GUIDE DE SENSIBILISATION AU RGPD

POUR LES COLLECTIVITÉS TERRITORIALES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

TABLE DES MATIÈRES

AVANT-PROPOS

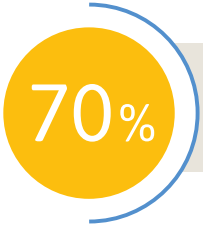
Les collectivités territoriales traitent de nombreuses données personnelles, que ce soit pour assurer la gestion des services publics dont elles ont la charge (état civil, inscriptions scolaires, listes électorales, etc.), la gestion des ressources humaines, la sécurisation de leurs locaux (contrôle d'accès par badge, vidéosurveillance) ou encore leur site web.

Les citoyens sont **de plus en plus sensibles à la protection de leurs données** et leur principal motif de crainte est la peur du piratage et du vol de données.

Le développement de **services en ligne** constitue un levier majeur de la modernisation de l'action publique. De ce fait, les collectivités recourent de plus en plus aux téléservices, aux systèmes d'information géographique, à la vidéosurveillance, aux dispositifs de lecture automatique de plaques d'immatriculation, aux solutions de ville intelligente, etc.

Le nombre de **cyberattaques** et plus globalement d'incidents de sécurité ne cesse d'augmenter, et ce, quelle que soit la taille des organisations visées.

Respecter les règles de protection des données est un facteur de transparence et de confiance à l'égard des administrés et des agents. C'est aussi un gage de sécurité juridique pour les élus qui sont responsables des fichiers et des applications utilisées au sein de la commune.



Selon un sondage IFOP réalisé en avril 2019 pour la CNIL, 70 % des Français se disent plus sensibles que ces dernières années à la protection de leurs données personnelles.

Le règlement général sur la protection des données (RGPD) s'inscrit dans la continuité des principes initialement présents dans la loi Informatique et Libertés de 1978. Malgré cela, la CNIL est consciente que la mise en conformité au RGPD peut parfois être complexe. L'importance des enjeux justifie un appui de sa part.

Aussi, afin d'accompagner les collectivités territoriales dans leur mise en conformité au RGPD, la CNIL a élaboré un guide de sensibilisation. Celui-ci s'adresse prioritairement aux communes de taille moyenne ou petite, ainsi qu'à leurs groupements intercommunaux, ne disposant pas nécessairement en interne de ressources dédiées spécifiquement à la protection des données. Ce guide propose des clés de compréhension des grands principes, les réflexes de bon sens à acquérir, un plan d'action pour se mettre en conformité et des fiches pratiques.

Ce guide ne répondra pas nécessairement à des besoins plus spécifiques. Mais, dans le cadre de son plan d'action global dédié à l'accompagnement des collectivités territoriales et de leurs groupements, la CNIL va progressivement enrichir la rubrique dédiée de son site. Des fiches techniques consacrées aux principaux sujets de préoccupation des différents niveaux de collectivités seront ainsi mises en ligne et régulièrement mises à jour. Par ailleurs, la CNIL proposera prochainement, en plus de son cours en ligne gratuit sur le RGPD, un module spécifique pour les collectivités.

Soucieuse d'accompagner toutes les collectivités dans leur mise en conformité au RGPD, la CNIL s'est rapprochée des principales associations regroupant les différents niveaux de collectivités et autres organismes intervenant auprès du secteur public local, avant la mise en œuvre de ce nouveau cadre juridique. L'appui fourni par ces associations, sous la forme d'une centralisation des problématiques et des remontées de terrain ou d'une mise à disposition de ressources peut permettre à la CNIL d'apporter des réponses concrètes et adaptées à chaque niveau de collectivités.

Ce dialogue continu avec les différents acteurs territoriaux répond à la volonté du législateur qui, dans le cadre de la rénovation du cadre législatif Informatique et Libertés français en 2018, a souhaité préciser les missions de la CNIL afin que celle-ci apporte une information adaptée et un accompagnement dédié aux collectivités et à leurs groupements.

La CNIL tient à remercier l'AMRF (Association des maires ruraux de France), l'AMF (Association des maires de France), l'ANDAM (Association nationale des directeurs d'associations de maires), l'ADF (Assemblée des départements de France), Régions de France, l'AFCDP (Association française des correspondants à la protection des données à caractère personnel) et la DGCL (Direction générale des collectivités locales) qui ont accepté de relire et d'enrichir ce guide.

POUR APPROFONDIR LES QUESTIONS ABORDÉES DANS CE GUIDE, VOUS POUVEZ CONSULTER

- Le dossier collectivités territoriales
- Le MOOC, formation en ligne gratuite sur le RGPD

QUE CHANGE LE RÈGLEMENT EUROPÉEN (RGPD) POUR LES COLLECTIVITÉS TERRITORIALES ?

