Le RGPD
dans les collectivités territoriales

Septembre 2018

Plan

- Qu’est-ce que le RGPD ?
  - Aspect règlementaire
  - Conséquence
- Quel est son but ?
- Quelques définitions
- Quels sont les acteurs, leurs droits et obligations ?

▪▪▪▪

- Comment se mettre en conformité et procéder ?
  - Recenser
  - Sécuriser

Qu’est ce que le RGPD ?

Plus qu’une formalité,
Une nouvelle approche
des données publiques

Septembre 2018

Qu’est-ce que le RGPD ?

Un processus qualité

I - Une réglementation :

Issu de la **Loi 78-17** du 6 janvier 1978 dite « Loi Informatique et Libertés » dernièrement modifiée en date du 20 juin 2018,

le **Règlement Général sur la Protection des Données** n°2016-679 a été adopté le 27 avril 2016 et publié au JO UE le 4 juin 2016.

Il est applicable en France depuis le 25 mai 2018.

Qu'est-ce que le RGPD ?

Un processus qualité

II - Une obligation :

Le règlement impose la mise en place de procédures pour l'obtention de résultats (transparence, traçabilité).

Organisme de contrôle : la CNIL.

Introduction de sanctions sévères pouvant aller de 10 à 20M€, de 2 à 4% du CA pour un sous traitant (entreprise privée) ou l'obligation de stopper le traitement ainsi que des sanctions pénales.

Son but
Sécuriser les données personnelles

- Homogénéiser et harmoniser les règles sur l'ensemble du territoire européen. (une règlement unique pour tous)
- Instaurer un climat de confiance entre le collecteur et le collecté (consentement express pour être assuré du respect de la vie privée).
- Renforcer ce droit des personnes et les rassurer avec le droit à la portabilité, le droit à réparation, l'effacement….
- Améliorer l'efficacité : obligation d'exactitude des données nécessitant l'identification des données strictement nécessaires, la mise à jour permanente et le respect de la durée de conservation.

Son but

- Sécuriser les données : protection du patrimoine d'informations ET des données des personnes pour minimiser le risque de fuite (fiabilisation du système).

- Crédibiliser la régulation par des sanctions encadrées, graduées et renforcées (jusqu'à 20M€) et une collaboration entre les autorités de protection des données.

Définitions

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

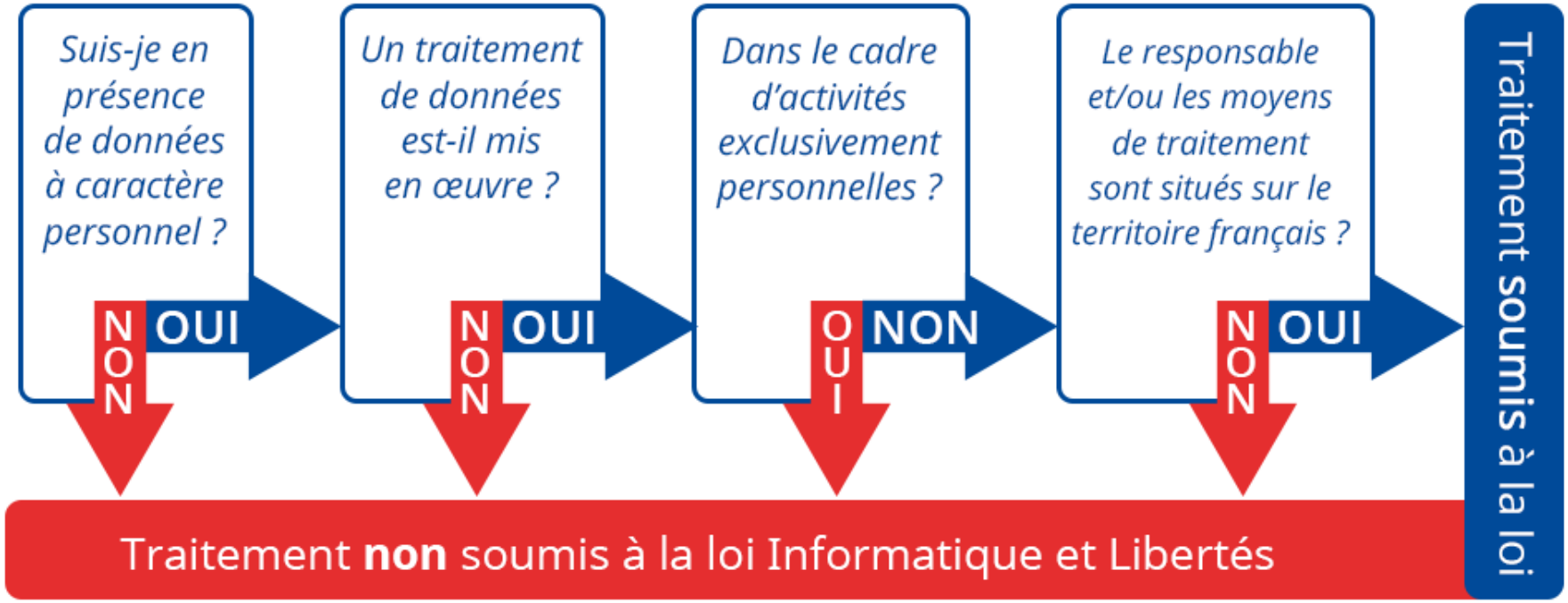
Il s’agit de toute information se rapportant à une personne physique.

