

# RGPD

## RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

---

**Mardi 9 octobre 2018**

**VIELMUR-SUR-AGOUT – 10h**

**CAGNAC-LES-MINES – 19h**

# PARTIE I : Cadre juridique du RGPD

- **RGPD : Règlement Général sur la Protection des Données applicable depuis le 25 mai 2018**

Règlement (UE) 2016/679, du 25 avril 2016, *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.*

- Loi « Informatique et Liberté » du 6 janvier 1978, modifiée en 2004, enrichie en 2016 et consolidée en 2018.
- Pourquoi avoir modifié le cadre juridique existant ?

# Qui est concerné ?

Le RGPD s'applique à toute organisation, publique ou privée, qui traite des données personnelles pour son compte ou non, dès lors :

- qu'elle est établie sur le territoire de l'Union européenne,
- ou que son activité cible directement des résidents européens.

# Qu'est ce qui est concerné ?

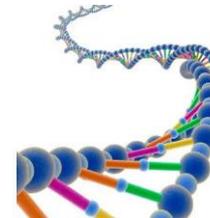
## Article 2 RGPD

*Le RGPD « s'applique au traitement de données à caractère personnel, automatisé en tout ou partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ».*

# Données personnelles (Article 4 RGPD)

« Toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne peut être identifiée directement ou indirectement.



# *Données personnelles (Article 4 RGPD)*

Autrement dit, l'identification d'une personne physique peut être réalisée :

- **Directement** : à partir d'une seule donnée
- **Indirectement** : à partir du croisement d'un ensemble de données

# Traitement (Article 4 RGPD)

- **Opération portant sur des données personnelles, quel que soit le procédé utilisé**

*Collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement.*

- Un traitement de données doit avoir **un objectif**, une finalité.
- **Fichier de données à caractère personnel :**  
*Tout ensemble structuré et stable de données à caractère personnel, accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.*

## *Traitement (Article 4 RGPD)*

- Il ne s'agit pas non plus nécessairement de fichiers, il peut également être question d'une installation de vidéosurveillance, d'un système de paiement par carte bancaire, de reconnaissance biométrique, d'une application pour smartphone, etc...
- **Le traitement n'est pas nécessairement informatisé :** les fichiers papiers sont également concernés.

# Données sensibles (Article 9 RGPD)

Information qui révèle les origines raciales ou ethniques, les opinions publiques, philosophiques ou religieuses, l'appartenance syndicale, la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique.

- Il est interdit de recueillir et d'utiliser ces données, sauf dans certains cas précis :
  - Si la personne a donné un consentement express (écrit, clair et explicite)
  - Si ces données sont nécessaires dans un but médical
  - Si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL
  - Si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique ou syndicale.
- **Attention** à ne pas confondre les données sensibles au sens du RGPD et les données sensibles pour une entreprise ou organisation (données financières, données relatives à la clientèle, dossiers délicats, ...).

# Principes relatifs au traitement des données à caractère personnel (Article 5 du RGPD)

- Licéité, loyauté, transparence
- Finalités de la collecte déterminées, explicites et légitimes
- Collecte adéquate, pertinente et limitée
- Les données doivent être exactes et à jour, sinon, elles doivent être supprimées ou rectifiées
- Limitation de la durée de conservation
- Traitement sécurisé, intègre et permettant de garantir la confidentialité

