Groupe Pédagofiche

Règlement Général sur la Protection des Données (RGPD)

Quels impacts pour les collectivités ?

Version mars 2021

Groupe Pédagofiche

AVANT-PROPOS

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

Les collectivités territoriales sont directement impactées par cette règlementation dès lors qu'elles traitent 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.

Le Contexte

De la loi « Informatique et Libertés » de 1978 au RGPD (mai 2018)

Les raisons :

- évolution des technologies
- volume des données collectées
- défaut de fiabilité / déficit de confiance
- nécessité d'harmoniser les niveaux de protection dans l'UE

Ce qui change :

- nouvelle logique de responsabilité
- DPD obligatoire
- droits des personnes renforcés ou nouveaux
- sanctions alourdies

Quelques définitions

Une donnée personnelle:

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

- **Définition très large :** 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;

- **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.

Groupe Pédagofiche

Exemples de traitements de données personnelles par les collectivités territoriales :

- Registres des personnes âgées ou handicapées mis en œuvre dans le cadre du plan d'alerte et d'urgence départemental en cas de risques exceptionnels (canicule, grands froids etc…);
- 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);
- Gestion de l'état civil;
- Fichiers des demandeurs d'emploi;
- Logement social;
- 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

- **l'élu** / responsable du traitement :
  - jusqu'à 20 millions € d'amende
- le **sous-traitant** :
  - 2 à 4 % du CA

Ces sanctions peuvent être rendues publiques.

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 :** le traitement effectif doit être conforme aux finalités annoncées. Exemples : le fichier des demandeurs d'emploi ne peut pas être utilisé pour de la communication politique /les données enregistrées aux fins d'inscription d'un acte sur le registre de l'état civil ne peuvent être utilisées par les élus municipaux pour adresser des félicitations ou des condoléances.

- **Principe de durée de conservation adaptée :** la durée n'excède pas celle nécessaire au regard des finalités pour lesquelles les données sont traitées. Exemple : les enregistrements de vidéo protection ne peuvent pas être conservés plus d'1 mois.

- **Principe d'exactitude :** les données sont exactes et, si besoin, tenues à jour.

- **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.

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 <u>obligatoire</u> 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

1 - Désigner un DPD

en interne : 3 possibilités

1 - L'agent exerçant les fonctions de Correspondant informatique et libertés (CIL) au sein de la collectivité

2 - Un agent déjà en poste dans la collectivité (titulaire, stagiaire, contractuel)

- Modifier la fiche de poste

3 - Un nouvel agent

- Agent titulaire : création de poste : délibération du CM + arrêté du maire
- Agent contractuel : rédaction d'un contrat de travail

Le maire, les adjoints et les conseillers municipaux ne peuvent, pour leur propre commune, exercer les missions de DPO.

Cas particulier : la mise à disposition d'un agent d'une autre collectivité

Groupe Pédagofiche

1 - Désigner un DPD

en externe : 3 possibilités

1 - Signer une convention avec le centre de gestion

2 - Recourir à un prestataire privé

⚠ Obligation de réaliser une mise en concurrence des prestataires

3 - Recourir à un syndicat mixte spécialisé
(informatique/numérique)

Groupe Pédagofiche

1 - Désigner un DPD

Dispositifs de mutualisation : 4 possibilités

1 - Signature d'une **convention entre collectivités et groupements** ayant pour objet la réalisation de prestations de service liées au traitement de données à caractère personnel (*article 31 de la loi 2018-493 du 20 juin 2018*)

2 - Signature d'une **convention** de prestation de service **entre des EPCI ou entre des communes membres d'un même EPCI à fiscalité propre** lorsque le rapport relatif aux mutualisations de services le prévoit (*article L. 5111-1 du CGCT*)

3 - Création d'un **service unifié** entre collectivités et groupements (*article 31 de la loi 2018-493 du 20 juin 2018*)

4 - Création d'un **service commun** entre un EPCI à fiscalité propre et une ou plusieurs de ses communes membres (*article L. 5211-4-2 du CGCT*)

Groupe Pédagofiche

1 - Désigner un DPD

	Points positifs	Points de vigilance
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

Groupe Pédagofiche

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 de données

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…).

