e-Collectivités Vendée

Maison des Communes

# Protection des données, nouvelles obligations

# Rappels des définitions, grands principes et acteurs

# Rappels : Définitions

- Données à caractère personnel (**Art 4 ):**

Constitue une donnée à caractère personnel toute information se rapportant à une **personne physique identifiée ou identifiable** :

- **Directement** *ou*
- **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

- **Loi Informatique et Libertés (LIL) vs Règlement général pour la protection des données (RGPD) : définition élargie et plus précise par rapport à la LIL**


Capucine
3 kg - 50 cm
samedi
12 juillet 2008
05 h 45


CARTE POSTALE
CORRESPONDANCE
ADRESSE
London


ShanIPCalc
Calculateur de Masque
Calculateur de Sous-réseaux
Convertisseur
A Propos...
Entrer l'adresse IP :
192 168 10 10
Classe C
Masque de sous-réseau :
255 255 255 240
/28
Nombre de sous-réseaux :
16
Machines par sous-réseau :
14
Lister les sous-réseaux
Aide
Quitter

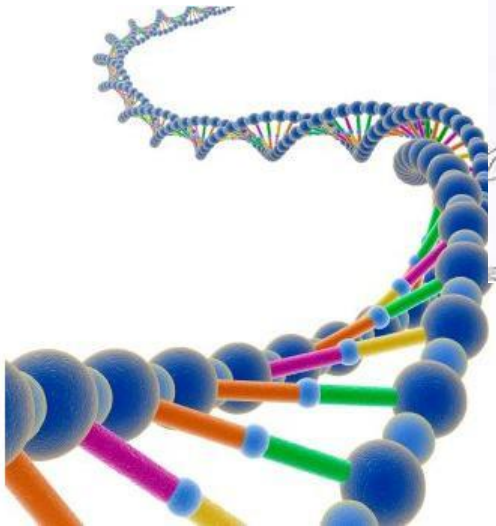

01 55 92 13 60


F
AB-
BRETAGNE
BREIZH
29
344-CA


carte d'assurance maladie
vitale
EMISE LE 08/01/2005
1 88 88 88 088 088 88
NNNNNNNNNNN
BBBBBBBBB


VISA
0123 4567 8901 2345
EXPIRE A FIN 02/02
123
CARTE BLEUE
MME ANNE DEMONCEAU


Perbieu
St Pierre




NETAG
Steve Carlsen
C.E.O. NETAG

# Rappels : Définitions

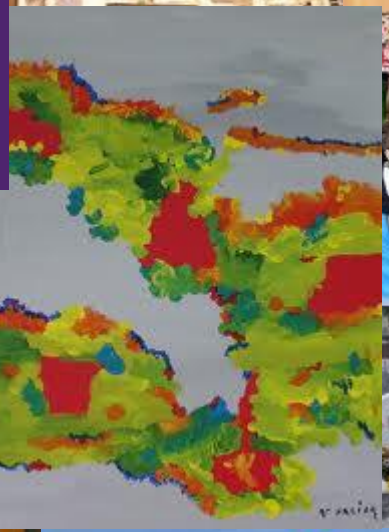
- Traitement **(Art 4)** :

Constitue un traitement de données à caractère personnel :

- 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

- **LIL vs RGPD : définition peu modifiée par rapport à la LIL**


RECENSEMENT DE LA POPULATION






# Rappels : Définitions

- Fichier :

Constitue un 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

# Rappels : Acteurs

- Le responsable du traitement (RT) :

  - Le·la maire
  - Le·la président·e de l'EPCI, du syndicat, du Conseil département ou du Conseil régional
  - Définition (Art 4):

    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.

  - La personne dont la responsabilité civile et pénale peut être engagée

- **Pas de changement dans la définition et la conception du responsable de traitement par rapport à la LIL**

# Rappels : Acteurs

- Le Correspondant Informatique et Libertés :
  - Diffuse la culture Informatique et Libertés
  - Instaure des bonnes pratiques
  - Est l'interlocuteur de la CNIL
  - Sensibilise les agents, la direction, les élus
  - Tient des registres de traitement et dresse un bilan annuel de ses activités
  - Désignation facultative pour la collectivité

- **Changement important avec le RGPD : disparition du CIL au profit du Délégué à la Protection des Données (DPD)**

# Rappels : Les grands principes de la collecte de données

- **Principe de finalité** : indiquer à quoi le fichier va servir.

Les données ne peuvent être recueillies que pour une finalité :

- Déterminée, explicite et légitime
- Correspondant aux missions de la collectivité

→ Autrement dit, ce principe limite la manière dont le responsable du traitement pourra utiliser ou réutiliser ces données dans le futur.

- **Principe de pertinence** : aussi appelé principe de proportionnalité ou de minimisation de la collecte.

Seules les données strictement nécessaires à la réalisation de l'objectif peuvent être collectées.

- **Principe de temporalité** : aussi appelé principe de conservation.

