# Les élus locaux et la protection des données personnelles, plus que 6 mois pour agir.


## Le nouveau réglement 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**, que ce soit pour assurer la gestion administrative de leur structure (fichiers de ressources humaines), la sécurisation de leurs locaux (contrôle d'accès par badge, vidéosurveillance) ou la gestion des différents services publics et activités dont elles ont la charge (gestion de l'état civil, de la liste électorale, liste des élèves déjeunant à la cantine municipale ou fréquentant le centre de loisirs, développement de téléservices, etc.).

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

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.

## Que risquent les élus en cas de non conformité ?

Afin de crédibiliser les dispositions du nouveau règlement, l'Union européenne a mis en place diverses sanctions :

**Le risque pénal :** les dispositions des L.2123-34, L.3123-28, L.4135-28 du Code général des collectivités territoriales reprenant elles-mêmes celles de l'article 121-3 du Code pénal rappellent que les élus, s'ils violent manifestement une obligation de prudence, ou commettent une faute caractérisée contribuant à la réalisation d'un dommage, ou dont l'absence n'a pas permis d'éviter ledit dommage, peuvent être sanctionnés pénalement.

De plus, l'article 226-16 du Code pénal sanctionne les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques. Ainsi, le non-respect des obligations d'information **peut être sanctionné** par une amende de 1 500 €, et le non-respect des obligations relatives au traitement des données par une amende de 300 000 € et 5 ans d'emprisonnement.

**Des sanctions administratives :** les fuites ou pertes de données personnelles, y compris en cas de négligence, seront sanctionnés par des amendes pouvant atteindre jusqu'à 20 millions d'euros.

**La perte de confiance des administrés en leurs élus :** il faut aussi compter les dégâts importants d'une perte de confiance ayant des répercussions très importantes sur l'image de l'administration et de ses élus.

Les sanctions peuvent être lourdes. C'est pourquoi, aujourd'hui 2/3 des régions, 50 % des départements, 2/3 des métropoles, 1/3 des communautés urbaines, 1/10 des communautés d'agglomération ont engagé les démarches nécessaires pour respecter ces obligations dans le cadre de la protection des données (selon les données de la CNIL). Or, à ce jour, seulement 2 % des communes s'y sont astreintes.

## Les élus locaux doivent porter la mise en conformité

### Les mesures à anticiper et les actions à mener

Compte tenu de l'échéance et des enjeux, les élus locaux doivent impérativement lancer *dès à présent*, des actions de mise en conformité à la règlementation telles que :

- **Désigner un Délégué à la protection des données. Cette désignation est désormais obligatoire pour toutes les collectivités.**

Il aura pour principales missions : d'informer et de conseiller le responsable de traitement de la collectivité ou le sous-traitant, ainsi que les agents, de diffuser une culture Informatique et Libertés au sein de la collectivité, de contrôler le respect du règlement et du droit national en matière de protection des données, de conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution, de coopérer avec la CNIL et d'être le point de contact de celle-ci.

Dans l'exercice de ces missions, le délégué devra être à l'abri des conflits d'intérêts, rendre compte directement au niveau le plus élevé de la hiérarchie et bénéficier d'une liberté certaine dans les actions qu'il décidera d'entreprendre.

- Etablir et mettre à jour une cartographie complète des traitements effectués par la collectivité (audits juridique et technique) ;
- Créer et/ou mettre à jour de la documentation et des procédures internes, à communiquer à la CNIL en cas de contrôle, sous forme de registre, charte ou note d'information (ex : en cas de violation des données et de notification d'incident aux autorités ou pour la gestion des réclamations) ;
- Mettre à jour les clauses des marchés publics, afin d'obtenir des partenaires et sous-traitants des garanties sérieuses, mais aussi de limiter sa responsabilité ;
- Fournir une information loyale et effective aux administrés, utilisant les portails internet ou téléservices, quant à la gestion de leurs données (ex : adaptation des mentions légales) ;
- Garantir aux administrés l'effectivité de leurs droits d'accès, de rectification, d'opposition, de limitation, à l'effacement ou encore à la portabilité de leurs données ;
- Sensibiliser et former régulièrement les agents de la fonction publique territoriale aux enjeux de la protection des données (ateliers de formation, fiches pratiques, etc).

### Le délégué à la protection des données : une fonction à mutualiser

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 mais également les Centres de gestion.

La mise en conformité est loin d'être insurmontable. Toutefois, il est indispensable d'avoir à l'esprit les risques encourus en cas de non-conformité et d'anticiper les étapes à suivre ainsi que les outils à mettre en place. En ce sens, la CNIL propose déjà de nombreuses informations dans la rubrique «collectivités» du site, dont une méthodologie en 6 étapes pour se préparer et anticiper les changements liés à l'entrée en application du règlement européen le 25 mai 2018.

Une réunion d'information a été organisée le 5 décembre au Centre de gestion du Finistère en lien avec Megalis Bretagne, et en partenariat avec l'Association des maires du Finistère.
(Plus d'information sur le site du CDG29 : www.cdg29.bzh/)

Organisme de mutualisation, tiers de confiance et de proximité, le Centre de gestion pourra vous accompagner dans la mise en œuvre de cette nouvelle responsabilité.

Contact : Laurence KERVIEL (lkerviel@cdg29.bzh)

Laurence KERVIEL
Juriste CDG29

*Pour tout contact "info-Maires" : Isabelle Lannuzel - Téléphone : 02 98 33 88 70 - Télécopie : 02 98 33 88 71 - e-mail : amf29@wanadoo.fr*
*"info-Maires" est édité par l'Association des Maires du Finistère. Directeur de la publication : Dominique CAP. ISSN 1765-414*
*Maquette : Atelier Pélican - Gouesnou. Impression : Imprimerie du Commerce - Quimper.*
*Remerciements à l'Office public de la langue bretonne pour les traductions.*