AGATE
AGENCE ALPINE DES TERRITOIRES

# LE REGLEMENT EUROPEEN GENERAL SUR LA PROTECTION DES DONNEES PERSONNELLES (RGPD)

*Une matinée pour comprendre son impact et préparer son entrée en vigueur*

Les Marches – 27 février 2018

# Introduction : Pourquoi une nouvelle réglementation sur la protection des données personnelles ?

1. Comprendre les notions essentielles

2. Origine et évolution de la réglementation : le changement de concept introduit par le RGDP par rapport à la Loi Informatique et Libertés

3. Les principes posés par le RGPD

4. Comment mettre en œuvre le RGPD ?



AGATE
AGENCE ALPINE DES TERRITOIRES

# INTRODUCTION :

## Pourquoi une nouvelle réglementation sur la protection des données personnelles ?

**<u>Deux concepts liés et qui s'opposent</u>**

- **OPEN DATA** = Mise à disposition de données gratuites

- **BIG DATA** = Utilisation de ces données à titre commercial.

# Pourquoi une nouvelle réglementation sur la protection des données personnelles ?

- « Si c'est gratuit, c'est moi le produit… »






- Le volume de données double tous les 18 mois
- De 12 (actuellement) à 50 milliards d'objets connectés en 2020.



AGATE
AGENCE ALPINE DES TERRITOIRES

# Pourquoi une nouvelle réglementation sur la protection des données personnelles ?

## Histoire :

- 1978 : **Loi Informatique et Libertés :** accès aux documents administratifs et réutilisation des données publiques

- 2010 : **Directive INSPIRE** : favoriser la protection de l'environnement (publication de données géographiques…)

- 2013 : **Charte internationale au G8 de l'OPEN DATA**
  - faire de l'open data la pratique par défaut des administrations (tout en respectant la vie privée)
  - fournir des données de qualité, accessibles, comparables
  - améliorer la gouvernance et encourager la participation citoyenne
  - favoriser le développement inclusif et l'innovation

- 2015 : **Loi Valtère** : gratuité des données publiques

- Oct 2016 : **Loi pour une république numérique, (collectivités + 3500 h) 3 volets :**
  - **ouverture des données publiques** (qui présentent un intérêt économique, social, sanitaire ou environnemental)

  => mise en place de l'OPEN DATA
  - protection des citoyens dans la société numérique (droit à l'oubli…)
  - l'accès au numérique pour tous (couverture mobile, très haut débit, handicap…).



AGATE
AGENCE ALPINE DES TERRITOIRES

# Pourquoi une nouvelle réglementation sur la protection des données personnelles ?

**Paradoxe de l'Open Data :**

- le bénéficiaire n'est pas le payeur => Incitations financières des pouvoirs publics pour que les collectivités locales trouvent leur compte dans l'Open Data ?

  Par exemple, la gestion du trafic routier, la prévention des risques naturels, la mesure de la pollution atmosphérique ou de l'efficacité énergétique des bâtiments des offices publics d'aménagement et de construction…

=> Toutes ces applications qui participent de la définition des smart cities, sont autant de cas d'usage de l'internet des objets et qui relèvent de la compétence des collectivités locales.

# Pourquoi une nouvelle réglementation sur la protection des données personnelles ?

**Quel intérêt pour les données collectées ?**

- L'Open Data représenterait entre 0,5 et 1,5 point de PIB en gains estimés directs ou indirects (Source : Etalab, 2010)
- 21 000 jeux de données sont recensés sur la plate-forme d'Etalab
- 1 400 réutilisations partagées sur cette plate-forme
- 12 000 inscrits qui les utilisent quotidiennement.

⇒ Pourquoi pas au bénéfice des collectivités ? Création de partenariats pour créer des couches de valeurs aux données brutes, revendables ensuite sur des places de marché ?

⇒ Selon Gartner, 20 % d'entre elles généreront des recettes à partir de l'Open Data via des places de marché des données d'ici 2020.