Une attention particulière doit être portée sur les données dites « sensibles » dans lesquelles l’on trouve, entre autre, l’origine raciale ou ethnique, l’appartenance syndicale, l’opinion politique, des données de santé, orientation sexuelle….

Définitions

- Qu’est-ce qu’un traitement ?

Il s’agit de toutes opérations appliquées à des données à caractère personnel.
Le champ est vaste, il peut s’agir de collecte, enregistrement, conservation, extraction, consultation, transmission, effacement, …



Extrait infographie CNIL

Quels sont les acteurs ?

Les acteurs

- Le responsable du traitement :

Est celui qui décide à quoi va servir le traitement et qui a pouvoir de signature.

Il est l'autorité territoriale, ou son délégué de pouvoir, qui sera soumis, en cas de défaut de mise en œuvre (résultat) du Règlement, à de lourdes sanctions engageant sa responsabilité personnelle (civile et pénale).

Une simple délégation de signature ne suffit pas à engager la responsabilité de l'intéressé.

Les acteurs

- Le sous traitant :

Est toute personne physique ou morale qui traite des données à caractère personnel pour le compte du Responsable du traitement.

Exemples :
- Le gérant d'une société de prestation de service informatique titulaire d'un marché est un sous traitant.

C'est lui qui aide le Responsable du traitement à respecter ses obligations dans le cadre de la prestation fournie.

Les acteurs

- Le destinataire :

Est celui qui reçoit des données à caractère personnel, le « traitant ». Il peut aussi être un tiers « autorisé ».

Exemple :
- L'Ursaff est un destinataire, au sens où il ne traite pas les données pour la collectivité (non sous traitant) mais pour son propre compte.

- Les tiers « autorisés »:

Sont des autorités publiques ou des auxiliaires de justice (huissier, justice, …)

- <u>Le Délégué à la Protection des Données</u> :

  DPD (D$_{ata}$ P$_{rotector}$ O$_{fficer}$ en version anglosaxone).

  Il se substitue à l'ancien CIL (Correspondant Informatique et Liberté) dont les missions évoluent. Il orchestre la mise en œuvre du RGPD au sein d'une structure.

  Son rôle :

- Informer et sensibiliser ; diffuser d'une culture « Informatique et Libertés »
- Veiller au respect du cadre légal
- Proposer et conduire des actions de sensibilisation sur les bonnes pratiques.
- Informer, responsabiliser et alerter si besoin, le responsable de traitement

- Le Délégué à la Protection des Données :

Suite…

- Analyser, investiguer, auditer, contrôler les déclarations
- Établir et maintenir une documentation au titre de « l'Accountability » : Responsabilité du Responsable de traitement de justifier le respect de la règlementation
- Assurer la médiation avec les personnes concernées
- Présenter un rapport annuel au responsable de traitement
- Interagir avec l'autorité de contrôle CNIL.

Les obligations

I - Vis à vis de la vie privée de la personne :

Pour être licite, le traitement doit recevoir :

- Le consentement préalable et actif de la personne, de traiter ses données

OU

- Entrer dans le cadre :

- d'une obligation légale incombant au responsable de traitement (Ex : Etat Civil)*
- d'une mission de service public (Ex : Action Sociale)*
- de la sauvegarde de la vie de la personne
- d'un contrat dont la personne est partie prenante
- de la réalisation de l'intérêt légitime du responsable de traitement

** A savoir, la majorité des actions des collectivités.*

Les obligations

- Informer la personne sur la finalité du traitement de ses données et de ses droits (voir infra).

