Le RGPD :

Quelles conséquences pour les collectivités ?

Le Règlement Général sur la Protection des Données personnelles (RGPD) a été adopté par le Parlement européen le 14 avril 2016. Il est applicable en France depuis le 25 mai 2018. Cette nouvelle législation complète la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ainsi que la loi du 7 aout 2016 pour une République Numérique.

Toute entité traitant des données de citoyens européens est concernée par le RGPD.

La nouvelle réglementation concerne toutes les collectivités locales quelle que soit leur taille, au même titre que les acteurs économiques et les associations.

Les collectivités deviennent responsables des données qu'elles détiennent.

Le RGPD transforme l'obligation de moyens de la législation actuelle en une obligation de résultats et renforce considérablement les sanctions encourues. En outre, il repose sur une logique de conformité, dont les acteurs sont responsables, avec un contrôle a posteriori du régulateur, la CNIL (Commission Nationale de l'Informatique et des Libertés).

La logique devient la protection des données dès la conception et par défaut.

De nombreuses formalités auprès de la CNIL disparaissent. En contrepartie, la responsabilité des organismes sera renforcée. Ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

La réforme de la protection des données poursuit trois objectifs :

- Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures
- Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants)
- Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.

Qu'est-ce qu'une donnée à caractère personnel ?

La notion de données personnelles est appréciée au sens large et intègre les données nominatives (noms, prénoms, adresse…) comme celles qui permettent une identification indirecte, comme la géolocalisation.

Enjeu du RGPD pour les collectivités

Les collectivités territoriales traitent chaque jour de nombreuses données personnelles. Certains de ces traitements présentent une sensibilité particulière.

Les collectivités recourent de plus en plus aux technologies et usages numériques. Le numérique leur permet de se moderniser et d'être plus efficace. Cependant, le nombre de cyberattaques augmente lui aussi.

Ainsi, les citoyens demandent aux collectivités d'être davantage vigilant dans l'utilisation de leurs données. Selon la CNIL, les nouveaux services numériques doivent répondre aux exigences de protection des données, dont la sécurité est une des composantes essentielles, pour qu'ils créent de la confiance auprès des administrés. Par conséquent, les collectivités doivent adopter une logique de responsabilisation.

Se préparer au RGPD en 6 étapes

La CNIL propose une méthodologie en 6 étapes afin de se préparer au RGPD

- *Désigner un pilote*

La désignation d'un délégué à la protection des données est obligatoire pour les communes à partir du 25 mai 2018.

Le délégué à la protection des données pilote la mise en conformité de la collectivité à la nouvelle réglementation. Puis, il contrôle l'application de celle-ci dans le temps. Son rôle est donc d'informer et de conseiller dans le temps le responsable du traitement des données, c'est-à-dire le maire. En outre, il forme l'ensemble des agents de sa collectivité.

Le délégué à la protection des données doit être nommé pour ses qualités professionnelles et techniques. Il doit attester de la mise à jour de ses compétences tout au long de sa mission et doit également être à l'abri des conflits d'intérêts.

À noter que ce poste de délégué à la protection des données peut être mutualisé ou externalisé.

- *Cartographier les traitements de données personnelles*

Afin de mesurer l'impact du règlement sur la protection des données de la collectivité, il faut, au préalable, recenser de façon précise les traitements de données personnelles mis en œuvre par la collectivité. Pour cela, il faut tenir un registre de traitements dans le but de faire le point.

Cet inventaire permet de dénicher les traitements à risques, réalisés sans base légale. Il convient de récupérer toutes les données. La cartographie concerne autant les données personnelles détenues en internes que celles en possession des différents prestataires de la collectivité.

- *Prioriser les actions à mener*

Sur la base du registre des traitements, il faut identifier les actions à mener pour se conformer aux obligations actuelles et à venir. Il convient de prioriser ces actions au regard des risques que font peser les traitements sur les droits et les libertés des personnes concernées.