# Pourquoi une nouvelle réglementation sur la protection des données personnelles ?

**Des exemples d'usages OPEN DATA/BIG DATA aux chiffres vertigineux :**

- Baisse de 250 Md€ sur la fraude fiscale et la collecte des impôts en Europe
- 700 Md€ de gains pour les consommateurs en pouvant géolocaliser ses achats à proximité = renfort de l'économie de proximité
- Santé : meilleures analyses, plus de tests, meilleure efficacité des traitements
- Banque assurance : produits ultra personnalisés.

=> 250 projets d'applications de start-up en France sur des données publiques pour fournir de nouveaux services aux usagers.

=> Attention : protection des données personnelles à ne pas oublier.

# 1ère PARTIE

# COMPRENDRE LES NOTIONS ESSENTIELLES


# Comprendre les notions essentielles : qu'est-ce qu'une donnée personnelle ?

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

Une donnée personnelle, c'est donc, au sens du RGPD, une information qui permet d'identifier une personne physique :

- directement : un nom, un prénom, la photo d'un visage, une vidéo montrant une personne, l'enregistrement d'une voix…

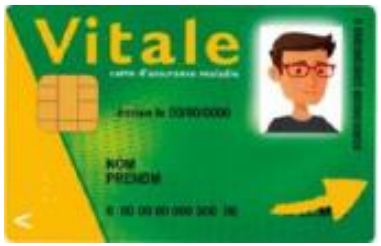
- indirectement : un numéro de sécurité sociale, un numéro de téléphone, une plaque d'immatriculation…




AGATE
AGENCE ALPINE DES TERRITOIRES

# Comprendre les notions essentielles : qu’est-ce qu’une donnée personnelle sensible ?

C'est une information qui révèle les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle d’une personne physique.




La loi interdit de recueillir et d'utiliser ces données. Sauf dans certains cas précis.

*Article 9 du RGPD*.




AGATE
AGENCE ALPINE DES TERRITOIRES

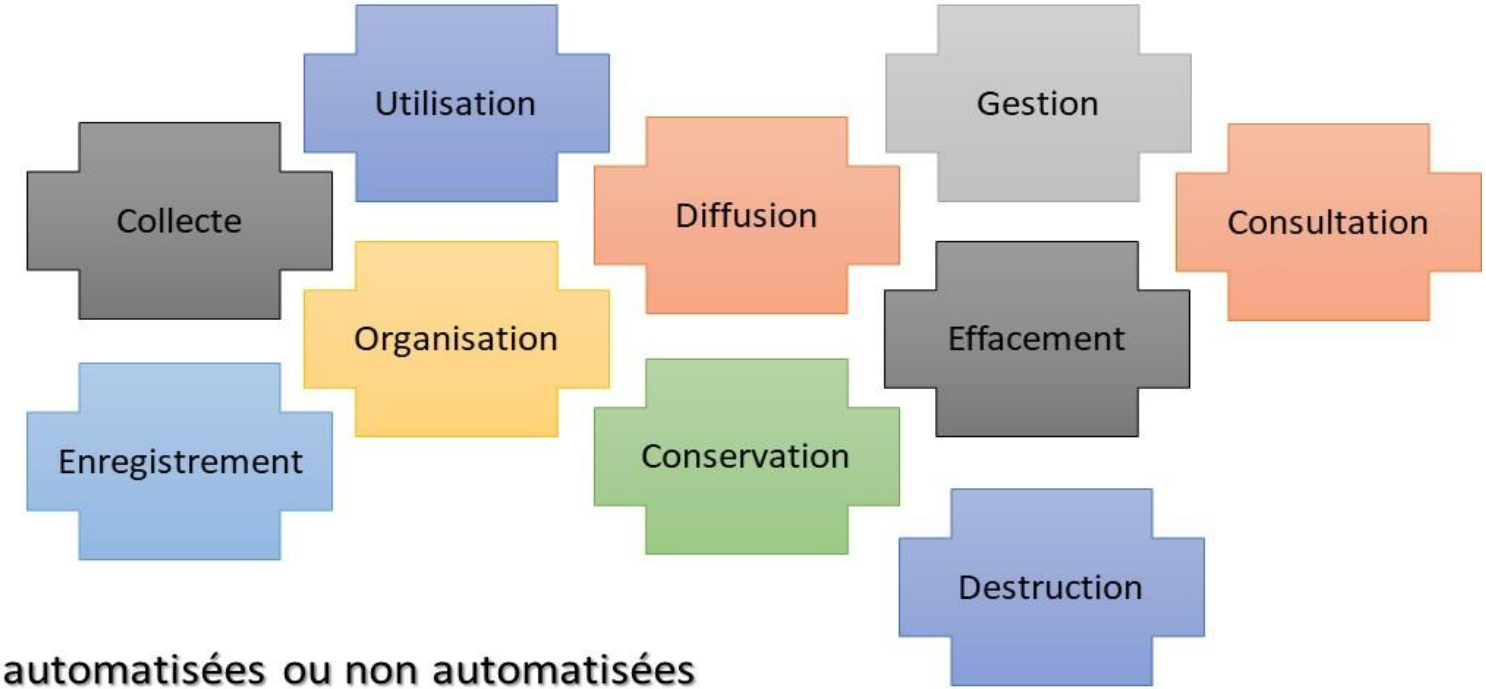
# Comprendre les notions essentielles : La protection des données est un droit fondamental

