Mai 2018

NOTE ÉTABLIE À LA DEMANDE DE L'AMF69 POUR SES ADHÉRENTS PAR LE GROUPE PÉDAGOFICHE

Règlement général sur la protection des données (RGPD) : les 10 points clés

Le 25 mai dernier le règlement européen sur la protection des données (RGPD) est entré en vigueur. L'objectif est de s'adapter aux nouvelles réalités numériques tout en unifiant le cadre juridique au niveau européen.

La France dispose déjà d'un arsenal juridique, la loi « informatique et libertés » du 6 janvier 1978 elle l'a donc adaptée. La modification est de taille car il s'agit d'un renversement des responsabilités.

Les collectivités territoriales quelle que soit leur taille, sont concernées par la nouvelle loi, comme toutes les personnes morales (associations, entreprises...) traitant des données personnelles.

1. Une logique inversée

Le nouveau règlement renverse les règles de contrôle. On passe d'une logique de contrôle *a priori*, basée sur des formalités déclaratives auprès de la CNIL, à une logique de responsabilisation des acteurs traitant des données personnelles, basée sur un contrôle *a posteriori*.

Pour se mettre en conformité, les collectivités doivent, nous dit la CNIL, « adopter et actualiser des mesures techniques et organisationnelles leur permettant de s'assurer et de démontrer à tout instant qu'elles offrent un niveau optimal de protection aux données traitées ».

2. Qu'est-ce qu'une donnée personnelle ?

Il s'agit de toute information directe ou indirecte se rapportant à une personne physique identifiée ou identifiable : nom, âge, date de naissance, adresse, sexe, photographie, empreintes..., mais aussi 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...).

Pour les collectivités, les données personnelles qu'elles traitent figurent dans les fichiers des personnels FPT, les fichiers d'administrés ou d'usagers des services publics (état civil, cantine, CCAS...), les moyens de télésurveillance...

ASSOCIATION DES MAIRES DU RHONE ET DE LA METROPOLE DE LYON ET DES PRESIDENTS D'INTERCOMMUNALITE (AMF69)
9 allée Alban Vistel – 69110 SAINTE-FOY-LÈS-LYON – 04 78 15 03 30 – presidence@amf69.fr – www.amf69.fr

3. L'élu est le responsable du traitement

Lorsqu'un traitement de données à caractère personnel est mis en place au sein de la collectivité, c'est le maire ou le président l'EPCI et non le DPO (*voir point 6*) qui est responsable en cas de non- conformité. Il est donc important de veiller, en amont, à l'objectif du traitement et aux moyens employés pour l'atteindre et par la suite, à éviter les utilisations inappropriées.

4. Les droits individuels renforcés

Le RGPD renforce ou crée certains droits (articles 15 à 22 du RGPD). Le responsable du traitement est garant de leur bonne exécution.

- **Droit d'accès :** la personne peut accéder aux données à caractère personnel la concernant ainsi qu'aux informations relatives à la finalité du traitement, aux catégories des données personnelles, à leur durée de conservation et aux destinataires auxquels elles sont communiquées.
- **Droit de rectification** : droit d'obtenir la rectification des données à caractère personnel qui sont inexactes, y compris que les données incomplètes soient complétées, en fournissant une déclaration complémentaire.
- **Droit à l'effacement** («**droit à l'oubli**») de données à caractère personnel : notamment lorsque les données ne sont plus nécessaires ou, dans les cas où un consentement est nécessaire, lorsque la personne retire son consentement ou s'oppose au traitement.
- **Droit à la limitation du traitement** : lorsque la personne conteste l'exactitude des données, pendant la durée permettant de les vérifier ; lorsque les données ne sont plus nécessaires pour le traitement mais sont encore nécessaires à la personne pour constater, exercer ou défendre des droits en justice ; lorsque la personne s'est opposée au traitement, le temps de vérifier si les motifs du traitement prévalent sur ceux de la personne concernée...
- **Droit à la notification** de la rectification, de l'effacement des données à caractère personnel ou de la limitation du traitement. Il s'agit pour le responsable du traitement d'une **obligation de notification**, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés.
- **Droit à la portabilité** des données : droit de recevoir les données à caractère personnel fournies dans un format couramment utilisé et lisible par machine, et de les transmettre à un autre responsable du traitement.
- **Droit d'opposition** : droit de s'opposer à tout moment à un traitement des données à caractère personnel, pour des raisons tenant à sa situation particulière.
- **Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé** produisant des effets juridiques pour une personne ou l'affectant de manière significative. Cela signifie que la personne a le droit d'obtenir une intervention humaine, d'exprimer son point de vue et de contester la décision.

5. Le 25 mai 2018. Une date impérative ?

C'est la date d'entrée en vigueur du RGPD. Mais dans les faits, une certaine élasticité est d'ores et déjà annoncée par la CNIL. L'idée est plutôt de privilégier la mise en œuvre progressive en sélectionnant les priorités.