Le règlement général sur la protection des données (RGPD) est entré en application le 25 mai 2018. Les grands principes déjà présents depuis 1978 dans la loi Informatique et Libertés ne changent pas. Mais le texte passe d'une logique de contrôle a priori, basée sur des formalités auprès de la CNIL, à une logique de responsabilisation de tous ceux qui traitent des données personnelles, entreprises comme collectivités territoriales. Ces principes doivent être intégrés le plus en amont possible, dès leur conception, dans l'ensemble de vos projets.

Avec le RGPD, les déclarations à la CNIL sont supprimées. En contrepartie, les collectivités doivent s'assurer que leurs fichiers et services numériques sont conformes au RGPD, et ce, de façon active et en continu. Ceci nécessite de tenir à jour une documentation des actions menées afin de pouvoir démontrer sa mise en conformité, par exemple en cas de contrôle de la CNIL.

Ainsi, vous devez :

- désigner un délégué à la protection des données ;
- recenser les traitements de données et tenir à jour un registre de ceux-ci ;
- encadrer la sous-traitance des traitements ;
- garantir la sécurité des données ;
- organiser la réponse aux demandes d'exercice des droits venant des administrés ;
- notifier à la CNIL, voire aux personnes concernées, les violations éventuelles de données personnelles (par exemple les failles de sécurité) ;
- effectuer dans certains cas des analyses d'impact sur la vie privée et les libertés pour certains traitements à risques.

Désormais, cette logique de responsabilisation concerne aussi les prestataires auxquels les collectivités sous-traitent la gestion (hébergement de données par exemple) ou l'entière mise en œuvre de leurs traitements de données personnelles. En tant que sous-traitants, ces acteurs sont en effet soumis à des obligations propres prévues par le RGPD. Ces obligations devront, pour une grande part, être inscrites dans les conventions passées avec la collectivité. Il est du devoir des sous-traitants de participer à la mise en conformité des collectivités territoriales, en les aidant, notamment en matière de sécurité des données, à satisfaire aux exigences du RGPD.

ATTENTION

Certains acteurs peu scrupuleux profitent du RGPD pour proposer des prestations coûteuses, générer des appels surtaxés ou faire croire qu'ils agissent pour le compte de la CNIL. Renseignez-vous sur leurs compétences et références avant de vous engager. La CNIL ne mandate aucune entreprise ou autre structure pour accompagner les organismes publics et privés dans leur mise en conformité au RGPD. La mise en conformité au RGPD nécessite plus qu'un simple échange ou l'envoi d'une documentation. Elle suppose un vrai accompagnement, par un professionnel qualifié en protection des données personnelles, pour identifier les actions à mettre en place et assurer leur suivi dans le temps. En cas de doute, contactez la CNIL.

QUEL EST LE RÔLE DE LA CNIL ?

La Commission nationale de l'informatique et des libertés (CNIL) est l'autorité de protection des données française. Elle conseille les professionnels et aide les particuliers à exercer leurs droits. Pour accomplir ses missions, elle dispose également de pouvoirs de contrôle et de sanction.

- elle accompagne les acteurs privés et publics dans leur démarche de mise en conformité en matière de protection des données personnelles ;
- elle encourage l'innovation dans un cadre respectueux de la réglementation ;
- elle reçoit et traite les plaintes des particuliers ;
- elle dispose de pouvoirs de contrôles sur place, en ligne, sur pièce ou sur audition ;
- elle peut prononcer des mises en demeure de se mettre en conformité ;
- elle peut prononcer des sanctions (amende financière jusqu'à 20 millions d'euros pour les organismes ayant commis des manquements graves à la loi Informatique et Libertés ou au RGPD).

La CNIL conduit un certain nombre d'actions et de programmes spécifiques afin d'accompagner les collectivités dans la mise en œuvre du RGPD avec l'appui, en particulier de plusieurs « têtes de réseaux » afin d'impulser et de guider les démarches de mise en conformité dans le secteur des collectivités territoriales. Ces actions comprennent la diffusion de contenus (site web de la CNIL, publications conjointes) ainsi que l'accompagnement du secteur (interventions extérieures et groupes de travail notamment).

Cette approche a un triple objectif :

1 - identifier et être à l'écoute des problématiques que rencontrent les collectivités ;
2 - garantir une diffusion la plus large possible des réponses apportées ;
3 - favoriser la collaboration entre collectivités.

POUR ALLER PLUS LOIN

Mieux connaitre la chaîne répressive de la CNIL

PROTECTION DES DONNÉES PERSONNELLES : DE QUOI PARLE-T-ON ?