**Le responsable de traitement doit être en mesure de prouver le respect de ces principes.**

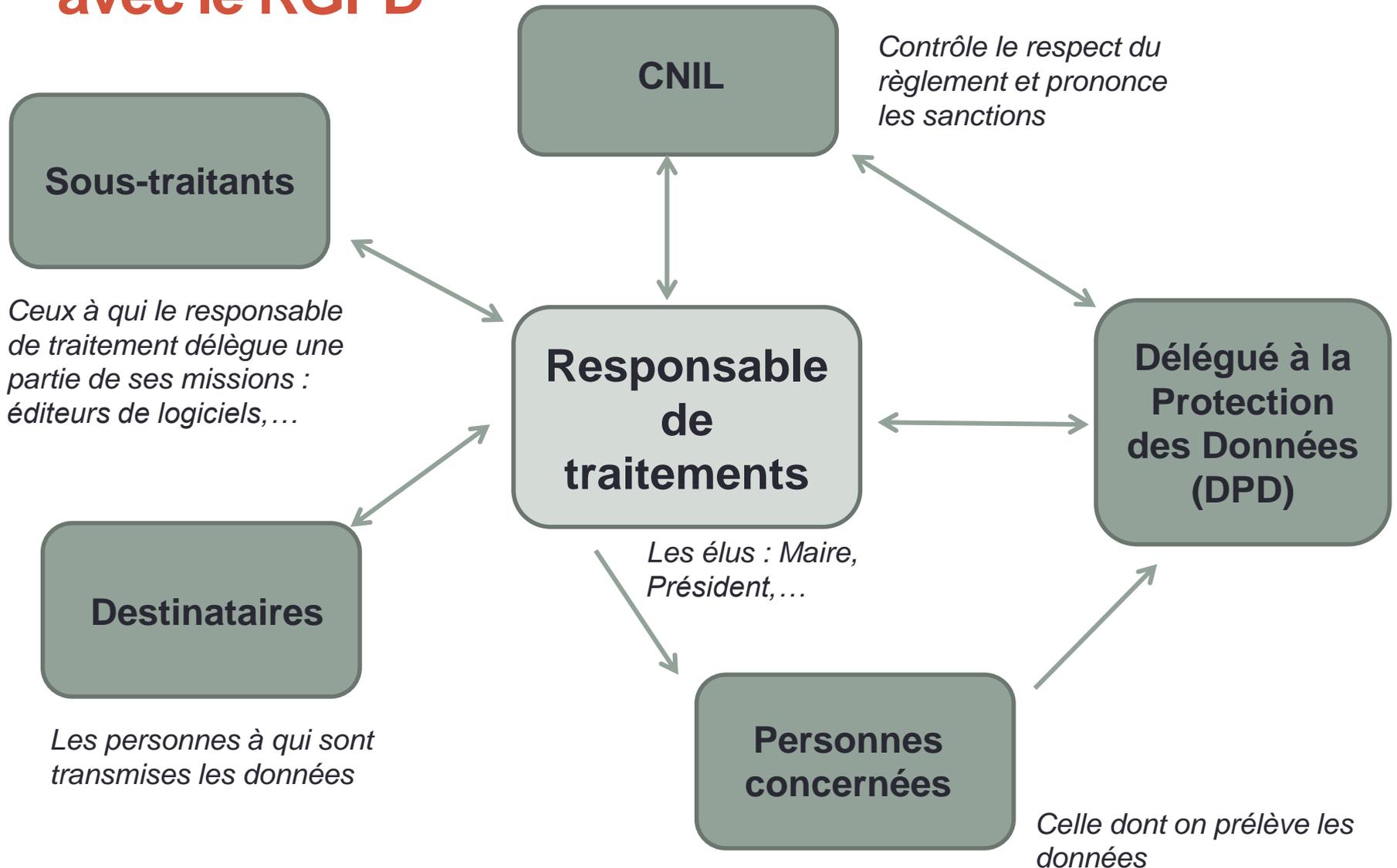
# Sanctions en cas de non-respect du RGPD (Article 83 du RGPD)

En FRANCE, l'autorité de contrôle est la **CNIL** :  
Commission Nationale de l'Informatique et des Libertés.

## **AMENDE MAXIMALE PREVUE PAR LE RGPD**

- 20 millions d'euros d'amende,
- ou pour une entreprise, jusqu'à 4% du chiffre d'affaire annuel mondial total de l'exercice précédent

# Les différents acteurs de la mise en conformité avec le RGPD



# **PARTIE II : Les différentes obligations de mise en conformité**

- **Etape 1 :**
  - Désigner obligatoirement un Délégué à la Protection des Données
- **Etape 2 :**
  - Réaliser un registre de traitements
- **Etape 3 :**
  - Prioriser et mettre à jour les procédures
- **Etape 4 :**
  - Réaliser des analyses d'impacts et analyses de risques
- **Etape 5 :**
  - Assurer et prouver la conformité permanente

# Etape 1 :

## Désignation obligatoire du DPD

- Désignation **obligatoire** du délégué à la protection des données, sans seuil de dispense.
- Cette fonction se situe au cœur de la conformité au règlement européen sur la protection des données (RGPD).

# Etape 1 :

## Les Missions du DPD Art. 39 §1 RGPD

- **Inform**er et **conseiller** le responsable de traitement (MAIRE) , le ou les sous-traitants (éditeurs de logiciels...) et agents,
- **Recenser** les différents traitements de données personnelles,
- **Identifier et prioriser** les actions à mener,
- **Conseiller** la collectivité sur la réalisation d'une analyse d'impact en cas de traitement à risque,
- **Mettre en place des procédures internes** pour garantir la protection des données,
- **Coopérer** avec la CNIL.

# Etape 1 :

## Responsabilité du DPD

- Pas de transfert possible de la responsabilité incombant au responsable de traitement ou au sous-traitant au profit du DPD,
- Il ne peut être tenu responsable en cas de non respect des dispositions du RGPD,

# Etape 1 :

## Attention au conflit d'intérêts !

- Appréciation de l'existence éventuelle d'un conflit d'intérêts étudiée au cas par cas.
- **Exemple** : on ne peut pas être à la fois DPD et :
  - élu dans la collectivité (maire, adjoint, conseillers municipaux),
  - DGS, directeur financier, secrétaire générale,
  - responsable du service informatique ,
  - Etc...
- Un DPD ne peut être « juge et partie » : il ne peut occuper une fonction ou un rôle au sein de la collectivité qui le conduit à déterminer les finalités et les moyens du traitement de données.

