Les élus et la protection des données à caractère personnel

FICHES PRATIQUES

2020

Centre de Gestion du Finistère
Prestation RGPD

Sensibilisation des élus au RGPD

Le Règlement général sur la protection des données est entré en vigueur le 25 mai 2018 au sein de tous les pays de l'Union Européenne.

Les services publics ont l'obligation de se mettre en conformité. Pour ce faire, ils doivent désigner un Délégué à la protection des données (DPD) qui réalisera un registre de traitements de données, des analyses d'impacts, des sensibilisations, des contrôles et qui apportera tous les conseils utiles dans le cadre de vos missions de service public.

« Ils n'ont en effet pas tous les mêmes moyens pour se conformer aux obligations découlant du RGPD : je pense aux communes de petite taille, qui peuvent d'ailleurs mutualiser la mission de délégué à la protection des données » Marie-Laure Denis, Présidente de la CNIL.

Le Maire/Président d'un EPCI est désigné comme le Responsable de traitement. Il a un rôle central puisqu'il est chargé de la gestion globale de l'application du RGPD dans sa collectivité. C'est sa responsabilité qui sera recherchée en cas de perte ou de vol et d'atteinte à la vie privée d'un usager.

En tant que Responsable de traitement, il lui incombe également de vérifier la conformité de ses sous-traitants via les marchés publics, les contrats et les avenants.

Pour toute information complémentaire, l'équipe est à votre disposition pour intervenir.

COMMISSION NATIONALE INFORMATIQUE ET LIBERTES (CNIL). ***Guide de sensibilisation au RGPD, pour les collectivités territoriales*****. [en ligne]. Paris. 2019, 43 p. Disponible sur : https://www.cnil.fr/sites/default/files/atoms/files/cnil-guide-collectivite-territoriale.pdf (consulté le 07/04/2020).**

L'accès aux documents, aux données

Occultation, anonymisation, minimisation

Les documents reçus et produits en mairie sont des documents administratifs communicables sous certaines conditions.

Ainsi, les documents qui contiennent des informations sur des personnes physiques ne peuvent être communiqués qu'aux intéressés ou à leurs mandataires afin de préserver le secret médical et le secret de la vie privée. Les informations qui révèlent le comportement d'une personne et dont la divulgation pourrait lui nuire ne peuvent pas être communiquées aux tiers.

En tant qu'élu, vous avez accès à un grand nombre de documents administratifs mais pas à ceux qui comportent des informations privées : jugement de divorce, taux du prélèvement à la sources des agents…

Votre agent responsable des Ressources Humaines saura vous conseiller dans le cas d'une demande d'accès d'un candidat ou d'un agent

Quelques bonnes pratiques :

- **L'accès au dossier complet agent est réservé aux gestionnaires RH.**
  Le service RH est là pour vous donner toutes les informations nécessaires.
- **Certaines mentions du bulletin de salaire d'un agent sont occultées avant communication.**
  Le NIR (numéro de sécurité sociale) mais aussi le taux du prélèvement à la source et d'autres informations sont strictement confidentielles.
- **Les *curriculums vitae* reçus restent en mairie.**
  Le RGPD introduit la notion de « porter préjudice » concernant les données personnelles, même si le candidat a fourni son CV, il n'a pas autorisé sa diffusion.
- **Les dossiers examinés en commission d'action sociale sont anonymisés.**
  La commission peut examiner une situation sans identifier la personne concernée.

L'utilisation des données

Limitation des données

« Chacun a droit au respect de sa vie privée. » *(Code civil, article 9 alinéa 1)*

Les collectivités traitent un nombre important de données à caractère personnel (fichier d'état civil, liste des enfants inscrits à la cantine, précisions sur les allergies alimentaires…)
Ces collectes de données sont souvent nécessaires pour remplir une mission de service public.
L'utilisation à d'autres fins est contraire aux principes fixés par le RGPD : un traitement = une finalité.

La confidentialité et le respect de la vie privée sont des principes à respecter en collectivité

Quelques bonnes pratiques :

- **Eviter l'utilisation du fichier d'état civil pour adresser des félicitations ou inviter aux vœux du Maire, ou extraire des données pour créer une liste d'enfants**
  Il y a d'autres fichiers utilisables comme la liste électorale ou d'autres moyens.
- **S'abstenir de demander la liste des adhérents d'une association**
  Si vous ne pouvez pas justifier de l'utilité de cette liste.
- **Vérifier que les tiers sont autorisés à accéder aux données**

Un "tiers autorisé" est un organisme qui peut accéder à certaines données contenues dans des fichiers publics ou privés parce qu'une loi l'y autorise expressément.

Quelques exemples de "tiers autorisés" :

L'administration fiscale, les organismes de sécurité sociale, dans le cadre de la lutte contre la fraude, les organismes en charge de l'instruction, du versement et du contrôle du RSA, les administrations de la justice, de la police et de la gendarmerie et les huissiers de justice.

