



Règlement général sur la protection des données (RGPD)

Les élus locaux et la protection des données personnelles

Le nouveau règlement européen portant sur la protection des données personnelles (dit RGPD)

Pour faire face à l'évolution des menaces pesant sur les données dans un monde de plus en plus connecté, l'Union Européenne s'est dotée en avril dernier d'un règlement général consacré à la protection des données personnelles (RGPD). L'objectif est de garantir le droit de chacun à la protection de ses données personnelles et de consolider le droit des personnes physiques dans une société devenue numérique. Ce texte s'impose directement aux Etats membres de l'Union Européenne à partir du 25 mai 2018. Il confère davantage de protection pour les citoyens tout en imposant plus de responsabilités à ceux qui collectent, stockent, échangent ou transfèrent des données personnelles. Au-delà de sa finalité, ce nouveau règlement repose sur une logique de responsabilisation des acteurs traitant les données. C'est pourquoi il impose de nouvelles contraintes aux collectivités et ce quelle que soit leur taille. Celles-ci doivent se mettre en conformité pour éviter de futures sanctions

Les élus sont responsables du traitement des données à caractère personnel utilisées dans leur collectivité

Selon le RGPD, est une donnée à caractère personnel toute donnée permettant d'identifier directement ou indirectement un citoyen européen. Ainsi, une fiche de paie, une facture, un dossier médical, un numéro de téléphone, un numéro de plaque d'immatriculation des véhicules en stationnement mais aussi une photo sont des données personnelles. Or, les collectivités collectent et traitent chaque jour de nombreuses données personnelles permettant d'identifier une personne :

- Gestion des ressources humaines
- Etat civil, élections
- Recensement
- Urbanisme
- Gestion de services au public comme la restauration et les activités extra/périscolaires
- Personnes âgées (plan canicule par exemple)
- Action sociale

Parallèlement, l'environnement numérique est confronté à de multiples risques tels que les cyberattaques

Elles sont donc tout particulièrement concernées par les nouvelles obligations découlant de cette réforme.

C'est dans ce contexte que différents textes ont été pris d'une part au niveau national, avec la loi pour la République numérique d'octobre 2016, et d'autre part avec un règlement européen sur la protection des données, d'application directe depuis le **25 mai 2018**.

Avec le nouveau RGPD, on passe d'une logique de contrôle a priori basé sur des formalités administratives auprès de la CNIL (Commission Informatique et libertés), à une logique de responsabilisation des acteurs privés et publics.

Désormais, cette logique veut que le collecteur/gestionnaire de la donnée en soit responsable. Ainsi, il doit pouvoir justifier auprès de la CNIL qu'il a bien pris toutes les mesures nécessaires pour que les données qu'il collecte et traite soient correctement protégées.

Mais qui est le responsable du traitement? La définition est inscrite à l'article 3 de la loi «informatiques et libertés» du 6 janvier 1978 modifiée qui définit le responsable du traitement comme étant «sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.» Au niveau local, c'est donc l'exécutif, le Maire ou le Président qui est le responsable du traitement, pénalement responsable en cas de non-conformité au règlement.

Il ne peut déléguer sa fonction de responsable de traitement à son directeur général des services ni à son directeur informatique. La désignation d'un délégué à la protection des données ne l'exonère pas non plus de sa responsabilité.

Il ressort de ce texte l'obligation pour chaque collectivité de mettre en place un Délégué à la Protection des Données – DPD – (Data Protection Officer en anglais, DPO) à compter de l'entrée en vigueur des dispositions de ce règlement.

Ce délégué a différentes missions :

- Informer et conseiller le responsable de traitement des données ainsi que les employés concernés
- Contrôler le respect du règlement européen et du droit national en matière de protection des données
- Conseiller la collectivité sur la réalisation d'études d'impact sur la protection des données et en vérifier l'exécution
- Coopérer avec l'autorité de contrôle (CNIL) et être le point de contact de celle-ci

Concrètement, ce délégué devra être désigné sur la base de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, être associé en temps utile et de manière appropriée à l'ensemble des questions informatique et libertés de la collectivité, bénéficier des ressources et formations nécessaires pour mener à bien ses missions.

La réalisation de l'étude d'impact sur la protection des données nécessite en effet des connaissances poussées de l'environnement juridique et technique des systèmes d'information.

Cette mise en conformité obligatoire aura un coût non négligeable et non compensé pour les collectivités territoriales. Dans ce contexte, la mutualisation de la fonction de Délégué à la Protection des Données apparaît comme une solution permettant aux collectivités, de mettre en place les outils nécessaires à un bon pilotage de la conformité, avec du personnel compétent et indépendant, tout en limitant le coût. La CNIL prône de manière très claire la mutualisation du Délégué à la Protection aux Données par des structures de mutualisation informatique (SMI), les EPCI...

Consulter la documentation de la CNIL :

- Règlement européen du 27 avril 2016 :

www.cnil.fr/fr/reglement-europeen-protection-donnees

- Règlement européen : se préparer en 6 étapes

www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes

www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf

- En quoi les collectivités territoriales sont-elles impactées par le règlement européen sur la protection des données ?

www.cnil.fr/fr/RGPD-quel-impact-pour-les-collectivites-territoriales

- Devenir délégué à la protection des données :

www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees

- Documenter la conformité :

www.cnil.fr/fr/documenter-la-conformite