Cela suppose qu'une fois informé, tout changement devra requérir une nouvelle information et consentement de la personne dont les données à caractère personnel sont utilisées.

Ex : Un élu ne peut utiliser un fichier inscription scolaire pour sa communication politique. Néanmoins il pourra utiliser la liste électorale

Les obligations

II - Vis-à-vis de la conformité au Règlement :

- Pouvoir justifier les moyens mis en œuvre pour être conforme (Accountability).
- Informer les « collectés » de leurs droits (gestion et perte de données)
- Instaurer des campagnes d'exactitude de données (MAJ).
- Conservation des données dans la limite de leur finalité ou obligation légale (ref : Bonnes pratiques, Archives, …)

Les obligations

- Sécurisation des systèmes d'information

Elle suppose la mise en place de moyens pour s'assurer que :

1°) seules les personnes habilitées auront accès aux données personnelles.

2°) les outils des agents sont protégés contre les « malwares », programmes malveillants qui peuvent absorber des données.

Ceci s'applique également aux données sensibles stockées sur papier dont la garantie de confidentialité doit être mise en œuvre (clés, barreaux …).

- Suivi

Rester en veille sur la donnée qui doit, dans le temps, rester confidentielle, fiable et disponible ou effacée.

Les droits

Vis à vis de la vie privée de la personne :

- Le droit d'accès
- Le droit à rectification
- Le droit à l'effacement
- Le droit à la portabilité des données
- Le droit à la limitation des traitements
- Le droit d'opposition

Ils doivent être communiqués au « collecté » pour qu'il puisse les exercer.

Les droits

- Le droit d'accès

Il permet à tout usager de pouvoir connaître et accéder aux données que détient un responsable de traitement.

⇒ Suppose une plateforme d'accès où sont recensés :

- Le responsable de traitement et ses coordonnées
- Le cadre juridique. Les finalités du traitement
- La destination des données (profilage ou traitement ultérieur)
- Le(s) destinataire(s) des données et si elles ont vocation à être envoyées à l'Etranger.
- La durée de leur conservation

= consultation du registre

Les droits

- Le droit d’accès

Suite…

<u>Les cas où la personne ne peut disposer de ces informations à sa demande</u> :
- La personne dispose déjà de ces informations
- Le traitement de recherche est trop conséquent (recherche archives, statistique…)
- Si contradiction avec le droit national ou atteinte aux intérêts légitime
- S’il y a obligation de secret professionnel (secret médical)

Les droits

- Le droit à la rectification

Toute demande de l'utilisateur pour modification de ses données doit être satisfaite dans un délai de 1 mois. Au plus, 3 mois si complexité avec plusieurs tiers. Au-delà d'1 mois, l'utilisateur devra être informé des motifs du dépassement de ce délai.

- Le droit à l'effacement ou droit à l'oubli

Bien qu'existante dans Le RGPD, cette notion ne devrait être que très peu usitée dans les collectivités. Il s'applique pour les données qui ne sont plus nécessaires à la finalité du traitement, l'opposition du « collecté » au traitement, le retrait de consentement, un traitement reconnu illicite ou dans le cadre de la protection des mineurs.

Les droits

- Le droit à la portabilité des données

Il permet à la personne de récupérer ses données pour les réintégrer, le cas échéant, dans d'autres services.
Ex : Cas de France Connect

- Le droit à la limitation des traitements

La limitation des traitements est le fait de suspendre l'utilisation des données lorsqu'elles sont inexactes ou que le traitement présente un caractère illicite.
Les données restent stockées mais ne sont pas utilisables jusqu'à nouveau consentement du « collecté ».

