

Pédago*Lab*

DONNÉES PERSONNELLES ET CYBERSÉCURITÉ

4 ans après, où en êtes-vous ?

Marie Gauthier, juriste RGPD (partie 1)

Bertrand Gayraud, responsable informatique (partie 2)

Groupe Pédagofiche

Règlement Général sur la Protection des Données (RGPD)

Quels impacts pour les collectivités ?





Avant-propos

Le Règlement Général pour la Protection des Données est entré en vigueur le 25 mai 2018, soit il y a plus de 4 ans.

Les collectivités territoriales sont directement impactées par cette règlementation dès lors qu'elles traitent chaque jour de nombreuses données personnelles concernant leurs administrés (état civil, listes électorales, inscriptions scolaires, aides sociales, données médicales, site internet etc…).

Pour autant, nombre de ces collectivités n'ont toujours pas désigné de délégué à la protection de données et n'ont pas initié de réelle démarche de conformité.

Il convient, en premier lieu, de comprendre la philosophie du RGPD de manière à mieux appréhender, dans un second temps, sa mise en application.

La philosophie du RGPD



L'objectif premier du RGPD est de **renforcer les droits des personnes concernées par le traitement de données personnelles** en proposant une règlementation applicable à tous les états membres de l'Union Européenne.

Le RGPD impose à tous les organismes (publics comme privés dès lors qu'ils traitent de données personnelles) une **obligation générale de transparence.**

Le RGPD consacre le **principe de responsabilité** : le responsable de traitement est tenu de garantir la sécurité des données personnelles. Il doit s'assurer et être en capacité de démontrer que le traitement a été réalisé conformément au RGPD.

Quelques définitions



<u>Une donnée personnelle</u>

Toute information se rapportant à une personne physique identifiée ou identifiable :

- **directement**
- **indirectement**, notamment par référence :

à un **identifiant**, tel que :

- un nom
- un numéro d'identification
- des données de localisation
- un identifiant en ligne

à un ou plusieurs éléments spécifiques propres à son **identité** :

- physique, physiologique, génétique, psychique
- économique, culturelle ou sociale

<u>Définition très large :</u> toutes données permettant d'identifier une personne physique (nom, date de naissance, immatriculation, données GPS, adresse IP, photographie, voix…).

Exemples de données personnelles traitées par les collectivités territoriales



- **Données individuelles :** nom, prénom, date et lieu de naissance, nationalité, adresse postale, numéro de téléphone, adresse email

- **Données familiales :** naissance, mariage (témoins, professions etc…), PACS, filiation, décès, liens familiaux

- **Données médicales et biométriques :** numéro de sécurité sociale, fiche médicale fournie par la famille, régime alimentaire (cantine scolaire), handicap, empreintes digitales (lors de l'établissement de la carte d'identité), photo

- **Données d'imposition :** impôts locaux, quotient familial, données de redevance des ordures ménagères

Exemples de données personnelles traitées par les collectivités territoriales

- **Données de ressources humaines :** CV, position, ancienneté, statut, absences, maladies, accidents de travail, sanctions, casier judiciaire, syndicalisme, géolocalisation des véhicules utilisés par les employés, situation de santé des conjoints ou enfants en vue d'ouverture de droits
- **Données financières :** aides sociales, CAF, dettes, RIB
- **Données d'urbanisme :** location, propriétés des parcelles
- **Données de concession :** lieu de la concession funéraire au cimetière
- **Données de police municipale :** suivi de délinquance, infractions, verbalisation, pièces d'identité, numéro d'immatriculation du véhicule



Conclusion : Les données personnelles sont omniprésentes pour toutes les opérations concernant une personne physique

Qu’est ce qu’une donnée sensible ?



- Les données sensibles forment une catégorie particulière des données personnelles.
- Ce sont des **informations qui révèlent les origines raciales ou ethniques, les opinions philosophiques ou religieuses, l’appartenance syndicale, la santé ou la vie sexuelle d’une personne physique.**
- **Ces données créent des risques particuliers pour les personnes ce qui nécessite une protection spécifique lors de leur traitement.**
- Le RGPD interdit de recueillir ou d’utiliser ces données sauf dans certains cas précis.

