RGPD
Règlement Général sur la Protection des Données

CONTEXTE

Le RGPD (Règlement Général sur la Protection des Données) remplace la directive européenne de 1995.

Il complète la Loi Informatique et Libertés de 1978 modifiée, et a pour objectif d'homogénéiser les pratiques sur l'ensemble du territoire européen : Une même réglementation pour tous.

Il constitue le texte de référence en matière de **protection des données à caractère personnel**.

Toute entreprise ou administration doit être conforme à ce règlement européen dès lors qu'elle est établie sur le territoire européen ou qu'elle traite des données relatives à des européens.

ENJEUX

- Une Responsabilité accrue de l'administration (Responsable de traitement : Maire ou Président) qui doit être en mesure de prouver, à l'autorité de contrôle CNIL, que le Règlement a été respecté (depuis l'obtention du consentement de récolte des données jusqu'à la durée de conservation de ces données),

- améliorer l'efficacité : Le RGPD impose que les données collectées soient exactes et oblige la mise à jour des fichiers. La collecte doit correspondre au strict nécessaire et les durées de conservation des données respectées,

- accorder plus de droits aux personnes concernées : Droit d'accès, de rectification, de suppression, d'opposition, mais aussi un droit à une information claire et un consentement explicite,

- renforcer la confiance et redonner aux usagers le contrôle de ses données à caractère personnel : Les personnes dont on collecte les données doivent en être informées en toute connaissance de cause et doivent être assurées du respect de leur vie privée,
  Mettre en œuvre cette pratique permet de valoriser une image responsable de la collectivité.

- améliorer la sécurité des données : Protéger son patrimoine informationnel et protéger les personnes concernées des atteintes à leurs données,
  Cela minimise le risque d'avoir une fuite de données pouvant avoir des conséquences désastreuses tant au niveau juridique qu'au niveau de l'image de la collectivité.

- rassurer : Les usagers (citoyens, personnel, invités, lecteurs, enquêtés, patients, fournisseurs, prestataires ...) sont informés de l'usage qui est fait de leurs données. Le cas échéant, ils ont donné leur accord libre, explicite et éclairé.
  Chacun sait ce qui est fait de ses données, pour quelles raisons, par qui et pour quelle durée.

CONDITIONS

Pour chaque liste de contacts ou application de gestion des données, internes ou externes, auprès de qui sont envoyées des informations ou font l'objet d'un traitement (mailing-list, application, …), il est obligatoire d'informer les interlocuteurs de cet enregistrement et leurs préciser les éléments suivants :

- ✓ L'objet de la liste ou du traitement (sa finalité)
- ✓ Leur droit d'accès, de rectification, de suppression et d'opposition à leurs données personnelles.
- ✓ les coordonnées du Délégué à la Protection des Données de la collectivité.

PROCEDURE

1 – **Désigner un Délégué à la Protection des Données.**

Sa déclaration doit être exercée et validée auprès de la CNIL.
Sa mission est d'informer, conseiller et contrôler : Il audite et diagnostique le traitement de toutes les données à caractère personnel détenues par la collectivité pour en établir un registre. Il gère les demandes de rectification ou d'accès, les modifications de données personnelles collectées, les changements de prestataire…. Il décèle les failles de sécurité et déclare les fuites auprès de la CNIL. Il établit des plans d'action et le bilan annuel de gestion des données collectées par la collectivité.
Il est le contact de la CNIL auprès de qui il doit être en mesure de prouver la conformité et le suivi de l'application du Règlement.
Attention : le DPD ne peut être juge et partie de l'utilisation des données personnelles.
Cette mission peut être mutualisée ou externalisée.

2 – **Recenser les traitements de données de chaque service et élaborer un registre.**

Prioriser les actions à mener selon les risques que font peser les traitements sur les droits et libertés des personnes.
Le registre doit être placé sous la responsabilité du Responsable de traitement de la collectivité.

3 - **Adresser à chaque usager ou indiquer sur les imprimés de récolte une formule du type** :

*"Les informations recueillies sur ce formulaire papier ou électronique sont enregistrées dans un fichier informatisé par ……(nom de la collectivité) pour ……(Objet/finalité)**.***
Elles sont conservées pendant ……. (durée de conservation) et sont destinées …….. (gestionnaire(s) de traitement/service)
Conformément à la loi « informatique et libertés », vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier en contactant ……(coordonnées du DPD)".

Le traitement dématérialisé (site internet, réseau en ligne, …) devra également faire l'objet d'une mention ou formulaire du type :

"*INFORMATIONS PERSONNELLES, MODIFICATIONS ET DÉSABONNEMENT*
Seule la…… …… (collectivité) est destinataire des informations que vous nous communiquez. Elles sont destinées au traitement de …… et seront conservées pour une durée de …….. nécessaire au traitement.
Conformément à la loi Informatique et Libertés du 6 janvier 1978 modifiée, vous disposez d'un droit d'accès, d'opposition et de modification sur les données qui vous concernent. Pour l'exercer, contactez …… (coordonnées du DPD)".

A SAVOIR

A défaut d'application des règles du Règlement, des sanctions plus lourdes existent avec amendes pouvant aller jusqu'à 20 M d'euros.

Organe de contrôle : la CNIL

PRISE D'EFFET

Entrée en vigueur le 25 mai 2018

REFERENCES

Règlement n° 2016/679 du 27 avril 2016
Loi 78-17 du 6 janvier 1978, modifiée