire au Journal Officiel, on relèvera que le document de l'Agence est déjà utile pour préparer les pratiques. ■

Le document est à retrouver sur **http://esante.gouv.fr/actus/services/hebergement-des-donnees-de-sante-nouveaux-referentiels**

HAUTE AUTORITÉ DE SANTÉ

Nouvelle présidence

Publié au Journal Officiel le 5 décembre dernier, le décret du 4 décembre 2017 portant nomination de la présidente de la Haute Autorité de Santé a nommé le professeur Dominique Le Guludec à cette fonction.

Elle vient ainsi remplacer Mme Agnès Buzyn, nommée ministre des Solidarités et de la Santé en mai 2017, et ce pour la durée du mandat restant à couvrir, soit jusqu'en mars 2023.

Spécialisée en biophyisique et en médecine nucléaire, le professeur Le Guludec est une ancienne interne des hôpitaux de Paris et occupait jusqu'à cette nomination la présidence du conseil d'administration de l'Institut de radioprotection et de sûreté nucléaire.

AGENDA

10 janvier 2018
Conseil d'administration
10 rue la Rosière - Paris 15e

11 janvier 2018
Journée d'étude
Grand Hôtel - Paris 9e

8 février 2018
Ateliers Présanse
Paris