- Les données personnelles sont des composantes de la personnalité d'un individu.

- La protection des données personnelles est définie comme un droit fondamental.

# Qu’est-ce qu’un traitement de données ?


Ensemble d’opérations . . .




. . . automatisées ou non automatisées



AGATE
AGENCE ALPINE DES TERRITOIRES

# Comprendre les notions essentielles : qui est le responsable du traitement ?

C'est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme, seul ou responsable conjoint avec d'autres, ayant pour mission de déterminer les finalités et moyens du traitement.

➔ Il est responsable de la conformité du traitement avec le RGPD.

Il n'est pas :

➔ Le sous-traitant

➔ Le service chargé de mettre en œuvre le traitement.



AGATE
AGENCE ALPINE DES TERRITOIRES

# 2è PARTIE

## ORIGINE ET ÉVOLUTION DE LA RÉGLEMENTATION : LE CHANGEMENT DE CONCEPT INTRODUIT PAR LE RGPD PAR RAPPORT À LA LOI INFORMATIQUE ET LIBERTÉS

# Le changement de concept

| AVANT LE RGPD : | APRÈS LE RGPD : |
| --- | --- |
| RÉGIME DE DÉCLARATION / D'AUTORISATION PRÉALABLE AUPRÈS DE LA CNIL | OBLIGATION DE GOUVERNER VOS DONNÉES PERSONNELLES |
| OBLIGATION DE MAINTENIR LES DÉCLARATIONS / AUTORISATIONS À JOUR | LA CONFORMITÉ N'EST PAS UN ÉTAT, MAIS UN PROCESSUS |
| CONFORMITÉ STATIQUE | MAINTIEN PERMANENT ET DOCUMENTÉ DE LA CONFORMITÉ DE LA COLLECTIVITÉ AU RGPD. ILLUSTRATION : OBLIGATION DE TENIR UN REGISTRE DE TRAITEMENT |
| SANCTIONS EN CAS DE MANQUEMENTS PAR LA CNIL | SANCTIONS ÉVENTUELLES SI LA COLLECTIVITÉ N'EST PAS EN MESURE DE RAPPORTER LA PREUVE DOCUMENTÉE DE SA CONFORMITÉ.<br><br>ECHELLE DE SANCTION : 4 % DU CA MONDIAL OU 20 M€. |



AGATE
AGENCE ALPINE DES TERRITOIRES

# 3è PARTIE

## LES PRINCIPES POSÉS PAR LE RGPD

# Les principes posés par le RGPD

- Licéité et transparence
- Limitation des finalités et minimisation des traitements
- Temporalité
- Sécurité
- Coresponsabilité des sous-traitants.



AGATE
AGENCE ALPINE DES TERRITOIRES

# Les principes posés par le RGPD :
# Licéité et loyauté

Tout traitement doit être permis par la loi et recueillir le consentement de la personnes concernée.

- Accord libre, spécifique, éclairé et univoque (et révocable).



AGATE
AGENCE ALPINE DES TERRITOIRES

# Les principes posés par le RGPD :

# la transparence

Les personnes concernées doivent recevoir une information poussée sur les données collectées, chaque finalité poursuivie, et les droits dont elles disposent.