- *Gérer les risques*

S'il est identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, il convient de mener pour chacun de ces traitements, une analyse d'impact sur la protection des données (Data Protection Impact Assessment).

L'analyse d'impact sur la protection des données (PIA) est une étude aidant à construire des traitements de données respectueux de la vie privée et permettant de démontrer la conformité de son traitement au RGPD. Un PIA est un outil d'évaluation d'impact sur la vie privée. Le PIA repose sur deux piliers :

- Les principes et droits fondamentaux, « non négociables », fixés par la loi. Ils ne peuvent faire l'objet d'aucune modulation, quelles que soient la nature, la gravité et la vraisemblance des risques encourus.
- La gestion des risques sur la vie privée des personnes concernés, qui permet de déterminer les mesures techniques et d'organisation appropriée pour protéger les données personnelles.

Un PIA contient :

- Une description du traitement étudié et de ses finalités
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités
- Une évaluation des risques pour les droits et libertés des personnes concernées les mesures envisagées pour faire face aux risques.

Mener un PIA est obligatoire pour tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées (Article 35 du RGPD).

Pour aider à déterminer si le traitement est susceptible d'engendrer des risques élevés, les 9 critères suivant sont définis dans des lignes directrices :

- Évaluation ou notation
- Décision automatisée avec effet juridique ou effet similaire significatif
- Surveillance systématique
- Données sensibles ou données à caractère hautement personnel
- Données personnelles traitées à grande échelle
- Croisement d'ensemble de données
- Données concernant des personnes vulnérables
- Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles
- Exclusion du bénéfice d'un droit, d'un service ou d'un contrat

Il est conseillé de faire un PIA si le traitement correspond au moins à 2 de ces critères

- *Organiser les processus internes*

Le RGPD oblige de rester en permanence en conformité avec la règlementation. Pour cela, il faut mettre en place des processus internes.

Organiser les processus internes implique de prendre en compte la protection des données personnelles dès la conception d'une application ou d'un traitement (minimisation de la collecte de données au regard de la finalité, cookies, durée de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données s'assurer du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données).

Cela implique aussi de sensibiliser et d'organiser la remontée d'information en construisant notamment un plan de formation et de communication pour les agents de la collectivité.

Organiser les processus internes signifie également traiter les réclamations et les demandes des personnes concernées quant à l'exercice de leur droits (droits d'accès, de rectification,

d'opposition, droit à la portabilité, retrait du consentement) en définissant les acteurs et les modalités (l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen).

Enfin, cela demande aussi d'anticiper les violations de données en prévoyant, dans certains cas, la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais.

La CNIL propose un téléservice de notification de violations de données personnelles.

- *Documenter la conformité*

Les collectivités doivent être capables de prouver que tout est mis en œuvre pour garantir la vie privée des usagers et des agents.

Afin de prouver la conformité au règlement, la collectivité doit constituer et regrouper la documentation nécessaire. Les actions et documents à réaliser à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Le dossier doit comporter **la documentation sur les traitements de données personnelles** (à l'instar du registre des traitements ; des analyses d'impact sur la protection des données (PIA) ; ou encore l'encadrement des transferts de données hors de l'Union européenne), mais aussi **l'information des personnes** (c'est-à-dire les mentions d'information ; les modèles de recueil du consentement des personnes concernées ; les procédures mises en place pour l'exercice des droits) et enfin **les contrats qui définissent les rôles et les responsabilités des acteurs** (en somme les contrats avec les sous-traitants ; les procédures internes en ces de violations de données : les preuves que les personnes concernées ont donnée leur consentement lorsque le traitement de leur données repose sur cette base).

Caractéristiques du délégué à la protection des données

Le délégué à la protection des données doit réunir 3 caractéristiques :

- *Détenir les compétences requises pour ce poste*

Ce poste suppose une expertise juridique et technique en matière de protection des données personnelles mais aussi une bonne connaissance du secteur d'activité, de l'organisation interne, en particulier des opérations de traitements, des systèmes d'information, des besoins en matière de protection et de sécurité des données. Ces compétences peuvent être acquises, par exemple, à l'occasion de formations adaptées à son profil.

