LIVRET DE SENSIBILISATION AU RGPD

EPD
ÉQUIPE PROTECTION DES DONNÉES

CDG 22
CENTRE DE GESTION
de la fonction publique territoriale

INTRODUCTION

Entré en application en 2018, le Règlement général sur la protection des données (RGPD) établit un cadre harmonisé pour la protection des données à caractère personnel au sein de l'Union européenne.

Dans l'exercice de leurs missions, les collectivités territoriales sont amenées à traiter un volume important de données personnelles, que ce soit pour assurer la gestion des services publics dont elles ont la charge ou pour leurs besoins internes, par exemple en matière de ressources humaines. À ce titre, elles sont pleinement soumises aux dispositions du RGPD et doivent veiller à en respecter les exigences.

Ce guide a pour objectif de présenter aux élus et aux interlocuteurs des collectivités (directeurs généraux des services, secrétaires de mairie) les connaissances essentielles relatives au RGPD : ses grands principes, les bonnes pratiques à adopter ainsi que les principales étapes pour engager une démarche de mise en conformité.

Le service Protection des données du CDG22 se tient à votre disposition pour toute question et pour vous accompagner dans cette démarche.

LES POINTS-CLÉS

- La collectivité, représentée par son exécutif est responsable des traitements de données personnelles qu'elle met en œuvre
- Le non-respect du RGPD peut entrainer des conséquences pour la collectivité (impact en termes d'image, impacts financiers)
- La désignation d'un délégué à la protection des données est une obligation pour les organismes publics
- La mission du délégué à la protection des données est de conseiller et d'accompagner la collectivité dans ses démarches de conformité RGPD
- Pour assurer leur conformité au RGPD, les collectivités doivent notamment respecter les grands principes de protection des données, mettre en place des mesures de sécurité adéquates et tenir un registre des activités de traitements

Le RGPD : de quoi s'agit-il ?

Le Règlement général sur la protection des données (RGPD) est un règlement européen qui encadre le traitement des données personnelles sur le territoire de l'Union européenne. Il s'inscrit dans la continuité de la Loi Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation de leurs données.

Il prévoit de nouvelles obligations pour les organismes privés et publics amenés à traiter des données personnelles dans le cadre de leurs activités.

Les enjeux de la conformité RGPD pour la collectivité

La mise en conformité au RGPD constitue une obligation réglementaire pour les collectivités territoriales. À ce titre, la CNIL, autorité chargée de veiller au respect de cette réglementation, peut prononcer des mesures correctrices ou des sanctions en cas de manquements.

À titre d'illustration, en 2023, une commune a fait l'objet d'une mise en demeure publique de la CNIL pour ne pas avoir désigné de délégué à la protection des données. D'autres collectivités territoriales ont également été sanctionnées financièrement pour divers manquements aux principes du RGPD, tels que l'absence d'information des personnes concernées ou des insuffisances dans la sécurisation des données.

La protection des données personnelles revêt par ailleurs une importance accrue dans un contexte de multiplication des cyberattaques visant les acteurs publics.

Le respect du RGPD et la mise en œuvre de mesures de sécurité appropriées permettent non seulement de se conformer aux obligations légales, mais également de réduire les risques et les conséquences de telles attaques pour les personnes concernées.

Respecter le RGPD est également un facteur de transparence à l'égard des administrés et des agents. C'est aussi un gage de sécurité juridique pour les élus (Maire, Président), responsables de traitement.

01 LES FONDAMENTAUX DU RGPD

Notions-clés

Qu'est-ce qu'une donnée à caractère personnel ?

Il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable. Par exemple :

- Un nom, un prénom, une photographie
- Un numéro de téléphone ou de plaque d'immatriculation

Certaines données sont considérées comme sensibles au sens de la règlementation. Il s'agit notamment des données de santé, des informations révélant les opinions religieuses, philosophiques ou politiques des personnes ou encore des données relatives à l'origine raciale ou ethnique. Le traitement de ces données est par principe interdit.

Qu'est-ce qu'un traitement de données ?