Le droit :

- d'accéder aux données collectées,
- de rectifier les données collectées,
- à l'oubli,
- à la portabilité,
- à la limitation et à l'opposition du traitement.



AGATE
AGENCE ALPINE DES TERRITOIRES

# Les principes posés par le RGPD : Proportionnalité et minimisation des traitements

Une donnée personnelle ne peut être collectée et traitée que pour réaliser une finalité précise.

Seules les données adéquates, pertinentes et limitées pour parvenir à une finalité définie doivent être collectées et traitées.



AGATE
AGENCE ALPINE DES TERRITOIRES

# Les principes posés par le RGPD :

# temporalité

Les données doivent être exactes, précises et actuelles, donc tenues à jour.

Les données personnelles ne peuvent pas être conservées indéfiniment.

Lorsqu'elles ne sont plus utiles, elles doivent être supprimées.

La durée de la conservation est :

- déterminée par le responsable du traitement selon la finalité,
- fixée par la loi dans certains cas.



AGATE
AGENCE ALPINE DES TERRITOIRES

# Les principes posés par le RGPD : sécurité

Tout responsable de traitement doit garantir, par des dispositifs et des procédures de sécurité, l'intégrité (perte, destruction ou dégâts) et la confidentialité des données personnelles.

Exemples :

- moyens permettant de garantir la confidentialité (pseudonymisation, chiffrement, verrouillage),
- moyens permettant de rétablir la disponibilité en cas d'incident,
- procédures permettant d'évaluer l'efficacité des mesures de sécurité,
- référentiels de sécurité : code de bonne conduite, labels, certificats…

# Les principes posés par le RGPD :

# La responsabilité du sous-traitant

Le responsable du traitement est celui qui définit les catégories de données collectées, les finalités et les moyens de mise en œuvre du traitement.

Il doit s'assurer qu'il recourt à des services, des plates-formes et des systèmes conformes aux exigences de la réglementation et **les prestataires qui sont ses sous-traitants lui sont redevables de cette conformité**.

Le sous-traitant doit fournir des services conformes et assister son client : la conformité est le fruit de leur coopération.



AGATE
AGENCE ALPINE DES TERRITOIRES

# 4è PARTIE

## COMMENT METTRE EN ŒUVRE LE RGPD ?

# Comment mettre en œuvre le RGPD ?

Les six étapes préconisées par la CNIL pour se préparer :

1. Désigner un pilote
2. Cartographier vos traitements de données personnelles
3. Prioriser les actions à mener
4. Gérer les risques
5. Organiser les processus internes
6. Documenter la conformité

# Comment mettre en œuvre le RGPD ?

## 1. Désigner un pilote : le Délégué à la protection des données (DPO ou DPD)

**Quelles sont les principales missions du DPO ?**

- Informer et conseiller le responsable de traitement de la collectivité ou le sous-traitant, ainsi que les agents
- Diffuser une culture Informatique & Libertés au sein de la collectivité
- Contrôler le respect du règlement et du droit national en matière de protection des données, via la réalisation d'audits en particulier
- Conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et en vérifier l'exécution
- Coopérer avec la CNIL et être le point de contact de celle-ci.

# Comment mettre en œuvre le RGPD ?

## 2. Cartographier vos traitements de données personnelles

Recenser de façon précise tous traitements de données personnelles que vous mettez en œuvre (a).

Le registre des traitements centralise les informations recensées (b).



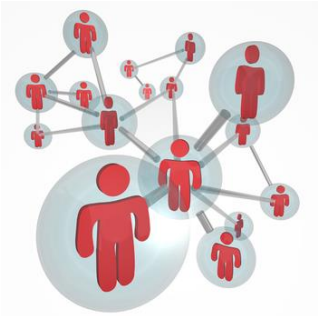
AGATE
AGENCE ALPINE DES TERRITOIRES

# Comment mettre en œuvre le RGPD ?

## 2. Cartographier vos traitements de données personnelles

### a) Le recensement des traitements de données personnelles :

**Qui ?** Le nom des responsables de traitements, des responsables de services opérationnels traitant les données, la liste des sous-traitants