# Etape 1 :

## Désignation du DPD

- Plusieurs solutions possibles :
  - **Interne** avec les contraintes énoncées précédemment.
  - **Externe** : prestataires extérieurs tels que les éditeurs, cabinet d'avocat...
  - **Mutualisation du DPD : l'Association des Maires et des Elus Locaux du Tarn devient DPD mutualisé**

# Les différentes obligations de mise en conformité

- **Etape 1 :**
  - Désigner obligatoirement un Délégué à la Protection des Données
- **Etape 2 :**
  - Réaliser un registre de traitements
- **Etape 3 :**
  - Prioriser et mettre à jour les procédures
- **Etape 4 :**
  - Réaliser des analyses d'impacts et analyses de risques
- **Etape 5 :**
  - Assurer et prouver la conformité permanente

# RGPD

## PASSER À L'ACTION

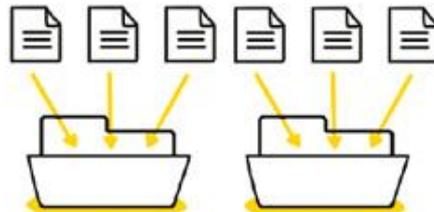
en 4 étapes

1



Constituez un registre  
de vos traitements de données

2



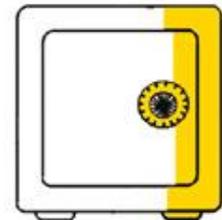
Faites le tri  
dans vos données

3



Respectez les droits  
des personnes

4



Sécurisez  
vos données

## Etape 2 :

# Réaliser un registre de traitements

- **Outil obligatoire et central pour la conformité,**
- 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 faudra aussi le faire vivre dans le temps en fonction des divers changement de traitements de données :**  
ajout de traitements, suppression, modification...



Constituez un registre  
de vos traitements de données

# Etape 2 : Réaliser un registre de traitements

- Le registre de traitements va venir en remplacement des formalités CNIL : déclaration simplifiée,...

**CNIL**  
 3, rue de Valenciennes - 92000 Nanterre  
 Tél : 01 41 39 71 00  
 www.cnil.fr

Ce formulaire est à retourner à la CNIL  
 N° d'enregistrement

**DÉCLARATION SIMPLIFIÉE**  
 ENGAGEMENT DE CONFORMITÉ

**1 Déclaration**

Vous êtes un organisme personnel  
 Vous êtes une personne physique

Nom et prénom ou raison sociale\* N° SIRET\*  
 Service N° SIRET\*  
 Adresse\* N° SIRET\*  
 Code postal\* Ville\* N° SIRET\*  
 Adresse électronique\* N° SIRET\*  
 Téléphone\*  
 Fax

Revenez à consulter au sein de l'organisme déclarant ou un complément d'information sur les données.

Non et prénom\*  
 Adresse électronique\*

**2 Liste de référence\***

Vous déclarez par le présent que votre traitement est strictement conforme aux règles décrites dans la liste de référence. Veuillez sélectionner la case correspondant à votre situation (vous n'êtes autorisé qu'à sélectionner la ou les références de base).

Nature de base	N° de référence				
<input type="checkbox"/> Aucune base	ND	ND	ND	ND	ND
<input type="checkbox"/> Autorisation unique	AU	AU	AU	AU	AU
<input type="checkbox"/> Acte réglementaire unique	RU	RU	RU	RU	RU
<input type="checkbox"/> Méthodologie de référence	MR	MR	MR	MR	MR
<input type="checkbox"/> Autorisation unique - RCJ	RCJ	RCJ	RCJ	RCJ	RCJ

**3 Exercices de données liés de l'Union Européenne\***

Vous déclarez que les parties des données personnelles dans votre traitement sont ingérées dans une ou plusieurs données de base de données de la page web de l'Union Européenne.

Non  Oui

**4 Signature**

Revenez à consulter au sein de l'organisme déclarant

Non et prénom\* Date\*  
 Fonction Signature  
 Adresse électronique\*

Le déclarant s'engage par le présent à respecter les obligations décrites à l'article 17 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (la Loi) et à respecter les obligations décrites à l'article 29 de la Directive n° 95/46/CE du 24 octobre 1995 relative à la protection des données à caractère personnel (la Directive). Le déclarant s'engage également à respecter les obligations décrites à l'article 17 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (la Loi) et à respecter les obligations décrites à l'article 29 de la Directive n° 95/46/CE du 24 octobre 1995 relative à la protection des données à caractère personnel (la Directive).