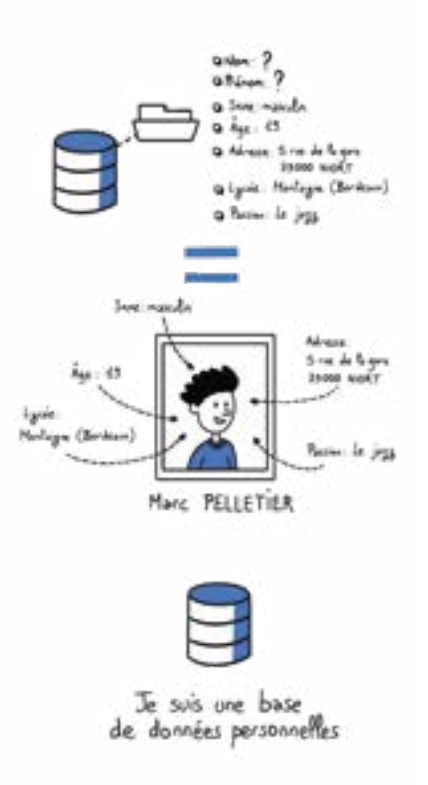
Qu'est-ce qu'une donnée personnelle ?

Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne physique peut être identifiée :
- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :
- à partir d'une seule donnée (exemple : nom) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre de telle association).

Par exemple, une enquête par questionnaire qui porte sur des élèves d'une école primaire peut, même lorsque les noms et prénoms ne sont pas indiqués, contenir des réponses qui, combinées les unes aux autres, permettent de retrouver l'identité des enfants. C'est le cas lorsque les réponses sont précises, par exemple : 7 ans, fille, classe de CE1, redoublement dans telle école primaire de telle ville.



En revanche, des coordonnées d'entreprises (par exemple, l'entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie1@email.fr ») ne sont en principe pas des données personnelles.

Qu'est-ce qu'un « traitement de données personnelles » ?

Un « traitement de données personnelles » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement. C'est donc une notion très large : tout maniement de données, y compris une simple consultation, est un « traitement de données personnelles ».
Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

EXEMPLES DE TRAITEMENTS

Tenue du registre d'état civil, gestion des inscriptions en crèche, scolaire et périscolaire, tenue du cadastre, gestion de la liste électorale, gestion des ordures ménagères, gestion des adhérents de la médiathèque, etc.
Il peut s'agir d'une base de données, d'un fichier papier ou numérique, d'une application mobile, de dispositifs biométriques, de sites web, etc.

La finalité

Un traitement de données doit avoir un objectif, **une finalité déterminée** préalablement au recueil des données et à leur exploitation. Autrement dit, il n'est pas permis de collecter des données lorsque l'on ne sait pas quel usage en faire. Par ailleurs, en principe, la finalité initiale doit être respectée, afin d'éviter tout « détournement de finalité ».

EXEMPLE DE FINALITÉ

Un maire ne pourra pas se servir du fichier des inscriptions scolaires pour faire de la communication politique. La liste électorale pourra en revanche être utilisée à une telle fin.

La licéité ou la base légale

Chaque traitement doit être licite. Cela signifie d'abord qu'il doit être conforme au droit en général (par exemple, un traitement de données ne peut pas avoir pour but une discrimination illégale). Cela signifie, ensuite, qu'il doit reposer sur l'une des six « bases légales » permises par le RGPD, c'est-à-dire l'une des hypothèses dans lesquelles le RGPD autorise un opérateur à traiter les données de personnes physiques : l'obtention du consentement préalable de la personne, l'exécution d'un contrat conclu avec elle, l'accomplissement d'une mission d'intérêt publique, le respect d'une obligation légale qui impose le traitement de ces données, etc.

POUR ALLER PLUS LOIN

Règlement européen, le consentement est-il obligatoire ?

Dans la majorité des cas, les collectivités n'auront pas à recueillir le consentement. Le plus souvent, les traitements mis en œuvre reposeront plutôt sur le respect d'une obligation légale ou l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique. Toutefois, certains traitements des collectivités devront tout de même reposer sur le consentement des personnes. Le consentement est défini comme une manifestation de volonté libre, spécifique, éclairée et univoque. Il doit être un acte positif clair.

EXEMPLE DE BASE LÉGALE

La tenue du registre de l'état civil est une obligation légale. Mais, dans le cas de la diffusion des évènements familiaux, les données enregistrées aux fins d'inscription d'un acte sur le registre de l'état civil ne peuvent être utilisées par les élus municipaux pour adresser des félicitations ou des condoléances. De même, ces informations ne peuvent être diffusées (dans la presse ou sur tout autre support) que si les personnes concernées ont, au moment de l'établissement de l'acte, donné leur consentement à ce message personnalisé ou à cette publication.