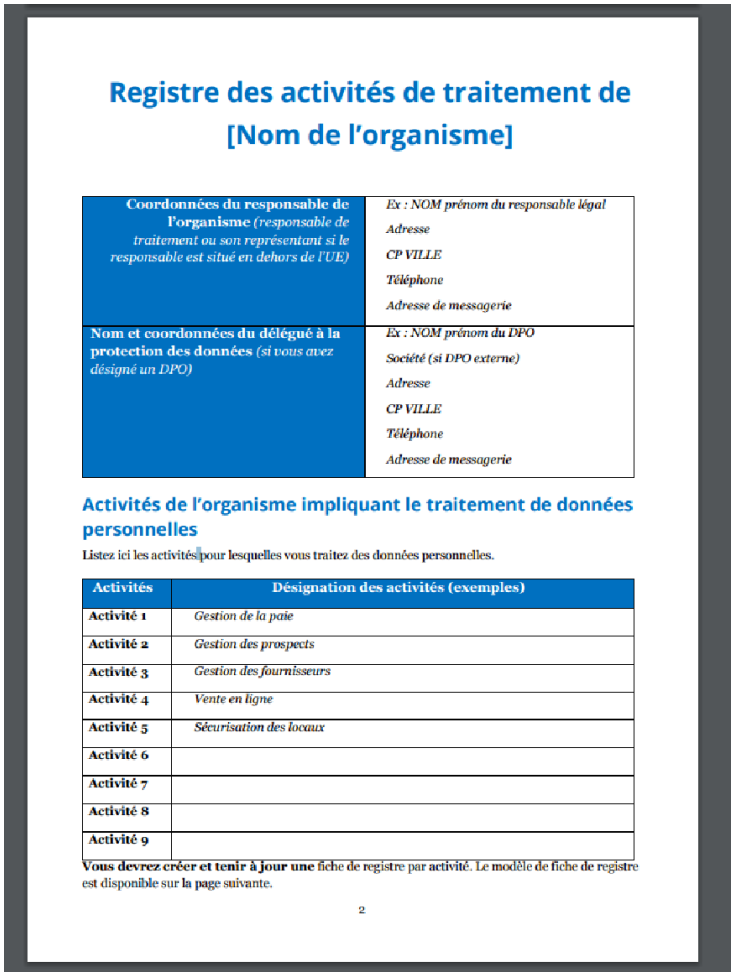
Pour chaque activité recensée, il convient de préciser :

- 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.

Groupe Pédagofiche

3 – Réaliser un registre des activités de traitement

Registre



Registre des activités de traitement de [Nom de l'organisme]

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	*Ex : NOM prénom du responsable légal* *Adresse* *CP VILLE* *Téléphone* *Adresse de messagerie*
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	*Ex : NOM prénom du DPO* *Société (si DPO externe)* *Adresse* *CP VILLE* *Téléphone* *Adresse de messagerie*

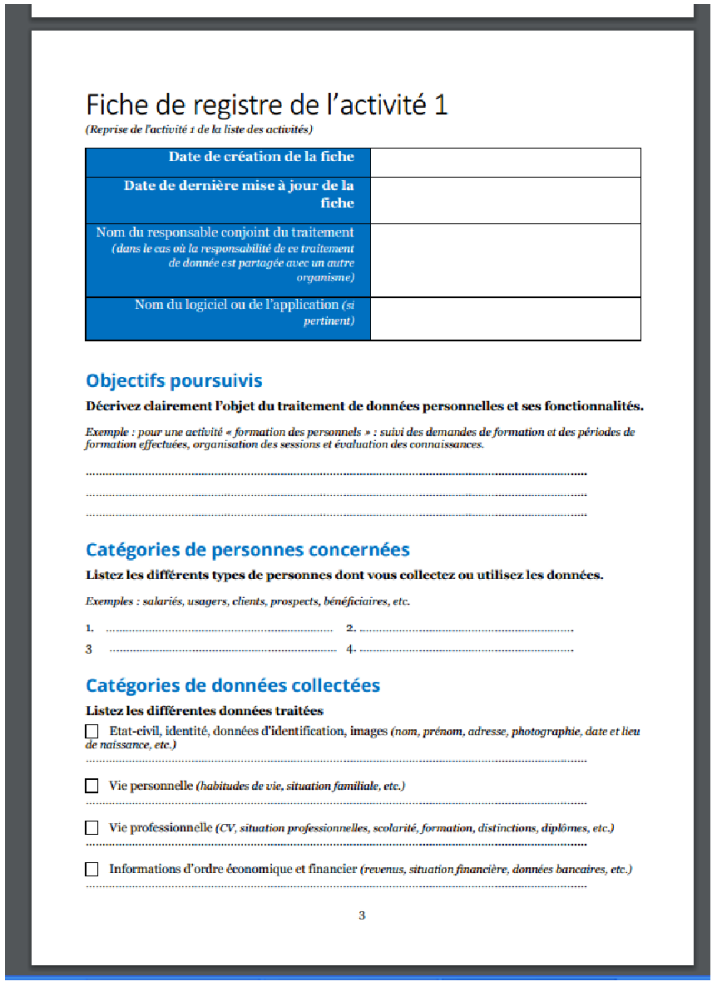
Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités (exemples)
Activité 1	*Gestion de la paie*
Activité 2	*Gestion des prospects*
Activité 3	*Gestion des fournisseurs*
Activité 4	*Vente en ligne*
Activité 5	*Sécurisation des locaux*
Activité 6	
Activité 7	
Activité 8	
Activité 9	

Vous devrez créer et tenir à jour une fiche de registre par activité. Le modèle de fiche de registre est disponible sur la page suivante.