 *Cela suppose un marquage électronique pour suivi*

Les droits

- Le droit d’opposition

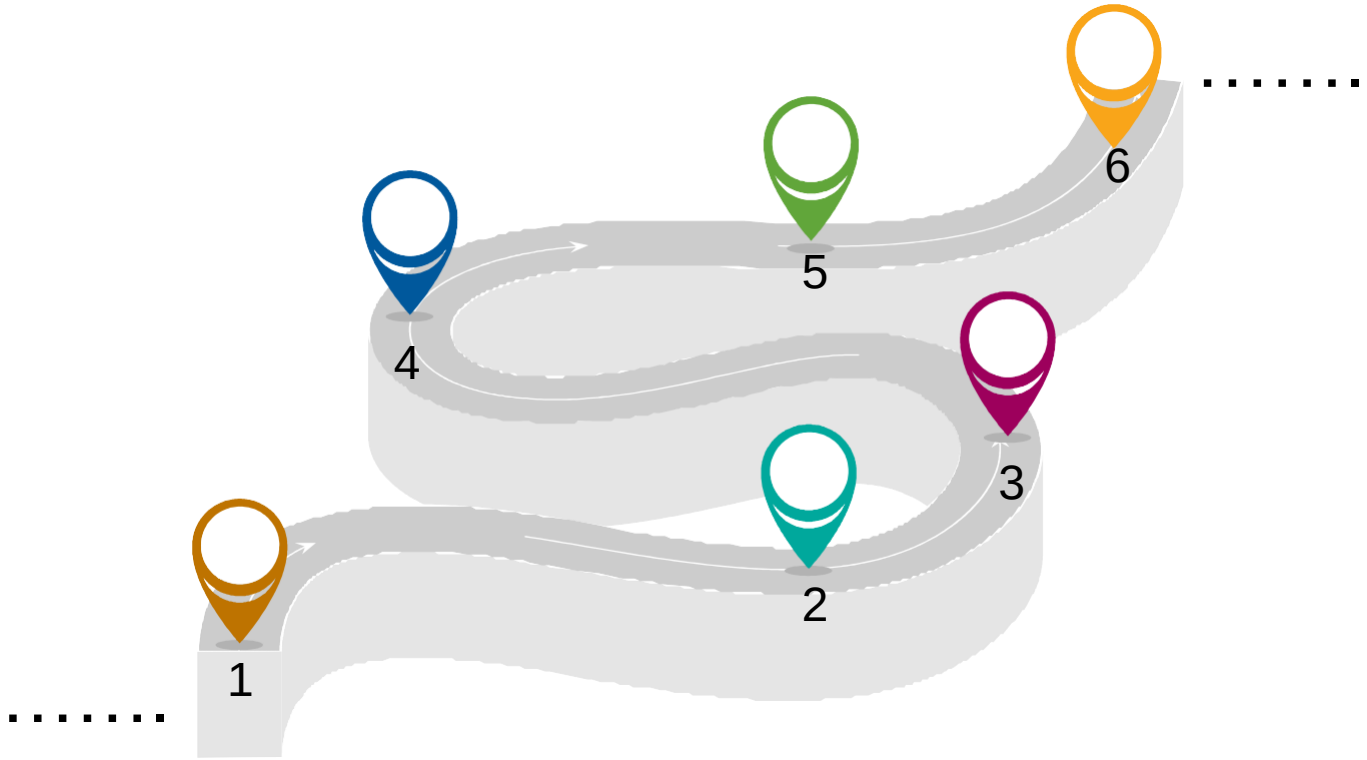
Il permet au « collecté » de s’opposer au traitement de ses données personnelles.

Pour répondre à ce droit, la collectivité devra prouver, le cas échéant, le bien fondé de l’utilisation de ces données.

En vidéo

- https://www.youtube.com/watch?v=WME4O1X4PBE
- https://www.dailymotion.com/video/x2eppuf
- https://www.dailymotion.com/video/x6b3fpu
- WWW.CYBERMALVEILLANCE.GOUV.FR.

Comment se mettre en conformité ?