Un traitement de données personnelles

Toute **opération ou tout ensemble d'opérations** effectuées ou non à l'aide de procédés automatisés et **appliquées à des données ou des ensembles de données à caractère personnel** telles que :

- la collecte,
- l'enregistrement,
- l'organisation, la structuration,
- la conservation,
- l'adaptation ou la modification,
- l'extraction, la consultation, l'utilisation,
- la communication par transmission,
- la diffusion ou toute autre forme de mise à disposition,
- le rapprochement ou l'interconnexion,
- la limitation,
- l'effacement ou la destruction.



Le traitement n’est pas nécessairement informatisé : les fichiers papiers sont également concernés.

Exemples de traitements de données personnelles par les collectivités territoriales

- Gestion de l'état civil
- Recensement de la population
- Listes électorales
- Cadastre
- Enquêtes à des fins statistiques
- Communication politique
- Facturation des services mis à la disposition des parents (transports et restaurants scolaires, centres aérés et garderies, crèches municipales)
- Fichiers des demandeurs d'emploi
- Fichiers de logements vacants
- Fichiers des maires relatifs à la prévention de la délinquance
- Gestion des aires d'accueil des gens du voyage
- Gestion des ordures ménagères
- Mise en recouvrement de taxes et redevances
- Système de vidéosurveillance
- Téléservices (état-civil, passeport, élections, carte d'identité etc.…).

Le responsable du traitement

« La **personne** physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, **détermine les finalités et les moyens du traitement.** »

Dans le cadre d'une collectivité, c'est son représentant légal :

- le maire
- le président de l'EPCI...



Une logique inversée



D’une logique de **contrôle a priori,** basée sur des formalités déclaratives auprès de la CNIL…

… à une **logique de responsabilisation** (« accountability ») basée sur un **contrôle a posteriori.**

La **collectivité** devient **responsable de la protection des données** traitées.
Elle doit s’assurer par elle-même de la conformité des traitements opérés sur les données personnelles.

Sanctions et voies de recours



En tant qu'autorité de contrôle, **la CNIL** peut :

- Effectuer des enquêtes de sa propre initiative ou suite à une réclamation d'une personne concernée
- Adopter des mesures correctrices : avertissement, rappel à l'ordre, mise en conformité dans un délai déterminé…
- Prononcer des amendes administratives jusqu'à **20 millions d'euros**
- Saisir les autorités judiciaires en vue de faire appliquer les dispositions du règlement.

Les **personnes concernées** par les traitements (administrés et agents) peuvent, si elles estiment que les droits que leur confère le règlement ont été violés par le responsable de traitement, saisir la juridiction compétente en vue d'obtenir la cessation du dommage et la réparation du préjudice moral et/ou matériel subi.

Les grands principes du RGPD



- **Principe de minimisation des données** : limiter la collecte aux seules données strictement nécessaires à l'objectif poursuivi. Exemple : le recueil du numéro de Sécurité sociale des parents n'est pas justifié pour le fichier des inscriptions scolaires.

- **Principe de loyauté du traitement** : les données ne peuvent être recueillies et traitées que pour un usage déterminé et légitime qui doit correspondre aux missions de la collectivité.. Exemples : le fichier des demandeurs d'emploi ne peut pas être utilisé pour de la communication politique.

- **Principe de durée de conservation adaptée** : la durée n'excède pas celle nécessaire au regard des finalités pour lesquelles les données sont traitées.

Les grands principes du RGPD



- **Principe de sécurité adaptée au traitement** : la sécurité doit être adaptée au niveau de risque induit par les finalités. Le maire ou tout autre représentant légal doit veiller à mettre en place et gérer le renouvellement des mots de passe, ou encore, déterminer différentes règles d'accès aux données et gérer les habilitations.

- **Principe de respect des droits des personnes** : lors du recueil des informations, les administrés doivent être informés de leurs droits.

La méthodologie à mettre en place

Protection des données « *dès la conception et par défaut* »

1. Désigner un DPD
2. Identifier les foyers de données personnelles
3. Réaliser un registre de traitements
4. Encadrer la sous-traitance de traitements
5. Sécuriser les données
6. Organiser la prise en charge des demandes d'exercice des droits des personnes

1 - Désigner un DPD

- La désignation d'un DPD constitue la première étape **obligatoire** à respecter par les Collectivités territoriales.