- *Disposer de moyens suffisants*

Le délégué à la protection des données doit disposer du temps suffisant pour exercer ses missions et bénéficier de moyens matériels et humains adéquats. En outre, il doit pouvoir accéder aux informations utiles et être associé en amont des projets impliquant des données personnelles.

- *Avoir la capacité d'agir en toute indépendance*

Le délégué à la protection des données ne doit pas être en situation de conflit d'intérêt en cas de cumul de sa fonction de délégué avec une autre fonction. En outre, il doit pouvoir rendre compte au plus haut niveau de la direction de l'organisme. Enfin, il ne peut être sanctionné pour l'exercice de ses missions de délégué à la protection des données et ne peut recevoir d'instruction dans le cadre de l'exercice de ses missions.

La mutualisation et externalisation du poste de délégué à la protection des données

L'article 37 du règlement européen autorise la mutualisation et l'externalisation du poste de délégué à la protection des données.

La plupart des communes ont des problématiques 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 et de la disponibilité nécessaires à un bon pilotage de la conformité.

- *Les structures de mutualisation informatique (SMI)*

Les SMI, 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. Ces structures portent très souvent le développement numérique des territoires, que ce soit à travers le réseau des infrastructures ou des services proposés (comme les plateformes de téléservices), et proposent aux collectivités un accompagnement dans leur transition numérique.

Elles regroupent maîtrise d'ouvrage et maîtrise d'œuvre et c'est à leur niveau que les besoins des collectivités sont identifiés, que des progiciels sont développés, que les mesures de sécurité et paramétrages par défaut sont définis, et qu'éventuellement les données sont hébergées. Ayant vocation à se multiplier, elles couvrent déjà 50% des départements et permettent aux collectivités adhérentes de rationaliser les dépenses tout en optimisant les conditions juridiques, organisationnelles et fonctionnelles du déploiement d'outils numériques de gestion de leurs missions de service public.

- *Les centres de gestion*

Les collectivités peuvent bénéficier des Correspondant Informatique et Libertés (CIL) mutualisés au niveau de centres de gestion de la fonction publique territoriale.

- *Les Établissements Publics de Coopération Intercommunale (EPCI)*

Les communautés de communes, d'agglomération, les communautés urbaines et les métropoles, peuvent également proposer aux collectivités qui en sont membres les services d'un délégué mutualisé.

En outre, sans aller jusqu'à mutualiser la fonction de délégué, les collectivités ayant les mêmes préoccupations peuvent opportunément travailler ensemble pour se préparer au mieux aux nouvelles obligations posées par le règlement européen.

- *Prestataires privés*

Il s'agit en l'occurrence d'un contrat de service avec par exemple un cabinet d'avocats, d'experts ou encore de délégué à la protection des données externe indépendant.

Notification des violations de données personnelles

- *Notification à la CNIL*

L'article 33 du règlement dispose qu'en cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à la CNIL dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

- *Notification à la personne concernée par la violation des données*

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

Responsabilité

La responsabilité est l'apanage du responsable de traitement, autrement dit, dans le cadre des communes, le maire.

À noter que la responsabilité est partagée avec le sous-traitant s'il existe. Selon l'article 4 §8 du règlement, le sous-traitant est une personne physique ou morale, autorité publique, service ou autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement.

Sanctions

La CNIL peut infliger des sanctions jusqu'à 20 000 000 millions d'euros. Les sanctions peuvent aussi être des recours juridictionnels.

Le montant des amendes administratives est déterminé en fonction :

- De la nature, la gravité et la durée de la violation du RGPD
- De la nature, la portée ou la finalité du traitement concerné
- Du nombre de personnes concernées affectées et du nombre de dommage subi.