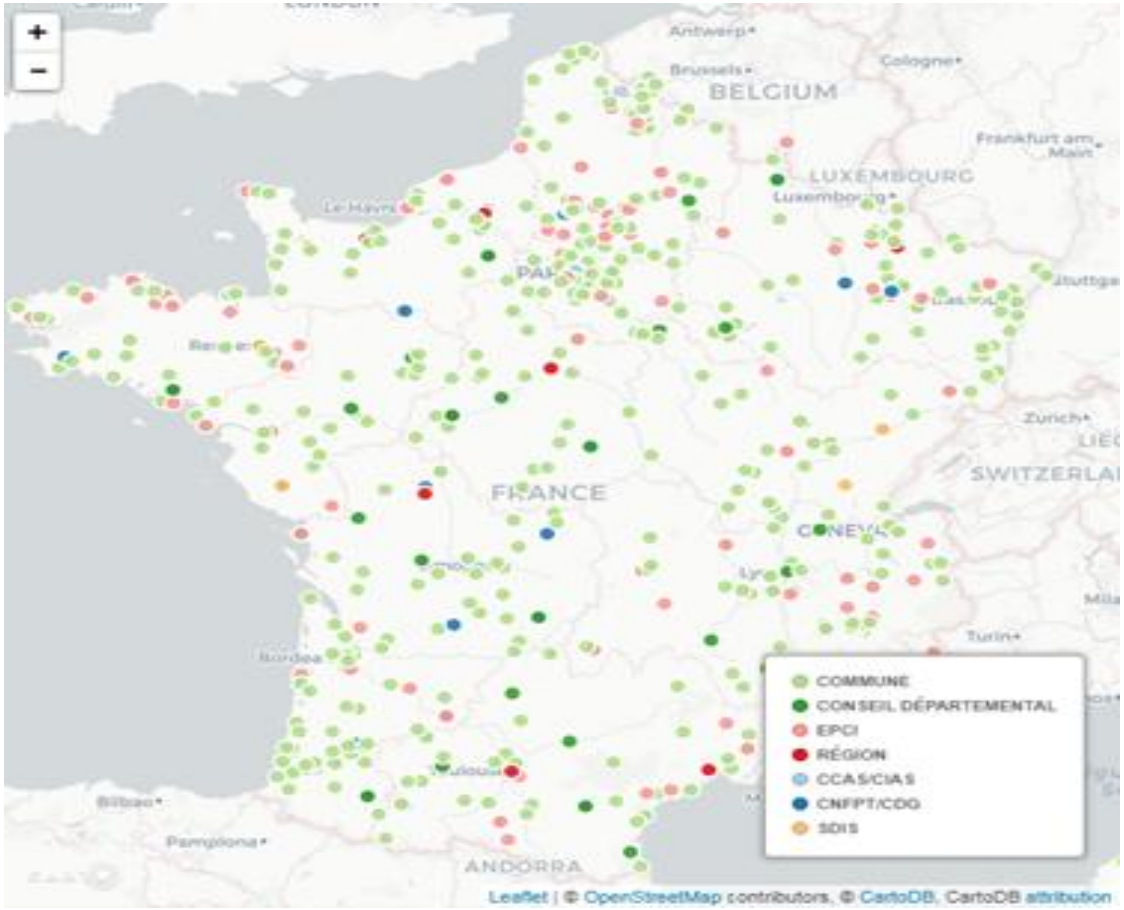


- A l’échelle territoriale, tous les services sont concernés : état civil, élection, urbanisme, action sociale, ressources humaines…

1°) Désigner un DPD (Délégué à la Protection des Données). Rappel : Il a pour mission de connaître tous les traitements de données à caractère personnel, de préparer les outils de gestion, d’informer, de répondre aux plaintes…

Possibilité de déléguer, mutualiser, externaliser cette mission. Dans ce cas, nommer un RPD (Référent/Relai à la Protection des Données) au sein de la collectivité permettra de faire le lien avec le DPD.

La carte des CIL des collectivités territoriales, établi par la gazette et publiée le 7/7/2015 suite à la diffusion de la CNIL en open data



2°) Cartographier tous les traitements réalisés et en établir un registre.

- Inventorier les données par la mise en place d'une procédure de recensement des traitements (quoi, où, pourquoi, qui, jusqu'à quand, comment ?)

- *Adopter des mesures permettant à chaque agent de sécuriser ses accès informatiques (Sensibilisation/formation, charte informatique …).*

- Etablir une charte pour la protection des données personnelles. Modèle ville de limoges

3°) Identifier les actions à mener pour se conformer aux obligations du RGPD et les prioriser au regard des risques encourus pour l'établissement et les personnes concernées.

- Nécessité d'obtention de consentement ou non

…

4°) Gérer les risques, anticiper et gérer la crise en cas de violation des données.

- Réaliser des études d'impact sur la vie privée (EIVP) en cas de données « sensibles ». Celle-ci peut être appelée PIA en terme Anglosaxon.

5°) organiser pour mettre en place des actions concrètes pour la maitrise du cycle de vie des données ; anticiper les situations de crise.

6°) Mettre en place un vrai système de suivi permettant de dégager sa responsabilité.

7°) Tenir à jour les documents permettant de prouver la conformité au règlement européen (suivi).

En savoir plus :

https://www.cnil.fr/professionnel

En espérant que le RGPD devienne vite, sans l’entraver, un réflexe de votre activité quotidienne

…

Merci de votre présence
et
de votre attention.

Avez-vous des questions ?

Pour plus d'informations
Délégué à la protection des données
Rue François Arago – 61250 Valframbert
0233804811
rgpd@cdg61.fr
www.cdg61.fr

Septembre 2018