" Chef d'orchestre "

Obligatoire



Indépendant

DPD : Délégué à la protection des données (DPO - data protection officer)

1 - Désigner un DPD



Ses missions : veiller au respect des nouvelles règles

- Il **informe et conseille** le responsable du traitement et les agents sur les obligations et les outils disponibles
- Il **contrôle le respect du RGPD**
- Il est l'**intermédiaire** entre la collectivité et la CNIL
- Il **conseille la collectivité sur la réalisation des analyses d'impact (PIA)** sur la protection des données et en vérifie l'exécution
- Il **tient le registre des traitements** et dresse un bilan annuel.

En clair, le DPO a un rôle actif pour assister le responsable de traitement dans la mise en conformité de son organisation.

1 - Désigner un DPD

Un niveau d'expertise et des moyens pour exercer son rôle

➡ **Connaissances spécialisées du droit et des pratiques** en matière de protection des données

➡ **Moyens suffisants** pour mener à bien ses missions :

- ressources en temps, personnels et matériels
- accès aux informations nécessaires
- associé aux questions « Informatique et Libertés »
- formations nécessaires

➡ **Agir en toute indépendance :**

- pas de conflit d'intérêts
- pouvoir rendre compte au plus haut niveau
- ne pas être sanctionné
- ne pas recevoir d'instruction

La fonction de DPD n'est pas exclusive : le DPD peut exécuter d'autres missions et tâches dès lors que celles-ci n'entrainent pas de conflits d'intérêt (il ne peut pas être le DGS ou le directeur financier par exemple).

1 - Désigner un DPD

	Points positifs	Points négatifs
DPD interne	• Agent déjà présent au sein de la collectivité • Coût	• Choix restreint • Indépendance • Formation nécessaire • Conflits d'intérêt • Temps et moyens insuffisants
DPD externe	• Profil déjà formé • Vision nouvelle de la collectivité • Indépendance	• Règles de publicité et de mise en concurrence • Choix - Coût • Temps d'adaptation • Respect de la confidentialité
Convention de prestations de services	• Profil déjà formé • Vision nouvelle • Indépendance • Coût	• Règles de publicité et de mise en concurrence • Choix • Temps d'adaptation • Respect de la confidentialité
Mutualisation d'un DPD (service unifié ou service commun)	• Agent : choix plus important qu'en interne • Coût mutualisé	• Indépendance • Formation nécessaire • Conflits d'intérêt

2 - Identifier les "foyers" de données personnelles

Quoi ?

- Les différents traitements de données personnelles
- Les catégories de données personnelles traitées (sensibles ou pas)

Qui ?

- Les acteurs internes et externes : responsable du traitement, DPD, responsables de services, prestataires sous-traitants…

Pourquoi ?

- Les objectifs poursuivis / finalités du traitement des données

2 - Identifier les "foyers" de données personnelles

Où ?

- Le lieu d'hébergement des données
- Les flux : origine et destination des données

Comment ?

- Les mesures de sécurité mises en place

Jusqu'à quand ?

- La durée de conservation



3 - Réaliser un registre des activités de traitement

Le maire se doit de tenir un registre de traitement.

C’est le document dans lequel seront référencés tous les traitements de données de votre collectivité, suite au travail de recensement.

Il faut le tenir à disposition de la CNIL pour prouver votre mise en conformité sous forme écrite et électronique. Il va venir en remplacement des formalités CNIL (déclaration simplifiée etc…).



3 - Réaliser un registre des activités de traitement



Pour chaque activité recensée, il convient de préciser :

- La finalité, l'objectif poursuivi; (ex : recensement citoyen)
- La catégorie de données utilisées (ex : nom, prénom, adresse, filiation)
- Les destinataires des données
- La durée de conservation de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive)
- Les mesures de sécurités mise en place pour la protection des données
- Le transfert des données hors de l'Union Européenne.