**Quoi ?** Les catégories de données traitées

**Pourquoi ?** Les finalités des collectes

**Où ?** Lieux d'hébergements

**Jusqu'à quand ?** Le temps légal de conservation

**Comment ?** Les mesures de sécurité pour minimiser les risques.

# Comment mettre en œuvre le RGPD ?

## b) Le registre des traitements

| | | | | | | |
|---|---|---|---|---|---|---|
| **DESCRIPTION DU TRAITEMENT** | | | | | | |
| NOM / SIGLE | | | | | | |
| DATE DE CRÉATION | | | | | | |
| MISE À JOUR | | | | | | |
| | | | | | | |
| **ACTEURS** | **NOM** | **ADRESSE** | **CP** | **VILLE** | **PAYS** | **TEL** |
| RESPONSABLE DU TRAITEMENT | | | | | | |
| DPD | | | | | | |
| REPRÉSENTANT | | | | | | |
| RESPONSABLE(S) CONJOINT(S) | | | | | | |
| | | | | | | |
| **FINALITÉ(S) DU TRAITEMENT EFFECTUÉ** | | | | | | |
| FINALITÉ PRINCIPALE | | | | | | |
| SOUS-FINALITÉ 1 | | | | | | |
| | | | | | | |
| **MESURES DE SÉCURITÉ** | | | | | | |
| MESURES DE SÉCURITÉ TECHNIQUES | | | | | | |
| MESURES DE SÉCURITÉ ORGANISATIONNELLES | | | | | | |
| | | | | | | |
| **CATÉGORIES DE DONNÉES PERSONNELLES CONCERNÉES** | **DESCRIPTION** | | | **DÉLAI D'EFFACEMENT** | | |
| ETAT CIVIL, IDENTITÉ, DONNÉES D'IDENTIFICATION, IMAGES… | | | | | | |
| VIE PERSONNELLE (HABITUDES DE VIE, SITUATION FAMILIALE, ETC.) | | | | | | |

# Comment mettre en œuvre le RGPD ?

## 3. Prioriser les actions à mener

Sur la base du registre et pour chacun des traitements recensés, vérifier le respect des principes posés par le RGPD :

- les données collectées sont-elles limitées au regard de la finalité du traitement ?
- les personnes concernées ont-elles donné leur consentement ? Sont-elles suffisamment informées ?
- vos sous-traitants respectent–ils ces principes ?

Si votre travail de vérification vous conduit à identifier le traitement de certains types de données (sensibles, traitements systématiques de données personnelles, transfert hors UE), une analyse d'impact sur la protection des données est vivement conseillée.

# Comment mettre en œuvre le RGPD ?

## 4. Gérer les risques

**Qu'est-ce qu'une analyse d'impact (PIA) sur la protection des données ?**

Une PIA est un outil d'évaluation pour construire des traitements de données respectueux de la vie privée et qui doit permettre de démontrer la conformité du traitement au RGPD.

**Que contient une analyse d'impact ?**

Un descriptif du traitement et de ses finalités, une évaluation de la proportionnalité au regard de ses finalités et une évaluation des risques pour les droits des personnes.

# Comment mettre en œuvre le RGPD ?

## 5. Organiser les processus internes

- Prendre en compte la protection des données dès la conception d'une application ou d'un traitement
- Sensibiliser et organiser la remontée d'informations
- Traiter les réclamations et les demandes des personnes concernées quant à l'exercice de leur droits
- Anticiper les violations de données.

# Comment mettre en œuvre le RGPD ?

## 6. Documenter la conformité

Pour prouver votre conformité au règlement en cas de contrôle notamment, vous devez constituer et regrouper la documentation nécessaire :

- la documentation sur vos traitements de données personnelles, dont le registre et les analyses d'impact
- la documentation sur l'information des personnes (mentions d'information, recueil de consentement, …)
- les contrats avec les sous-traitants.



AGATE
AGENCE ALPINE DES TERRITOIRES

# *Merci de votre attention !*

Contact : **Emmanuel PETIT**
Directeur du Pôle Gestion des collectivités

**AGATE**
Agence Alpine des Territoires
25 rue Jean Pellerin
73026 CHAMBERY
04 79 68 53 00
contact@agate-territoires.fr