Protection des données personnelles : de nouvelles obligations issues du droit européen

5 octobre 2017. Veille juridique (/publications-federation/publications-pub-federation/veille-juridique-menu)

Pour faire face aux enjeux du numérique, l'Union européenne s'est doté d'une nouvelle réglementation par l'adoption d'un Règlement européen sur la protection des données personnelles (RGPD).

Ce texte a pour objectif de renforcer les droits et le contrôle des citoyens européens sur l'utilisation de leurs données personnelles, et d'unifier la réglementation pour les entreprises et organismes. De nombreuses formalités auprès de la CNIL vont disparaître. En contrepartie, la responsabilité des organismes sera renforcée. Le responsable du traitement ou les éventuels sous-traitant devront assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Le règlement européen s'imposera aux États membres dès le 28 mai 2016, sans qu'il soit besoin de le transposer dans les législations nationales. Les traitements de données existant devront d'ici cette date être mis en conformité avec les dispositions du règlement.

Toutes les structures et tous les organismes de solidarité sont ainsi concernés par cette mise en conformité aux nouvelles obligations européennes dès lors qu'ils mettent en place un traitement des données des personnes qu'ils accueillent.

Ce qui change avec le nouveau règlement européen :
Alors que les obligations des organismes au regard de la loi informatique et libertés reposent en grande partie sur les formalités préalables (déclaration, autorisation), le règlement européen sur la protection des données repose sur une logique de responsabilisation et de transparence.
Cette notion de responsabilité (accountability) se traduit notamment par la prise en compte de la protection des données dès la conception d'un service ou d'un produit et par défaut ; et par la mise en place d'une organisation, de mesures et d'outils internes garantissant une protection optimale des personnes dont les données sont traitées.

En pratique, les organismes devront :
- réaliser l'inventaire des traitements de données personnelles mis en œuvre ;
- évaluer leurs pratiques et mettre en place des procédures (notification des violations de données, gestion des réclamations et des plaintes, etc.) ;
- identifier les risques associés aux opérations de traitement et prendre les mesures nécessaires à leur prévention ;
- maintenir une documentation assurant la traçabilité des mesures.

La conformité au règlement européen impose la mise en place de différents outils :
- Un registre détaillé des traitements devra obligatoirement être conservé par le responsable du traitement et par ses éventuels sous-traitants et être mis à disposition des autorités de contrôle.
- Avant la mise en place d'un traitement de données pouvant présenter des risques pour la protection des données personnelles, l'organisme devra réaliser une analyse d'impact sur la vie privée (PIA);
- L'organisme responsable du traitement et, le cas échéant les sous-traitants, auront l'obligation d'informer les autorités en cas « d'accès non autorisé » à des données personnelles (piratage).

Il est recommandé, pour mettre en oeuvre ces outils, de désigner au sein de l'organisme un **« délégué à la protection des données »**. Ce délégué sera chargé d'informer et de conseiller le responsable de traitement ou le sous-traitant ainsi que leurs employés, de contrôler le respect du règlement et du droit national en matière de protection des données ainsi que de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci. La désignation de ce délégué sera obligatoire pour les organismes publics et ceux dont l'activité de base les conduit à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

Pour aider les organismes à s'organiser et à anticiper les changements liés à l'entrée en application du règlement européen le 25 mai 2018, **la CNIL propose une rubrique dédiée, une méthode et des outils pour se préparer au règlement en 6 étapes (ces outils seront adaptés et enrichis au gré de la publication des lignes directrices du G29 et des réponses aux questions les plus fréquemment posées par la CNIL).**

- **Lien vers le site de la CNIL :** méthodologie en 6 étapes (https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes)

Imprimer