Une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu de conserver les données et elles doivent être supprimées.

# Les autres grands principes de la LIL

- Sécurité des fichiers

Obligation de prendre toutes les mesures nécessaires pour :

  - Garantir la sécurité des données collectées
  - Garantir leur confidentialité

Obligation d'adapter ces mesures en fonction des risques qui pèsent sur les données

- Information des personnes de leurs droits :

  - Droit d'accéder à ses données
  - Droit de les rectifier
  - Droit de s'opposer à leur utilisation

- Formalités préalables auprès de la CNIL

  - Déclaration normale
  - Demande d'autorisation
  - Demande d'avis
  - Simplifications

# Le Règlement général pour la protection des données

## (RGPD)

# Nouvelles obligations ?

- La Loi informatique et Libertés : en vigueur depuis le **6 janvier 1978**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Legifrance.gouv.fr
LE SERVICE PUBLIC DE LA DIFFUSION DU DROIT

**Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**
Version consolidée au 13 septembre 2017

- Le Règlement général sur la protection des données (RGPD) : en vigueur à partir du **25 mai 2018**.


*RGPD*
*aussi appelé GDPR en anglais*

# Le RGPD

- Un long processus :
  - 4 ans de négociation, 4 000 amendements, 88 pages
  - Adopté le 27 avril 2016
  - Publié au JOUE le 4 juin 2016
  - Entrée en application des dispositions : 25 mai 2018
- Constat :
  - Manque d'harmonisation entre les niveaux de protection au sein de l'UE
  - Évolution rapide des technologies
  - De plus en plus de données collectées
  - Nécessité de susciter ou maintenir la confiance
- Des renvois aux droits nationaux :
  - 56 cas où les États Membres gardent leur pouvoir , notamment :
    - santé, NIR, emploi,
    - exécution d'une mission d'intérêt publique ou exercice de l'autorité publique,
    - archivage, statistiques, recherche scientifiques, recherche historique
  - Loi informatique et libertés 2 en attente

## Ce qui change :

- Une nouvelle logique de responsabilité
- Les droits des personnes renforcés
- Un risque aggravé de sanctions
- Un Délégué à la Protection des Données (DPD) obligatoire

# Une nouvelle logique de responsabilité

- Réflexion sur la protection des données dès la création / conception d'un service : « Privacy by design » :

  - Dès la conception d'un service et par défaut
  - Mise en œuvre de mesures techniques et / organisationnelles
  - Veiller à limiter la quantité de données traitées

- Suppression des obligations de déclarations préalables pour les traitements sans risque pour la vie privée

  - Logique de responsabilisation des élu·e·s (RT)
  - Obligations de mettre en place des mesures de protection, de les documenter et de démontrer la conformité à tout moment (mise en conformité dynamique et permanente)
  - Maintien des déclarations préalables pour les demandes d'autorisation

# Une nouvelle logique de responsabilité

- Etudes d'impact sur la vie privée (EIVP) obligatoires :

  - pour les traitements « à risques », traitant des données sensibles ou reposant sur du profilage
  - pour faire apparaître les caractéristiques du traitement, les risques et les mesures adoptées pour protéger les données
  - Documentation CNIL sur les EIVP : ICI

*Aussi appelé « PIA » pour Privacy Impact Assessment en anglais*

- Partage des responsabilités : le sous-traitant aussi doit respecter le RGPD

  - Potentielle co-responsabilité
  - Obligation de désigner un DPD et de tenir un registre des traitements
  - Obligation de conseil pour permettre la conformité au RGPD (EIVP, failles de sécurité, audit, destruction des données)

# Les droits des personnes renforcés

- Obligation d'information dans des termes clairs

  - L'information doit être claire, intelligible et facilement accessible
  - Les personnes doivent donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer, de façon « non ambigüe »
  - La charge de la preuve pèse sur le responsable de traitement

- Obligation d'information en cas de perte de données :

  - Obligation d'informer la CNIL dans les 72 heures
  - Obligation d'informer les personnes concernées si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes
  - Droit à réparation du préjudice, auprès de l'élu·e (RT) ou de son sous-traitant

- Délais pour faire droit à une demande : « dans les meilleurs délais » et au plus tard en 1 mois

# Un risque aggravé de sanctions

- L'élu·e et le sous-traitant peuvent faire l'objet de sanctions administratives : jusqu'à 20 millions d'euros pour le responsable du traitement et de 2 à 4 % du chiffre d'affaires annuels du sous-traitant

- Des sanctions pénales toujours en vigueur :
  - Article L226-16 à L226-24 et articles R625-10 à R625-13 du code pénal
  - Peine d'amendes à peines de prison avec sursis

- En cas de non-conformité, le risque est ailleurs : réputation, image, perte de confiance, climat social

- Loi République numérique et loi Informatiques et Libertés 2 (à venir) pour adapter précisions en droit français
  - https://www.cnil.fr/fr/hertz-france-sanction-pecuniaire-pour-violation-de-donnees-personnelles

# Un délégué à la protection des données obligatoire

# Le délégué à la protection des données

- Désignation **obligatoire** du délégué à la protection des données, sans seuil de dispense.