**CNIL**  
 3, rue de Valenciennes - 92000 Nanterre  
 Tél : 01 41 39 71 00  
 www.cnil.fr

Ce formulaire est à retourner à la CNIL  
 N° d'enregistrement

**DÉCLARATION NORMALE**  
 (Article 17 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

**1 Déclaration**

Vous êtes un organisme personnel  
 Vous êtes une personne physique

Non et prénom ou raison sociale\* N° SIRET\*  
 Service N° SIRET\*  
 Adresse\* N° SIRET\*  
 Code postal\* Ville\* N° SIRET\*  
 Adresse électronique\* N° SIRET\*  
 Téléphone\*  
 Fax

Revenez à consulter au sein de l'organisme déclarant ou un complément d'information sur les données et procédures de traitement.

Non et prénom\*  
 Adresse électronique\*

**3 Service chargé de la mise en œuvre du traitement (Sous d'implémentation)**

Indiquez ici le service qui est chargé de la mise en œuvre du traitement (Sous d'implémentation).

Le traitement est assuré par un tiers personnel, juridique ou un service externe du déclarant, veuillez compléter la section ci-dessous.

Non et prénom ou raison sociale\* N° SIRET\*  
 Service N° SIRET\*  
 Adresse\* N° SIRET\*  
 Code postal\* Ville\* N° SIRET\*  
 Adresse électronique\* N° SIRET\*  
 Téléphone\*  
 Fax

**Ce formulaire est à retourner à la CNIL**  
 N° d'enregistrement

## Etape 2 :

# Réaliser un registre de traitements

- **Qui ?** DPD en collaboration avec le référent désigné par la collectivité
- **Quand ?** dès que possible
  
- **Quelques exemples de traitements de données dans les mairies :**
  - Gestion de la paye,
  - Gestion des inscriptions des élèves :
    - Dans les écoles,
    - A la cantine,
    - Au Centre de Loisirs,
  - Gestion de la liste électorale
  - Gestion d'une mailing list
  - Vidéosurveillance
  
- **Comment ?**
  - Une première page avec les noms et coordonnées du responsable du traitement et du DPD,
  - Une fiche pour chaque traitement de données recensée

# Etape 2 : Réaliser un registre de traitements

## Fiche de traitement de données

- **Qui est en charge du traitement ?**
  - Nom et coordonnées du responsable de traitement et du DPD
  - Liste des sous-traitants
- **Qu'est ce qui est traité ?**
  - J'identifie les catégories de données traitées : nom , prénom, adresse,...
  - J'identifie les données sensibles entraînant des risques accrus
- **Pourquoi cela est traité?**
  - Je communique la ou les finalités pour laquelle ou lesquelles, je collecte et traite ces données (ex: gestion des RH,...)
- **Pendant quelle durée ces données seront conservées?**
  - Je précise les délais prévus pour l'effacement des différentes catégories de données
- **Comment cela est protégé?**
  - Je précise les mesures de sécurité mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc les impacts sur la vie privée
  - Je cible les données sensibles

<b>TRAITEMENT N°: 4</b> <b>Intitulé : Recensement citoyen</b> <b>Date d'inscription au registre : 01/2014</b> <b>Mise à jour (date et Objet) :</b>  <b>Nom du Responsable du Traitement : Maire de <span style="background-color: blue; color: white;">MELIGNY</span></b> <b>Lieu du Traitement Service Accueil Population Election</b>		<b>Formalités CNIL</b> Déclaration normale <input checked="" type="checkbox"/>	
<b>Applicatifs ou fichiers :</b>	Avenir - Logitud		
<b>Date de mise en œuvre :</b>	2000		
<b>Finalité principale du traitement :</b>	Recensement citoyen		
<b>Détail des finalités du traitement :</b>	Obligation légale pour les enfants atteignant l'âge de la majorité (Loi du 28/10/1997)		
<b>Fonctions des personnes ou service auprès duquel s'exerce le droit d'accès : (préciser leurs coordonnées)</b>	Service Accueil Population Election		
<b>Catégorie des personnes concernées par le Traitement :</b>	Jeunes atteignant l'âge de la majorité		
<b>Données traitées :</b>	<b>Catégories de données traitées</b>	<b>Détail des données traitées</b>	
	Identité, livret de famille, domicile	Nom, Prénom, adresse, filiation	
<b>Catégorie de destinataires habilités à recevoir communication des données :</b>	<b>Catégories de destinataires</b>	<b>Données concernées</b>	
	Transmission tous les trimestres au Bureau du Service National à Paris	Nom, Prénom, adresse, filiation	
<b>Durée de conservation des données :</b>	Aucune		
<b>Mesures de sécurité mises en place :</b>	Confidentialité de l'applicatif, sessions verrouillées		