ASSOCIATION DES MAIRES DU RHONE ET DE LA METROPOLE DE LYON ET DES PRESIDENTS D'INTERCOMMUNALITE (AMF69)
9 allée Alban Vistel – 69110 SAINTE-FOY-LÈS-LYON – 04 78 15 03 30 – presidence@amf69.fr – www.amf69.fr

6. Du CIL au DPO

Depuis le 25 mai, la désignation d'un délégué à la protection des données -DPD (ou son sigle anglais DPO - Data Protection Officer) est obligatoire pour les collectivités. Il remplace le correspondant informatique et libertés -CIL- dont la désignation était facultative. Son rôle est de veiller au respect des nouvelles règles de traitement des données : pour cela il informe et conseille le responsable du traitement et les agents sur les obligations et les outils disponibles. Le DPO est aussi l'intermédiaire entre la collectivité, les particuliers et la CNIL.

Il doit pouvoir agir de manière indépendante du responsable du traitement. Ce dernier lui fournit les ressources nécessaires (temps, formation, finances, personnel) et l'accès aux données.

7. Possibilité de partager un DPO

Le poste de DPO peut être mutualisé à l'échelon supra communal. C'est déjà le cas du CIL dans certains centres de gestion mais il est aussi possible d'envisager un DPO pour l'EPCI dont la commune est membre ou encore de recourir à une structure de mutualisation informatique. C'est une manière à la fois de garantir l'indépendance du DPO par rapport à une désignation en interne et de s'assurer que toutes les collectivités, quelle que soit leur taille, en seront dotées. Le RGPD pose néanmoins comme condition que le DPO soit « facilement joignable » : il incombe donc au responsable du traitement de bien veiller à ce que les coordonnées du DPO soient disponibles et à jour afin que les personnes intéressées puissent aisément et directement prendre contact avec lui.

8. Protection des données « dès la conception du traitement et par défaut »

La collectivité est désormais responsable de la protection des données traitées. Elle doit appliquer un principe nouveau de **protection des données dès la conception** (*Privacy by design*) **du traitement et par défaut** (*Privacy by default*). Cela signifie qu'elle doit tenir compte des règles de protection des données dès la phase de conception du produit, du service ou du traitement, et dès qu'elle définit des outils et des paramétrages par défaut.
Par exemple :

- favoriser les menus déroulants ou les cases à cocher plutôt que les zones de commentaires libres, pour limiter dès le départ le nombre et la nature des données enregistrées ;
- restreindre au maximum les droits d'accès informatiques aux données et les opérations susceptibles d'être réalisées ;
- pseudonymiser les données chaque fois qu'une identification n'est pas nécessaire ;
- faire une purge automatique des données à la fin de la durée de conservation nécessaire.

À noter que les prestataires informatiques et autres sous-traitants sont soumis aux mêmes nouvelles obligations :

- *protection des données dès la conception et par défaut ;*
- *sécurité des données traitées ;*
- *obligation d'assistance, d'alerte et de conseil des collectivités territoriales.*

ASSOCIATION DES MAIRES DU RHONE ET DE LA METROPOLE DE LYON ET DES PRESIDENTS D'INTERCOMMUNALITE (AMF69)
9 allée Alban Vistel – 69110 SAINTE-FOY-LÈS-LYON – 04 78 15 03 30 – presidence@amf69.fr – www.amf69.fr

9. La méthodologie

La protection des données « dès la conception et par défaut » exige :

1. de **nommer un DPD** ;
2. de **recenser les traitements** existants ;
3. d'**identifier les actions à mener en priorité** en fonction des risques de non-conformité engendrés par l'application des nouvelles règles ;
4. de **gérer les risques** inhérents à certaines données sensibles, et le cas échéant de procéder à une analyse d'impact sur la protection des données (*voir point 10*).
5. d'**organiser la protection des données** par la mise en place de procédures internes qui garantissent cette protection à tout moment, par la prise en compte des événements extérieurs (faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire...)
6. de **documenter la conformité**, c'est-à-dire regrouper la documentation nécessaire pour prouver la conformité au RGPD.

10. Analyse d'impact sur la protection des données (PIA)

Certaines données à risques élevés pour la vie privée des personnes doivent faire l'objet d'une analyse d'impact sur la protection des données (en anglais, DPIA pour Data protection impact *assessment* ou PIA pour *Privacy Impact Assessment*). Le PIA est mis en œuvre si le traitement répond à **au moins 2 des 9 critères** suivants :

- 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'ensembles 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 contrat.

C'est le cas de la télésurveillance, de données génétiques ou biométriques ou relatives à des condamnations...

Note réalisée par Béatrice Merlo, Groupe Pédagofiche.

ASSOCIATION DES MAIRES DU RHONE ET DE LA METROPOLE DE LYON ET DES PRESIDENTS D'INTERCOMMUNALITE (AMF69)
9 allée Alban Vistel – 69110 SAINTE-FOY-LÈS-LYON – 04 78 15 03 30 – presidence@amf69.fr – www.amf69.fr