- Profil :

  - Doit être qualifié : qualités professionnelles, connaissances spécialisées du droit et des pratiques en matière de protection de données
  - Doit bénéficier d'actions de formation continue

- Obligations pour la collectivité de :

  - fournir au DPD les ressources nécessaires à ses missions
  - l'associer d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données
  - lui donner accès aux données
  - lui permettre de se former

# Le délégué à la protection des données
## DPD *(ou DPO en anglais)*

- **Informer, conseiller et accompagner**, afin de faire respecter le règlement européen et le droit national dans sa collectivité
- **Sensibiliser** aux enjeux de la protection des données personnelles
- Superviser des **audits internes** sur la protection des données personnelles
- Conseiller le responsable sur l'opportunité de réaliser une analyse d'impact sur la vie privée (EIVP) et d'en vérifier l'exécution
- Recevoir les réclamations relatives à la protection des données et y répondre
- Coopérer avec la CNIL et être son point de contact dans la collectivité
- Tenir le registre des traitements et dresser le bilan annuel

→ **Missions élargies par rapport au CIL : plus grandes responsabilités !**

# CIL vs Délégué à la protection des données

2017

## Le CIL : Correspondant informatique et libertés

- Il diffuse la culture « Informatique et Libertés » et instaure des bonnes pratiques dans la collectivité.
- Il est l'interlocuteur de la CNIL au sein de la collectivité et veille au respect de la loi Informatique et Libertés. Il sensibilise les agents, la direction et les élus.
- Il tient des registres de traitement et dresse un bilan annuel de ses activités
- Sa désignation était facultative jusqu'à présent

2018

## Le DPD : Délégué à la Protection des Données ou Data Protection Officer (DPO)

- **Informer, conseiller et accompagner** au sein de sa structure, afin de faire respecter le règlement européen et le droit national en matière de protection des données personnelles
- **Sensibiliser** au sein de sa structure aux enjeux de la protection des données personnelles
- Superviser des **audits internes** sur la protection des données personnelles
- Conseiller le responsable sur l'opportunité de réaliser une **analyse d'impact sur la vie privée** (EIVP) et d'en vérifier l'exécution
- Recevoir les **réclamations** relatives à la protection des données et y répondre
- **Coopérer avec l'autorité de contrôle** (la CNIL) et être son point de contact au sein de sa structure

# Le délégué à la protection des données

- Possibilité de :

  - Externaliser un DPD : avocat, prestataire

  - **Mutualiser** un DPD : à l'échelle de l'EPCI, à l'échelle d'un département, etc.

    - Mutualiser pour éviter le conflit d'intérêt : DGS ≠ DPD
    - Mutualiser pour disposer
      - des ressources nécessaires
      - d'un DPD formé et habitué aux problématiques de protection des données
      - d'un DPD indépendant

  - Désigner le DPD dès maintenant avec prise d'effet au 25/05/2018 (pas de transfert automatique d'un statut à l'autre)

# La mise en conformité en 6 étapes

- Désigner un pilote
- Cartographier
- Prioriser
- Gérer les risques
- Organiser
- Documenter

# Documentation CNIL

- Règlement européen du 27 avril 2016 :
  - https://www.cnil.fr/fr/reglement-europeen-protection-donnees
- Règlement européen : se préparer en 6 étapes
  - https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes
  - https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf
- En quoi les collectivités territoriales sont-elles impactées par le règlement européen sur la protection des données ?
  - https://www.cnil.fr/fr/RGPD-quel-impact-pour-les-collectivites-territoriales
- Devenir délégué à la protection des données :
  - https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees
- Documenter la conformité :
  - https://www.cnil.fr/fr/documenter-la-conformite

# Documentation CNIL

- Modèle de registre règlement européen :
  https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx

- Etudes d'impact sur la vie privée (PIA en anglais) :
  - PIA-1, la méthode : Comment mener une étude d'impact sur la vie privée
  - PIA-2, l'outillage : Modèles et bases de connaissances de l'étude d'impact sur la vie privée
  - PIA-3, les bonnes pratiques : Mesures pour traiter les risques sur les libertés et la vie privée

- Le droit à la portabilité en question :
  - https://www.cnil.fr/fr/le-droit-la-portabilite-en-questions

# Glossaire

- CIL : correspondant informatique et libertés
- CNIL : commission informatique et libertés
- DPO : *data protection officier* = délégué à la protection des données en anglais
- EIVP : étude d'impact sur la vie privée
- EM : Etats membres de l'Union européenne
- LIL : loi informatique et libertés
- PIA : *privacy impact assessment* = étude d'impact sur la vie privée en anglais
- RGPD : règlement général à la protection des données
- RT : responsable du traitement