<b>Traitement n°8</b>	<b>DPD 08 VŒUX Plus utilisé MAJ janv2017</b>	
<b>Nom et adresse du responsable du traitement :</b>	MAIRIE DE [REDACTED] HOTEL DE VILLE 10 RUE PHILIPPE MARCOMBES 63033 [REDACTED]	
<b>Date de mise en œuvre :</b>	2009	
<b>Finalité principale :</b>	Envoi des Vœux par mail	
<b>Détail des finalités du traitement</b>	Envoi de mails de vœux	
<b>Service chargé de la mise en œuvre</b>	Cabinet du Maire	
<b>Exercice du droit d'information et droit d'accès</b>	Cabinet du Maire Par voie postale ou sur place	
<b>Catégories de personnes concernées par le traitement</b>	Les internautes qui utiliseront	
<b>Données traitées</b>	<b>Catégories de données traitées</b>	<b>Détails des données traitées</b>
	Identité des personnes	Nom prénom adresse mail émetteur et destinataire Message vœux
<b>Catégories de destinataires</b>	<b>Catégories de destinataires</b>	<b>Données concernées</b>
	Services communaux habilités à le connaître	Nom prénom adresse mail émetteur et destinataire Message vœux
<b>Durée de conservation</b>	1 an	
<b>Mise à jour (date et objet):</b>	02/01/2009	

# Zoom sur la durée de conservation

- Qu'en est il des délais obligatoires et réglementaires de conservation des données (Paie, RH, compta,...) par rapport au droit d'effacement du RGPD ?
- Vidéo : <https://www.youtube.com/watch?v=OUMGp3HHeI4&t=128s>



# Les différentes obligations de mise en conformité

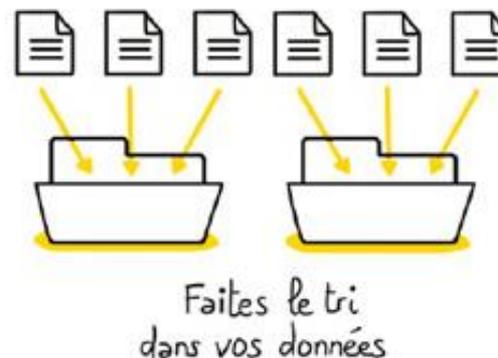
- **Etape 1 :**
  - Désigner obligatoirement un Délégué à la Protection des Données
- **Etape 2 :**
  - Réaliser un registre de traitements
- **Etape 3 :**
  - Prioriser et mettre à jour les procédures
- **Etape 4 :**
  - Réaliser des analyses d'impacts et analyses de risques
- **Etape 5 :**
  - Assurer et prouver la conformité permanente

## Etape 3 :

# Faire le tri dans les données

- **Qui** ? le référent en collaboration avec le DPD
- **Quand** ? après la constitution du registre
- Le tri dans les données permet de s'interroger sur celles dont la collectivité a réellement besoin.

**Exemple** : est-ce utile de conserver le listing des enfants d'un administré qui ont quitté l'école et qui sont majeurs?



## Etape 3 :

# Sécurisez les données

- **Qui** ? DPD en collaboration avec le référent désigné par la collectivité / service informatique
- **Quand** ? Suite à la constitution du registre
- **Sécuriser les données** : mise en place d'une politique de sécurisation, pour garantir un niveau de protection des données raisonnable en fonction de la sensibilité des données.
- **Mettre en place des procédures internes** qui prennent en compte des évènements qui pourraient survenir dans le vie du traitement : faille de sécurité, gestion de la demande de rectification, changement de prestataire...
- **Exemples** : mises à jour des antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement des données dans certaines situations.



Sécurisez  
vos données

## Etape 3 :

# Mise en place de procédures

- **Notification des violations** de données personnelles

- Auprès de la CNIL

Dans les meilleurs délais possibles et au plus tard 72h après avoir pris connaissance de la violation

**NB** : même obligation pour le sous-traitant, mais notification à faire au responsable de traitement.

- Auprès de la personne concernée par la violation des données,

Cette violation est susceptible d'engendrer un risque élevé pour ses droits et libertés (évaluer par le biais d'analyses d'impact si nécessaire) :

- Notification dans les meilleurs délais.
    - Si cela exige des efforts disproportionnés : communication publique ou autre mesure permettant aux personnes concernées d'être informées.

- **Création d'un registre des violations** des données

- **Révision des contrats si besoin et création du registre des sous-traitants**

## Etape 3 :

# Respectez les droits des personnes

- **Qui** ? DPD en collaboration avec le référent désigné par la collectivité
- **Quand** ? à la suite d'une demande d'un administré ou d'un salarié
- **Respectez les droits des personnes** en particulier ce qui nous autorise à traiter ces données : C'est à dire le « fondement juridique » : il peut s'agir du **consentement** de la personne, de l'exécution d'un contrat, du respect d'une obligation légale.
- **Exemple**: pourquoi détenez-vous mes coordonnées bancaires ?  
-> Afin d'effectuer le virement du salaire.