2



Fiche de registre de l'activité 1

(Reprise de l'activité 1 de la liste des activités)

Date de création de la fiche	
Date de dernière mise à jour de la fiche	
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	
Nom du logiciel ou de l'application *(si pertinent)*	

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.

.....

.....

.....

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. ..... 2. .....

3 ..... 4. .....

Catégories de données collectées

Listez les différentes données traitées

☐ Etat-civil, identité, données d'identification, images *(nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*

.....

☐ Vie personnelle *(habitudes de vie, situation familiale, etc.)*

.....

☐ Vie professionnelle *(CV, situation professionnelles, scolarité, formation, distinctions, diplômes, etc.)*

.....

☐ Informations d'ordre économique et financier *(revenus, situation financière, données bancaires, etc.)*

.....

3

- https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

4 – Encadrer la sous-traitance des traitements

Nouveauté du RGPD : la responsabilité du sous-traitant

Le sous-traitant :

1- doit respecter le RGPD;

2- doit agir selon les instructions du responsable du traitement.

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.**

- *Guide CNIL « Guide de sensibilisation au RGPD pour les collectivités territoriales »:*https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

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.

Groupe Pédagofiche

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.

Groupe Pédagofiche

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.

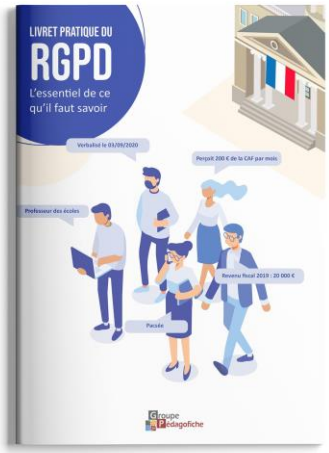
Si vous disposez d'un site internet, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée telle que « dpo@nomdelamairie.fr ».

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

1- Comprendre le RGPD : notre livret pratique

La compréhension du règlement étant le préalable à sa bonne application, nous avons écrit et édité un livret pratique RGPD qui contient l'essentiel de ce qu'il faut savoir sur la mise en œuvre du RGPD au sein des collectivités territoriales.

Ce livret vous permettra d'appréhender au mieux vos nouvelles obligations en matière de traitement des données personnelles. Il est présenté sous forme de 6 focus :



1. Philosophie du RGPD
2. Définitions utiles
3. Mesures à mettre en place
4. Rôle du délégué à la protection des données (DPO)
5. Droits garantis par le RGPD
6. Gestion du consentement

Groupe Pédagofiche

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

2- 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.

b) Vous avez désigné un DPO en interne : votre DPO interne a besoin de nos supports. Notre équipe accompagnera le DPO désigné en interne dans son travail de mise en conformité de la collectivité au RGPD. Avec cette formule, nous livrons l'ensemble de la documentation nécessaire à la mise en conformité RGPD, à savoir notamment un registre des traitements, la politique de confidentialité ainsi que des affiches de droit à l'information qui devront par la suite être affichées au sein de la mairie.

c) Votre DPO a besoin de notre analyse juridique ponctuelle : notre offre de support. 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.). Notre équipe, constituée d'experts RGPD et d'avocats, lui apportera des réponses claires et opérationnelles, et ce dans un temps limité.

Contacts

Pour plus d'informations sur nos produits et services, contactez notre équipe :

Anthony PETIT, Responsable commercial, Responsable des ventes,
Tel. 04 73 60 46 85
Mob. 06 11 79 58 80
anthony.petit@pedagofiche.fr

Marina TINET , Assistante commerciale
Tel. 04 73 60 59 93
marina.tinet@pedagofiche.fr

Lucile DE JESUS, Assistante commerciale
Tel. 04 70 96 51 43
lucile.dejesus@pedagofiche.fr

Marie GAUTHIER, Juriste, Experte RGPD
Tel : 04 73 60 59 93
marie.gauthier@pedagofiche.fr

Groupe Pédagofiche – CS 80005 NOHANENT – 63408 CHAMALIÈRES Cedex – Tél : 04 73 60 59 93 / Fax : 04 73 62 88 76
www.mairiexpert.fr / email : mairiexpert@pedagofiche.fr