LE NOUVEAU RÈGLEMENT SUR LA PROTECTION DES DONNÉES

Par Alexandra Aderno, avocate au Cabinet Seban & Associés

Quand et à qui s'applique le nouveau règlement sur la protection des données ?

Le règlement 2016/679 du Parlement européen et du conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, adopté le 14 avril 2016, sera applicable à partir du vendredi 25 mai 2018. Dans la mesure où il s'agit d'un règlement, il n'est pas nécessaire de le transposer dans les États membres pour qu'il s'applique.

Par ailleurs, le règlement s'appliquera, d'un point de vue matériel, à tous traitements de données à caractère personnel complètement ou partiellement automatisés et à ceux non automatisés contenus dans un fichier, et, d'un point de vue territorial, à tout traitement effectué par un responsable de traitement ou un sous-traitant installé dans l'Union européenne ou, si ce n'est pas le cas, s'il met en œuvre des traitements visant à fournir des biens et des services à des résidents de l'Union européenne ou s'il suit des comportements qui ont lieu dans l'Union européenne.

Quelles sont les grandes orientations de ce texte susceptibles d'impacter les collectivités ?

Alors que la directive 95/46/CE sur la protection des données reposait en grande partie sur la notion de « formalités préalables » (régime déclaratif et d'autorisation), le nouveau règlement européen inverse cette logique de contrôle a priori et crée une logique de responsabilisation.

Désormais, les acteurs publics seront responsables, dès la conception, du traitement de leurs données. Cette responsabilisation s'accompagne de la nécessité de gagner en technique en repensant la gestion de données. La mise en conformité des collectivités territoriales sera conduite à travers une mutualisation des moyens et des effectifs pour échapper aux lourdes sanctions prévues.

Qu'est-ce qu'implique la protection des données dès la conception et par défaut ?

Les collectivités devront tenir compte, dès la phase de conception du produit, du service ou du traitement, des contraintes imposées par le règlement. Il s'agit de mettre en place des mesures techniques et organisationnelles appropriées telles que la pseudonymisation ou encore la minimisation de données. Ce type de mesures peut se traduire, par exemple, par des restrictions de droits d'accès informatiques aux données ou par un mécanisme automatique de purge des données à l'issue de la durée de conservation nécessaire à la réalisation de la finalité. De plus, la collectivité doit garantir que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

Comment les collectivités peuvent garantir la conformité de leurs systèmes ?

Afin d'assurer la bonne gouvernance des données traitées et de démontrer la conformité du système, les collectivités devront tenir un registre des activités de traitement comprenant notamment les finalités du traitement, les catégories des personnes concernées et les catégories des destinataires auxquels les données sont communiquées. De plus, si elles font appel à un sous-traitant pour effectuer le traitement de données, elles devront passer des contrats de prestations de services au sein desquels le process d'autorisation, de certification des données et d'instruction sera précisément décrit. Elles pourront également formaliser des politiques de confidentialité des données et mettre en place des procédures relatives à la gestion des demandes d'exercice des droits des personnes concernées tels que le droit de rectification ou le droit d'opposition.

Les collectivités devront-elles désigner un délégué à la protection des données ?

Les collectivités seront obligées de désigner un délégué à la protection des données, successeur du correspondant informatique et libertés (CIL) dont la désignation est aujourd'hui facultative, à compter du 25 mai 2018. À cet égard, la Commission nationale informatique et libertés (CNIL) a alerté les communes, dont seulement 2 % ont engagé un CIL, sur la nécessité de préparer la désignation du délégué.

Quelles sont les missions d'un délégué à la protection des données ?

Ce délégué assure différentes missions dont : l'information et le conseil au responsable de traitement de la collectivité ; la diffusion d'une culture informatique et libertés au sein de la collectivité ; le contrôle du respect du règlement et du droit national en matière de protection des données, via la réalisation d'audits en particulier ; le conseil à la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données ; la coopération avec la CNIL.

Dans l'exercice de ses missions, le délégué doit se prémunir contre les conflits d'intérêts. Il rend compte de ses activités directement au niveau le plus élevé de la hiérarchie. Il bénéficie d'une liberté certaine dans les actions qu'il entreprend. En outre, la collectivité doit s'assurer qu'il dispose d'un niveau d'expertise et de moyens suffisants pour exercer son rôle de façon efficace. Le délégué doit donc être désigné sur la base de ses connaissances spécialisées du droit et des pratiques en matière de protection des données et est associé en temps utile et de manière appropriée à l'ensemble des questions relatives au traitement de données. Enfin, ce délégué doit bénéficier des ressources et formations nécessaires pour mener à bien ses missions.

Comment appréhender la désignation du délégué à la protection des données ?

Les responsables de traitement peuvent opter pour un délégué à la protection des données mutualisé ou externe. Comme le taux de désignation de CIL est très faible dans les communes, contrairement aux régions, aux départements et aux intercommunalités, la mutualisation des délégués peut apparaître comme un schéma attractif pour elle. Cette solution, encouragée par la CNIL, permet de limiter les coûts et de bénéficier de professionnels disposant des compétences et de la disponibilité nécessaires à un bon pilotage de la conformité.

Comment mutualiser le délégué à la protection des données ?

Les structures de mutualisation informatique, spécialisées dans le développement de l'e-administration sur leur territoire, constituent une bonne solution de mutualisation de la fonction de délégué pour les collectivités. Certaines de ces structures, telles que l'Agence landaise pour l'informatique (ALPI), proposent déjà un service de CIL mutualisé aux communes de leur ressort territorial. D'autres, telles que l'ADICO dans l'Oise (Association pour le développement et l'innovation numérique des collectivités), travaillent sur une offre de délégué mutualisé.

Parmi les missions qui seront confiées aux délégués à la protection des données mutualisés, la réalisation d'audits de gestion et de gouvernance des données auprès des communes constituera une part prépondérante de leurs activités.

Quelles sont les sanctions encourues ?

En cas de non-conformité, le règlement européen a renforcé le panel des sanctions encourues. Les responsables de traitement pourront faire l'objet de sanctions administratives importantes en cas de méconnaissance du règlement. Peuvent notamment être prononcées : une mise en demeure ; un avertissement ; une limitation temporaire ou définitive d'un traitement ; une suspension des flux de données ; un ordre de satisfaire aux droits des personnes ; un ordre de rectifier, limiter ou effacer les données.

Parmi les nouveaux outils créés, la certification délivrée aux collectivités peut être retirée. Enfin, les amendes en cas de mauvaise gestion et de fuite des données personnelles peuvent désormais atteindre 20 millions d'euros. Dans ces conditions, il est d'autant plus important que les collectivités assurent la mise en conformité de leurs systèmes, notamment de vidéoprotection. ●

Une application dès le 25 mai 2018

Le nouveau règlement général sur la protection des données sera applicable dès le 25 mai 2018. À cette date, la logique de démarches préalables, comprenant un régime déclaratif et un régime d'autorisation, sera abolie et laissera place à une logique de responsabilisation. Il appartiendra donc aux collectivités de mettre en conformité leurs systèmes de traitement des données, de désigner obligatoirement un délégué et de tenir un registre afin d'éviter les lourdes sanctions qui pourront peser sur elles.