Respectez les droits  
des personnes

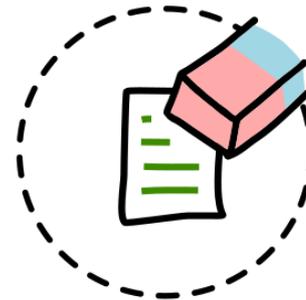
# RGPD : les droits de la personne



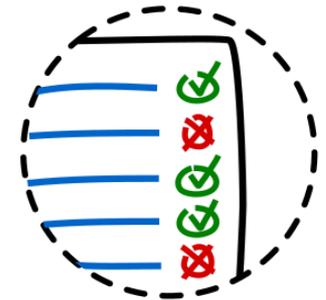
Accès



Rectification



Effacement



Limitation



Opposition



Portabilité



Réclamation



Actions

# Zoom droit d'accès

- **Quel est le délai raisonnable de réponse lorsqu'une demande est faite, par la personne concernée, sur le recueil de ses données personnelles ?**
- Idéalement dans les meilleurs délais, soit 1 mois maximum après réception de la demande.
- Une prolongation de 2 mois est possible uniquement si la personne en est informée et s'il est prouvé que la demande est complexe et nécessite un délai supplémentaire.

## Etape 3 :

# Récapitulatif

- **Collecter et traiter** seulement les données strictement nécessaires,
- **Vérifier les mesures de sécurité mises en place**
- **Réviser les mentions d'information**
- **Vérifier que les sous-traitants** connaissent leurs nouvelles obligations et leurs responsabilités  
<https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses>
- **Prévoir l'exercice des droits des personnes**
- **Mettre en place des règles de bonnes pratiques, charte informatique.**

# Les différentes obligations de mise en conformité

- **Etape 1 :**
  - Désigner obligatoirement un Délégué à la Protection des Données
- **Etape 2 :**
  - Réaliser un registre de traitements
- **Etape 3 :**
  - Prioriser et mettre à jour les procédures
- **Etape 4 :**
  - Réaliser des analyses d'impacts et analyses de risques
- **Etape 5 :**
  - Assurer et prouver la conformité permanente

# Étape 4 :

## Analyses d'impact relatives à la protection des données : DPIA

**Principe de privacy by design** (protection de la vie privée dès la conception du traitement)

- **Par qui ?**

Le responsable de traitement avec l'aide du DPD.

- **Quand ?**

L'analyse d'impact est obligatoire lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

### **Quelles conséquences ?**

Si l'analyse d'impact révèle l'existence d'un risque élevé, il convient de consulter la CNIL.

## Etape 4 :

# Analyses d'impact relatives à la protection des données

- Un traitement devra faire l'objet d'un DPIA quand il est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes. Il sera également obligatoire lorsqu'il remplira l'un des 2 critères suivants :
  - Evaluation (profilage, scoring...) ;
  - Basé sur une décision purement automatique pouvant entraîner des effets juridiques ;
  - Surveillance à grande échelle et systématique (une entreprise qui surveille ses salariés) ;
  - Manipulation de données sensibles\* ;
  - Collecte de données sur une cible très large
  - Croisement de données ;
  - Traitement portant sur des personnes fragiles ou vulnérables (enfants, malades...) ;
  - Traitement utilisant une nouvelle technologie ;
  - Traitement aboutissant à l'exclusion du bénéfice d'un droit ou d'un contrat ;