La demande d'un tiers autorisé doit :

- Être écrite et préciser le texte législatif justifiant la demande.
- Viser des personnes nommément identifiées ou identifiables (le tiers autorisé ne peut pas avoir accès à l'intégralité d'un fichier).
- Être ponctuelle.
- Préciser les catégories de données auxquelles il souhaite accéder.

Sécurisation des données

Hygiène informatique et sécurité physique

La ville de Vannes a été victime d'un "ransomware", le 25 février 2016. Un agent de la collectivité avait ouvert une pièce jointe dans un mail, le virus s'est ainsi propagé sur tout le réseau. Les équipes de la direction informatique ont pu restaurer les fichiers sans avoir à payer la rançon.
La métropole de Marseille a été paralysée pendant plusieurs jours par des hackers qui demandaient une rançon.
Dans la nuit du 13 au 14 mars les serveurs de la ville ont subi de nombreuses attaques.
Les services sont ainsi bloqués pendant plusieurs mois, et un travail important est engagé avec des prestataires pour débloquer les systèmes.

L'agence national des systèmes d'information (ANSSI) met à disposition des guides simples à suivre : **GUIDE DES BONNES PRATIQUES DE L'INFORMATIQUE** avec ses 12 règles essentielles pour sécuriser vos équipements numériques.
Et pour aller plus loin : **GUIDE D'HYGIÈNE INFORMATIQUE**, renforcer la sécurité de son système d'information en 42 mesures.

Quelques bonnes pratiques :

- **Eviter de brancher son ordinateur privé au réseau de la collectivité**.
  Sauf si l'ordinateur présente un antivirus à jour, des mots de passe forts, et une habilitation pour accéder aux fichiers de la mairie.
- **Utiliser un mot de passe complexe sur tous ses outils bureautiques** (téléphone portable, ordinateur, tablette).
- **Stocker la clé de signature électronique dans un endroit sécurisé.**
- **Ne pas communiquer les mots de passe entre agents, entre élus et entre élus et agents.**
- **Différencier les outils privés des outils professionnels par des mots de passe différents**
  Vous limitez le risque de logiciels piratés.
- **Utiliser une adresse mail dédiée professionnelle.**
  Elle permet de garantir la continuité de service : une adresse de service (rh@ville.fr) et un alias mon.nom@ville.fr, deux adresses pour une seule boite de messagerie.
- **Bureau fermé à clé.**
- **Salle archives et salle serveur fermées à clé.**
- **Sauvegardes externes sous clé.**
  L'idéale est de faire 3 sauvegardes dont une hors du réseau et du bâtiment.
- **Gestion des autorisations et habilitations.**
- **Vérification périodique des procédures et systèmes.**
  Y compris pour les systèmes d'alarme.
- **Chiffrement de listes de noms, chiffrement des sauvegardes externes.**
  Pensez au chiffrement (cryptage) pour les transferts de fichiers, également par courriel.

La gestion des sous-traitants

Conseil, assistance, alerte, sécurisation

Les sous-traitants sont soumis à des obligations :

- **Une obligation de transparence et de traçabilité.**
  Il doit rédiger un contrat, respecter les instructions du responsable de traitement, informer sur une sous-traitance ultérieure, tenir un registre de traitement et le RT a la possibilité de l'auditer.

- **Privacy by design et prise en compte des principes du RGPD.**
  Garanties nécessaires dès leur conception, par défaut.

- **Sécurisation des données.**
  Confidentialité ; notification des violations de données, toutes les mesures nécessaires pour garantir la sécurité, au terme de la prestation : supprimer toutes les données ou les renvoyer au client, détruire les copies existantes sauf obligation légale de conservation.

- **Obligation d'assistance, d'alerte et de conseil.**
  Informer le RT que ses instructions violent le respect du RGPD, lorsqu'une personne exerce l'un de ses droits (accès, rectification…), aider le RT pour les violations de données et AIPD.

👍Quelques bonnes pratiques :

- **Revoir vos contrats avec vos sous-traitants.**
  Demander un avenant incluant les points RGPD.
- **Contractualiser avec votre prestataire informatique.**
  Vérifier l'existence d'un contrat.
- **Conventionner pour les transferts de données.**
  Revoir les conventions existantes souvent trop légères
- **Vérifier la conformité des prestataires au RGPD.**
  Demander leur registre des traitements de données à caractère personnel.

Parmi vos prestataires, ceux concernant vos sites internet seront à consulter en priorité car ils sont vos vitrines et facilement contrôlables par la CNIL (même à distance).

Si le cookie utilisé provient du serveur d'un tiers, ce dernier peut être qualifié de sous-traitant, car il traite « des données à caractère personnel pour le compte » et selon les instructions de l'éditeur (article 35 de la loi informatique et libertés).