4 - Recadrer la sous-traitance des traitements

Nouveauté du RGPD : la responsabilité du sous-traitant

Le sous-traitant :

- doit respecter le RGPD
- doit agir selon les instructions du responsable du traitement



4 - Recadrer la sous-traitance des traitements



Les obligations des sous-traitants :

Il convient de préciser dans le contrat conclu avec le sous-traitant :

- une obligation de transparence et de traçabilité : le sous-traitant doit mettre à votre disposition toutes les informations nécessaires pour démontrer le respect de vos obligations et pour permettre la réalisation d'audits ;
- la prise en compte des principes de protection des données dès la conception et par défaut ;
- une obligation de garantir la sécurité des données traitées ;
- une obligation d'assistance, d'alerte et de conseil (par exemple une procédure de notification des violations de données personnelles doit être fixée).

5 - Organiser la protection des données

Exemples de précautions élémentaires en matière de sécurité informatique :



- Définir un identifiant unique par utilisateur et interdire les comptes partagés ;
- Choisir un mot de passe **complexe** qui protège l'accès aux données ;
- Modifier ce mot de passe régulièrement ;
- Utiliser des antivirus régulièrement mis à jour ;
- Détruire tout email d'origine inconnue ou douteuse ;
- Limiter la connexion de supports mobiles (clés USB, disques durs externes, etc…) à l'indispensable
- Prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné.

5 - Organiser la protection des données



Que faire en cas de violation de données ?

Si des données ont été, de manière accidentelle ou illicite, altérées, perdues, divulguées (à de mauvais destinataires) ou détruites et que cette violation présente un risque pour les droits et libertés des personnes, **il convient de le signaler à la CNIL dans les 72 heures.**

Cette notification s'effectue sur le site web de la CNIL :
https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Par ailleurs, si cette violation de données présente un risque élevé pour les personnes, il convient de les en informer.

6 - Organiser la prise en charge des demandes d'exercice des droits des personnes

A chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc..) doit comporter des mentions d'information qui répondent aux questions suivantes :

- Pourquoi vous collectez les données ?
- Qu'est-ce qui vous autorise à traiter ces données ?
- Qui a accès à ces données ?
- Combien de temps vous les conservez ?
- Comment les personnes concernées peuvent exercer leurs droits ?
- Est-ce que ces données sont transférées hors de l'UE ?



Les mentions d'information doivent être adaptées aux situations et aux supports de collecte.

6 - Organiser la prise en charge des demandes d'exercice des droits des personnes

La collectivité doit organiser des modalités permettant aux administrés d'exercer leurs droits.

Elle doit répondre dans les meilleurs délais à leurs demandes de droits d'accès, de rectification ou de suppression de leurs données, voire d'opposition, sauf si le traitement répond à une obligation légale.

Ces droits doivent pouvoir s'exercer par voie électronique à partir d'une adresse dédiée.

Si vous disposez d'un site internet, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée telle que « dpo@nomdelamairie.fr ».



Comment mettre en place le RGPD au sein de votre collectivité ?

Mettre en place le RGPD : Nos solutions adaptées à vos besoins



a) Vous n’avez pas désigné de DPO : notre solution de DPO externalisé

La collectivité confie la qualité de DPO à notre société. En plus de la documentation pratique, notre mettrons à votre disposition les outils et les moyens nécessaires à la mise en conformité de votre organisme (écarts de conformité constatés et méthodologie de réduction des écarts, préconisation de sécurité, avenants pour les prestataires, procédures, etc.).En outre, nous nous chargerons d’établir et d’actualiser le registre de traitement.

Comment mettre en place le RGPD au sein de votre collectivité ?

Mettre en place le RGPD : Nos solutions adaptées à vos besoins



b) Vous avez désigné un DPO en interne : nous lui apportons notre assistance

Notre équipe accompagnera le DPO désigné en interne dans son travail de mise en conformité de la collectivité au RGPD.

c) Votre DPO a besoin de notre analyse juridique ponctuelle : audit, conseil, assistance.

Avec cette offre, votre DPO pourra solliciter nos experts pour toute question juridique liée à la l'application du RGPD (sujets organisationnels ; mise en place de nouveaux projets internes ; etc.).

Groupe Pédagofiche

Merci

pour votre attention