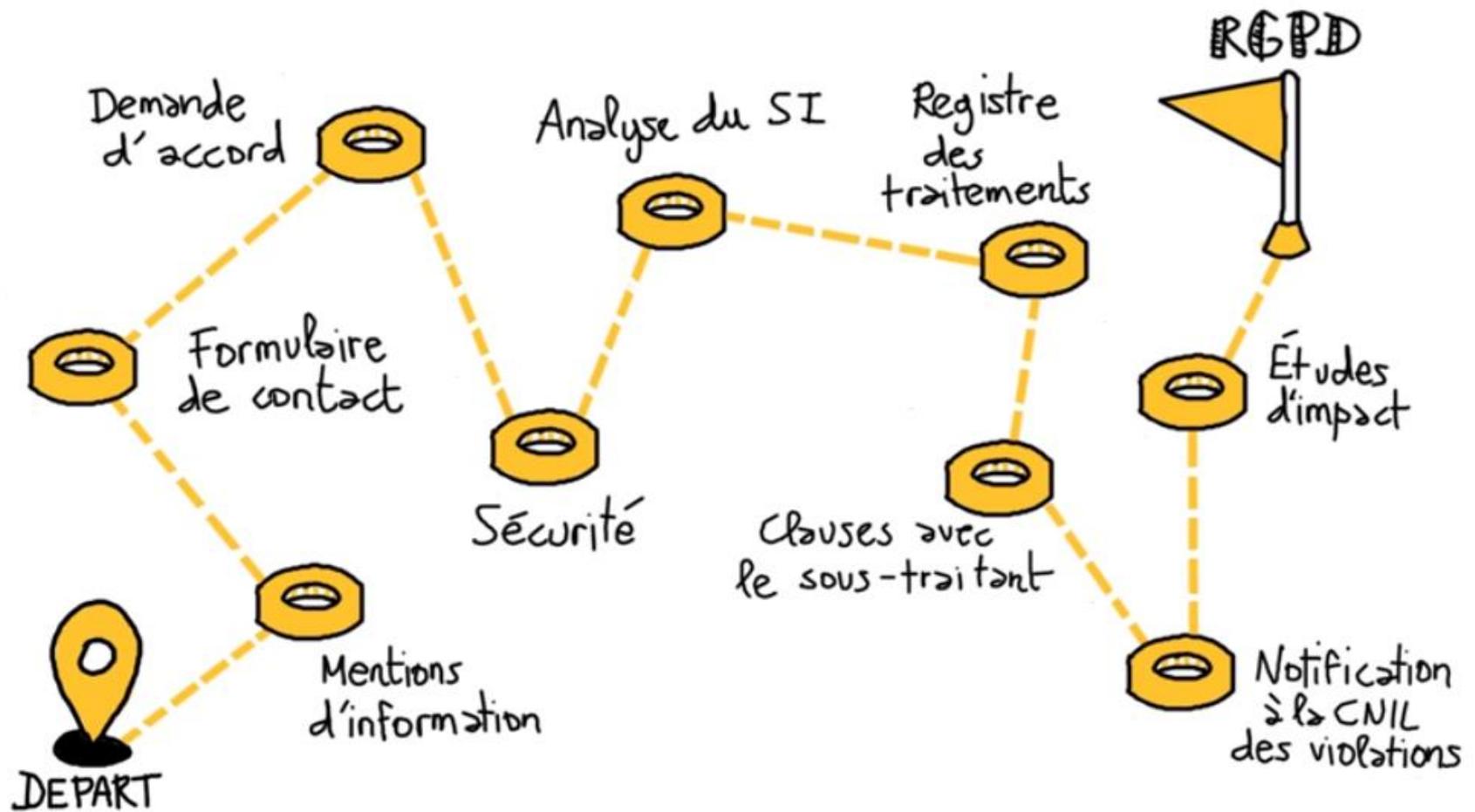
# Les différentes obligations de mise en conformité

- **Etape 1 :**
  - Désigner obligatoirement un Délégué à la Protection des Données
- **Etape 2 :**
  - Réaliser un registre de traitements
- **Etape 3 :**
  - Prioriser et mettre à jour les procédures
- **Etape 4 :**
  - Réaliser des analyses d'impacts et analyses de risques
- **Etape 5 :**
  - Assurer et prouver la conformité permanente

## **Etape 5 :**

# **Assurer et prouver le conformité permanente**

- Principe d'accountability (nécessité de rendre compte).
- Nécessité de pouvoir prouver à tout moment son implication dans la protection de données personnelles, en cas de contrôle de la CNIL par exemple.
- Documentation systématique des actions et décisions au regard du RGPD :
  - Le registre de traitements à jour,
  - Le registre des sous-traitants,
  - Le registre des notifications de violations des données.



- Vidéo : <https://www.youtube.com/watch?v=OUMGp3HHeI4&t=128s>

# Les différentes obligations de mise en conformité

- **Etape 1 :**
  - Désigner obligatoirement un Délégué à la Protection des Données
- **Etape 2 :**
  - Réaliser un registre de traitements
- **Etape 3 :**
  - Prioriser et mettre à jour les procédures
- **Etape 4 :**
  - Réaliser des analyses d'impacts et analyses de risques
- **Etape 5 :**
  - Assurer et prouver la conformité permanente

# Qu'est ce qu'un dossier conforme ?

- Pour **prouver votre conformité au RGPD**, vous devez constituer et regrouper **plusieurs documents, qui devront être actualisés régulièrement**.  
Quels sont ces documents ?
- **la documentation sur les traitements et la sécurité des données :**
  - le registre de traitements, des sous-traitants et de violations
  - les analyses d'impacts (PIA)
- **Les documents relatifs à l'information des personnes concernées par vos fichiers.**
  - les mentions d'information
  - les modèles de recueil de consentement
  - les procédures d'exercice des droits
- **les pièces définissant les rôles et les responsabilités**
  - les contrats avec les sous-traitants
  - les procédures en cas de violation des données
  - la preuve du consentement des personnes



# A l'avenir je me pose les questions suivantes

RÉFLEXE

1

PERTINENCE

## NE COLLECTEZ QUE LES DONNÉES VRAIMENT NÉCESSAIRES

Posez-vous les bonnes questions : Quel est mon objectif ? Quelles données sont indispensables pour atteindre cet objectif ? Ai-je le droit de collecter ces données ? Est-ce pertinent ? Les personnes concernées sont-elles d'accord ?

RÉFLEXE

2

TRANSPARENCE

## SOYEZ TRANSPARENT

Une information claire et complète constitue le socle du contrat de confiance qui vous lie avec les personnes dont vous traitez les données.

**RÉFLEXE**  
**3**  
RESPECT DES  
DROITS

**PENSEZ AUX DROITS DES PERSONNES**

Vous devez répondre dans les meilleurs délais, aux demandes de consultation, de rectification ou de suppression des données.