Il s'agit d'une opération ou d'un ensemble d'opérations portant sur des données personnelles (collecte, extraction, consultation...).
Le RGPD s'applique dès lors qu'un traitement de données personnelles est mis en œuvre, indépendamment du support des données. Ce qui signifie que le RGPD est applicable aussi bien aux données traitées sur support informatisé qu'aux données traitées au format papier.

Les grands principes du RGPD

Le respect des finalités du traitement

En vertu de ce principe, les données doivent être collectées dans un but déterminé et légitime (par exemple, inscription au service périscolaire). Les données ne doivent pas être réutilisées et traitées ultérieurement de manière incompatible au regard de l'objectif initial pour lequel elles ont été collectées.

La minimisation des données

Ce principe impose de ne collecter que les données strictement nécessaires à l'accomplissement de la finalité.

Conservation limitée des données

Les données ne doivent pas être conservées au-delà de ce qui est nécessaire pour atteindre la finalité. Une durée de conservation doit être déterminée ou a minima, les critères pour la fixer. Dans ce cadre, il revient aux collectivités de respecter les obligations leur incombant au titre de la règlementation relative aux archives publiques.

Respect des droits des personnes

Les personnes concernées par un traitement de leurs données personnelles disposent de droits sur ces données (droit d'accès, droit d'effacement...). Il revient au responsable de traitement de garantir aux personnes l'exercice de leurs droits. A ce titre, le responsable de traitement doit également informer les personnes des traitements réalisés sur leurs données via des mentions d'information adaptées.

La sécurité des données

Le responsable de traitement est soumis à une obligation de sécurité. Il doit mettre en place des mesures techniques et organisationnelles pour assurer la sécurité des données qu'il traite.

Les acteurs de la mise en conformité

Le responsable de traitement

C'est la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal (Maire pour la commune, Président pour l'EPCI par exemple).

En tant que représentant de la collectivité, le Maire ou le Président incarne juridiquement le responsable de traitement et reste garant du respect du RGPD aux yeux de la CNIL.

Le sous-traitant

C'est la personne physique ou morale qui traite des données au nom et pour le compte d'un autre organisme (le responsable de traitement), dans le cadre d'un service ou d'une prestation. Par exemple, un hébergeur, un prestataire de logiciel ou de maintenance informatique pourra être considéré comme sous-traitant au regard du RGPD.

Le Délégué à la protection des données

Le délégué à la protection des données informe et conseille la collectivité sur la conformité RGPD des traitements mis en œuvre. Il accompagne le responsable de traitement pour la rédaction et la tenue de la documentation obligatoire. C'est également le point de contact des personnes concernées par un traitement de données et l'interlocuteur privilégié de la CNIL.

La désignation d'un délégué à la protection des données est obligatoire pour les organismes publics.

La CNIL

La CNIL est l'autorité française chargée de protéger les données personnelles et les libertés individuelles. Elle veille au respect du RGPD, contrôle les organismes publics et privés, accompagne les citoyens dans l'exercice de leurs droits et peut sanctionner les manquements constatés.

02 QUELLES SONT LES PRINCIPALES ACTIONS POUR ÊTRE CONFORME AU RGPD ?

La conformité au RGPD repose sur l'application, au quotidien, des grands principes de protection des données. Il s'agit d'une démarche dynamique et continue. Elle implique également la réalisation de plusieurs actions concrètes, telles que la tenue d'un registre des traitements, la mise à jour des formulaires et des mentions d'information à destination des usagers, ou encore la mise en place de mesures adaptées pour garantir la sécurité des données.

Rédiger le registre des traitements

Afin d'assurer leur conformité au RGPD, les collectivités sont tenues d'établir un registre des traitements, permettant de recenser l'ensemble des traitements de données mis en œuvre dans le cadre de leurs missions.

Encadrer les relations avec les sous-traitants

Les relations avec les sous-traitants (cf. définition ci-dessus), doivent faire l'objet d'un encadrement contractuel spécifique permettant de fixer les obligations et engagements du sous-traitant lorsqu'il traite des données pour le compte de la collectivité.

Mettre en place une information des personnes sur le traitement de leurs données personnelles

Afin de respecter les droits des personnes et assurer la transparence sur les traitements de données personnelles, il convient de mettre en place des modalités permettant d'informer les personnes de ces traitements.

