# Réglementation générale de protection des données (RGPD). Obligations des collectivités territoriales au 25 mai 2018

## Revue - Vie Communale

### Source - Courrier des lecteurs

**1.**

 Le RGPD encadre le traitement des données personnelles. Une donnée personnelle est une information directe ou indirecte se rapportant à une personne physique identifiée ou identifiable : nom, âge, date de naissance, adresse, sexe, photographie, empreintes, etc., mais également immatriculation, données GPS, adresse IP... Par extension, sont soumis au RGPD les traitements, automatisés ou non, de données à caractère personnel, c’est-à-dire toutes les actions portant sur ces données personnelles (collecte, enregistrement, consultation, utilisation, diffusion). Le RGPD renforce ou crée certains droits : - le consentement : les utilisateurs doivent être informés de l’usage de leurs données et doivent en principe donner leur accord pour le traitement de celles-ci ou pouvoir s’y opposer ;

- la portabilité : ce droit nouveau permet à une personne de récupérer ses données ;

- le droit à l’oubli : chaque individu a le droit de demander l’effacement des données. Dans le cadre du RGPD, les collectivités doivent respecter les obligations suivantes : - les données ne peuvent être recueillies que pour une finalité déterminée, explicite et légitime. Ce principe limite la manière dont le responsable du traitement pourra utiliser ou réutiliser ces données dans le futur ;

- seules les données strictement nécessaires à la réalisation de l’objectif peuvent être collectées ;

- une fois que l’objectif poursuivi par la collecte des données est atteint, il n’y a plus lieu de conserver les données et elles doivent être supprimées ;

- la sécurité des données collectées et leur confidentialité doivent être garanties ;

- les personnes doivent être informées de leurs droits (droit d’accéder à ses données, de les rectifier, de s’opposer à leur utilisation) ;

- les formalités préalables auprès de la CNIL sont toujours en vigueur. Les collectivités seront ainsi appelées à : - tenir un registre de leurs activités de traitement (ex. : fichiers d’aide sociale) ;

- encadrer les opérations sous-traitées dans les contrats de prestation de services ;

- formaliser des politiques de confidentialité des données, des procédures relatives à la gestion des demandes d’exercice des droits ;

- adhérer à des codes de conduite ou encore certifier des traitements.

**2.**

 Depuis le 25 mai 2018, la désignation d’un délégué à la protection des données, successeur du correspondant informatique et libertés (CIL), est obligatoire pour les organismes et autorités publics, et donc pour les collectivités. Mais il est possible de mutualiser un délégué à la protection des données à l’échelle de l’EPCI par exemple.

**3.**

 Le délégué 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 contrôler le respect du règlement et du droit en matière de protection des données ;

- de coopérer avec la CNIL. 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.

* [*En savoir plus*](https://www.cnil.fr/fr/RGPD-quel-impact-pour-les-collectivites-territoriales)