**RÉFLEXE**  
**4**  
MAÎTRISE

**GARDEZ LA MAÎTRISE DES DONNÉES**

Le partage et la circulation des données personnelles doivent être encadrés et contractualisés, afin de leur assurer une protection à tout moment.

**RÉFLEXE**  
**5**  
GESTION DES  
RISQUES

**IDENTIFIEZ LES RISQUES**

Vous traitez énormément de données, ou bien des données sensibles ou avez des activités ayant des conséquences particulières pour les personnes, des mesures spécifiques peuvent s'appliquer.

**RÉFLEXE**  
**6**  
SÉCURITÉ

**SÉCURISEZ VOS DONNÉES**

Les mesures de sécurité, informatique mais aussi physique, doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident.

# Service DPD mutualisé de l'Association des Maires et des Elus Locaux du Tarn

L'Association des Maires et des Elus Locaux du Tarn vous propose la mise à disposition un DPD pour vous accompagner dans votre mise en conformité.

**Le service sera proposé par les membres du Pôle numérique.**

## ▶ **Experts**

Il est entouré d'une équipe pluridisciplinaire dans les domaines juridique, informatique et d'archivage.

## ▶ **Indépendant**

L'externalisation de la fonction de DPD est une manière à la fois de garantir l'indépendance du délégué par rapport à une désignation en interne, de réduire les coûts et de permettre à toutes les collectivités, quelle que soit leur taille, d'en être dotées. L'absence de conflits d'intérêt dans l'exécution de ses missions garantit son indépendance.

C'est aussi un moyen pour se **mettre en conformité** avec la loi.

## ▶ **« En réseau »**

Dans le domaine de la protection des données, l'Association des Maires et des Elus Locaux du Tarn coopère et participe à différents réseaux de partenaires qui favorisent l'échange de pratiques et d'expériences.

## ▶ **Un service de proximité : joignable**

Avec une équipe pluridisciplinaire, le DPD sera joignable à tout moment par les personnes concernées : responsable de traitement, CNIL,...

# Service DPD mutualisé de l'Association des Maires et des Elus Locaux du Tarn

- **Un plan d'action** annuel adapté à votre collectivité vous sera proposé
- Plusieurs rencontres dans la collectivité seront organisées
- **Il est nécessaire et indispensable de désigner**, au sein de la collectivité, **une personne qui fera office de contact principal avec le service DPD mutualisé.**
- Pour désigner l'Association des Maires et des Elus Locaux du Tarn comme votre DPD :
  - prendre une délibération
  - signer une convention
  - faire la désignation sur le site de la CNIL
- Sur demande nous vous enverrons les modèles

# Les missions du DPD mutualisé

- **1/ Phase initiale**

- **Partie administrative**

- Rencontres / réunions d'information sur le RGPD
- Formalités administratives : désignation du DPD, notifications aux agents et aux instances représentatives du personnel
- Inventaire des traitements de données personnelles
- Constitution d'un registre de traitement
- Recommandations, informations
- Mise en place de procédures internes et de documentation

- 

- **Partie technique**

- Sécurité informatique
- Analyse de risque sur les données les plus sensibles

- 

- **2/ Phase de suivi et de veille**

- Gestion et suivi des recommandations et préconisations
- Mise à jour du registre
- Veille juridique sur le traitement des données personnelles
- Rencontres avec le responsable du traitement et/ou la personne désignée au sein de la collectivité

# Proposition tarifaire de l'Association des Maires et des Elus Locaux du Tarn

L'Association des Maires et des Elus Locaux du Tarn propose un accompagnement sur 3 ans renouvelable, avec :

- **phase initiale** : audit, recensement des données,...
- **phase de suivi**, de veille, de mise à jour des registres,...

Communes	Prix première année	Prix par an années suivantes
0 à 249 habitants	180 €	126 €
250 à 499 habitants	220 €	154 €
500 à 1499 habitants	280 €	196 €
1500 à 3499 habitants	380 €	266 €
3500 à 4999 habitants	500 €	350 €
5000 à 9999 habitants	650 €	455 €
10000 à 19999 habitants	850 €	595 €
Au-delà de 20000 habitants	1 200 €	840 €
Forfaits	Prix première année	Prix par an années suivantes
Communauté d'agglomération	1 500 €	1 050 €
Communauté de communes	1 200 €	840 €
Autres structures, sur devis	à partir de 200 €	à partir de 140 €

# Contacts

- **DPD mutualisé** : [dpd@maires81.asso.fr](mailto:dpd@maires81.asso.fr)
- **Pôle numérique** :
  - Camille Tardez : 05 63 60 16 32
  - Patricia Rabion : 05 63 60 16 47
- **Service juridique** :
  - Aurélie Ragaru : 05 63 60 16 38

**Merci**  
**de votre attention**