Par exemple :

- *Intégrer des mentions d'information sur les formulaires de collecte de données*
- *Procéder à un affichage RGPD dans les locaux de la collectivité*
- *Rédiger une politique de confidentialité sur le site internet de la collectivité.*

Organiser et faciliter l'exercice des droits des personnes concernées

En vertu du RGPD, les personnes disposent de plusieurs droits sur leurs données personnelles. Le responsable de traitement doit mettre en place une organisation permettant de répondre efficacement aux demandes des personnes dans les délais prévus par la règlementation (1 mois à compter de la réception de la demande).

Par exemple : procédure interne dédiée à la gestion des demandes, formulaire dédié pour le recueil de ces demandes, etc.

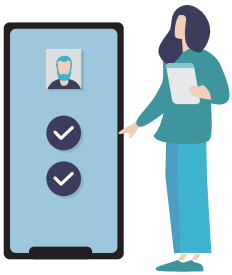
Mettre en place des mesures permettant d'assurer la sécurité des données

Exemples de bonnes pratiques (liste non exhaustive) :

- *Utiliser des mots de passe robustes, uniques et renouvelés régulièrement (12 caractères ou plus avec un chiffre, une majuscule, une minuscule, un signe de ponctuation ou un caractère spécial)*
- *Stocker les mots de passe de manière sécurisée (utilisation d'un coffre-fort de mot de passe par exemple)*
- *Procéder à des sauvegardes régulières*
- *Verrouiller les postes informatiques en cas d'absence*
- *Prévoir des habilitations strictes sur le réseau et les logiciels métiers*
- *Mettre en place des mesures de sécurité physiques pour les dossiers papier (verrouillage des locaux, utilisation d'armoires ou placards fermés à clés)*
- *Gestion des accès aux locaux.*

Exemples de pratiques déconseillées (liste non exhaustive) :

- *Utiliser un mot de passe trop faible*
- *Ne pas stocker son mot de passe de manière sécurisée*
- *Partager son mot de passe*
- *Stocker des données sensibles sur des clés USB non sécurisées ou dans des endroits non fermés à clé*
- *Envoyer des documents professionnels contenant des données personnelles sur sa boîte mail personnelle*
- *Télécharger des pièces jointes ou cliquer sur des liens provenant d'expéditeurs inconnus ou suspects*
- *Partager des données et des documents à des personnes non habilitées (interne et externe à la collectivité)*



Gérer les violations de données

Lorsque des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées ou divulguées (mail transmis à des mauvais destinataires, équipements perdus ou volés, publication involontaire de données sur internet, etc.), il s'agit d'une violation de données personnelles.

Que faire en cas de violation de données ?

- Contactez immédiatement votre délégué à la protection des données

- L'incident devra être documenté dans le registre des violations de la collectivité

- Si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées, elle devra être notifiée à la CNIL dans les 72 heures à compter de la prise de connaissance

- Si cette violation est susceptible de représenter un risque élevé pour les droits et libertés des personnes concernées, celles-ci devront être informées de cet incident par la collectivité ou le prestataire si cela est prévu dans le contrat.

03 L'ACCOMPAGNEMENT DU CDG22 DANS LA MISE EN CONFORMITÉ RGPD DES COLLECTIVITÉS

Lorsque le CDG22 est désigné comme Délégué à la protection à des données de la collectivité, il l'accompagne pour sa mise en conformité RGPD.

Dans ce cadre, le Service Protection des données réalise les missions suivantes :

- Actions de sensibilisation au RGPD
- Réalisation d'états des lieux des traitements de données et des mesures de sécurité
- Préconisation et conseil sur les traitements de données mis en œuvre par la collectivité
- Accompagnement à la rédaction du registre des traitements
- Accompagnement pour le traitement des demandes d'exercice de droits
- Accompagnement pour le traitement des incidents (violations de données)
- Analyse de documents (formulaires, contrats avec les sous-traitants)
- Fourniture de guides, de modèles et de procédures

02.96.58.63.66

cil@cdg22.fr

EPD

ÉQUIPE PROTECTION
DES DONNÉES