Sécurité Numérique
L'impact du règlement européen sur la protection des données pour les collectivités territoriales

Depuis plusieurs années, l'Union européenne travaille à créer un espace numérique plus sûr et sécurisé. Le Règlement européen n° 2016/679, dit règlement général sur la protection des données (RGPD, ou GDPR, pour General Data Protection Regulation), voté en juillet 2016 par le Parlement européen, et qui sera opposable à compter du 25 mai 2018, fait partie de cette stratégie.

Avec le RGPD, les collectivités devront adopter des mesures à la fois techniques et organisationnelles, leur permettant de s'assurer et de démontrer qu'elles offrent un niveau optimal de protection aux données personnelles traitées. Les organismes publics et privés auxquels les collectivités sous-traitent la mise en œuvre de tout ou partie de leurs traitements (comme les prestataires de service hébergeant des données) devront obligatoirement participer à cette démarche de mise en conformité, sous peine de sanctions. Le principe de protection des données par défaut (*Privacy by default*) devra être pris en compte dès la phase de conception (*Privacy by design*) du produit, du service ou du traitement (art.25). Par exemple il sera nécessaire d'anonymiser les données toutes les fois où leur exploitation sous une forme identifiante n'apparaît pas nécessaire à la satisfaction du besoin, ou encore purger les données à l'issue de la durée de conservation nécessaire à la réalisation de la finalité.

- La gouvernance des données

Avec le RGPD, nous rentrons dans l'ère de la gouvernance des données personnelles. Une bonne gouvernance nécessite une documentation continue des actions menées pour être en capacité de piloter et de démontrer la conformité. Les collectivités devront ainsi tenir un registre de leurs activités de traitement, 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... Dans certains cas, pour les traitements à risques, elles devront effectuer des analyses d'impact sur la vie privée et notifier à la CNIL, voire aux personnes concernées, les violations de données personnelles. De plus, le RGPD impose une « responsabilité conjointe » entre le responsable du traitement des données et les sous-traitants qui seront dorénavant solidaires dans leur responsabilité civile et administrative. La conséquence est ainsi une double responsabilité, la personne concernée pouvant exercer ses droits « à l'égard de et contre chacun des responsables du traitement » (art.26).

- La désignation d'un délégué à la protection des données (DPO)

A compter du 25 mai 2018, la désignation d'un délégué à la protection des données (Data protection Officer, ou DPO), successeur du correspondant informatique et libertés (CIL) dont la désignation est aujourd'hui facultative, sera obligatoire pour les organismes et autorités publics, et donc pour les collectivités. Le DPO 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 national en matière de protection des données, via la réalisation d'audits ; ou encore de conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution. Il devra 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.
De plus, la collectivité territoriale devra s'assurer qu'il dispose d'un niveau d'expertise et de moyens suffisants pour exercer son rôle de façon efficace. Le DPO devra ainsi être associé à l'ensemble des questions informatiques et bénéficier des ressources et formations nécessaires pour mener à bien ses missions. Dans ce contexte, la mutualisation de la fonction de DPO apparaît un enjeu essentiel pour les collectivités territoriales, notamment pour celles de petite taille.

- **Mutualisation de la démarche**

Aujourd'hui, si certaines collectivités ont déjà engagé cette démarche (2/3 des régions et métropoles, 1/10 des communautés d'agglomération...), seulement 2% des communes ont désigné un correspondant. Pour ces collectivités, qui ont des préoccupations identiques, la mutualisation de la fonction semble tout à fait adaptée. Elle permet de limiter les coûts et de bénéficier de professionnels disposant des compétences nécessaires à un bon pilotage de la conformité.
Les EPCI et les syndicats mixtes (Pays - Pôle territorial) peuvent également proposer aux collectivités qui en sont membres les services d'un DPO mutualisé.

Bénédicte Pilliet, Directeur fondateur de CyberCercle