La formule suivante peut être adoptée pour figurer sur les documents distribués aux personnes accomplissant des démarches relatives à l'état civil :

MODÈLE DE MENTION POUR L'ÉTAT CIVIL

« La mairie de..... vous propose de faire part de la naissance de votre enfant, de votre mariage dans le bulletin municipal. Afin de respecter votre vie privée, cette diffusion nécessite votre consentement.

M., Mme..... (Nom, Prénom) accepte qu'une information relative à l'événement d'état civil déclaré ce jour soit publiée dans le bulletin municipal.

Le ..... (date) »

Le responsable de traitement

La personne morale ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser, est appelée « responsable de traitement ».

EXEMPLE DE RESPONSABLES DE TRAITEMENT

La commune est responsable de la tenue, de la gestion et de la révision annuelle de la liste électorale en application des dispositions du code électoral. La commune est responsable de la tenue du fichier des personnes vulnérables dans le cadre du « plan canicule » en application des dispositions du code de l'action sociale et des familles. Dans le cas de traitements mis en œuvre par une EPCI (traitement des déchets, gestion des aires d'accueil pour gens du voyage), c'est l'intercommunalité qui est le responsable de traitement.

POUR ALLER PLUS LOIN

- Un petit lexique RGPD vous est proposé en annexe de ce guide.
- Une liste non exhaustive des traitements de données le plus souvent mis en œuvre par les collectivités vous est proposée en annexe de ce guide.

DÉSIGNEZ UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

Le RGPD impose à toutes les structures publiques de désigner un délégué à la protection des données. Cela concerne les collectivités ainsi que tout organisme ou autorité publique locale agissant en tant que responsable de traitement ou sous-traitant (CCAS, EPCI, etc.).

Les missions

1 - **Informer et conseiller la collectivité**, notamment son représentant légal (maire, président de conseil régional et départemental, président d'établissement public de coopération intercommunale), ainsi que les agents sur la conformité au RGPD des traitements (actuels et à venir). Le délégué conseille par exemple la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données.

2 - **Contrôler le respect du règlement et du droit national en matière de protection des données**. Dans la majorité des cas, le délégué tient et actualise le registre des traitements. Ce registre lui offre une vue d'ensemble sur les traitements : quels objectifs, quelles données, quels destinataires, quelles durées de conservation, quelles mesures de sécurité, etc ?

3 - **Être le point de contact pour les personnes dont les données sont traitées par la collectivité et l'interlocuteur privilégié de la CNIL.** Pour cela, les coordonnées du DPO doivent être facilement accessibles. Il est donc nécessaire de les mentionner sur les différents formulaires et sur le site web.

POUR FACILITER LA TENUE DU REGISTRE

La CNIL propose un modèle de registre, destiné à répondre aux besoins les plus courants en matière de traitements de données

Les compétences

Le DPO doit être choisi sur la base de ses connaissances du droit et des pratiques en matière d'application du RGPD. Toutefois, le RGPD n'impose pas aux organismes de recourir à une profession particulière pour la désignation de leur DPO : aucun agrément n'est prévu, aucune exigence de diplôme ou condition statutaire n'est fixée. Il peut donc s'agir d'une personne physique ou morale issue du secteur juridique ou technique, en interne à la collectivité ou en externe (avocat, consultant, etc.).
Les compétences pourront être acquises ou développées au moyen d'un plan de formation adapté au profil du délégué. Les compétences pourront être attestées, sans qu'il n'y ait aucune obligation en la matière, par le recours à un mécanisme de certification, tel que celui établi par la CNIL.

MOOC RGPD de la CNIL

À NOTER : la CNIL met à disposition un cours en ligne gratuit (MOOC) sur le site https://atelier-rgpd.cnil.fr/ qui délivre une attestation de suivi. Il s'agit d'un bon moyen pour un DPO nouvellement désigné de vérifier et valider son niveau d'expertise. C'est également un outil efficace de diffusion aux agents des fondamentaux du RGPD et de la loi Informatique et Libertés.

POUR ALLER PLUS LOIN

Consulter les référentiels de compétences du DPO

Le statut

Le délégué doit pouvoir :

• **rendre compte au niveau le plus élevé de la hiérarchie.**
Quelle que soit sa position précise dans l'organigramme, le délégué doit avoir accès et rendre compte de l'exercice de sa mission au niveau exécutif de la collectivité (maire, président du conseil départemental ou régional, directeurs généraux).

• **être en mesure d'exercer ses fonctions et missions en toute indépendance.**
Cette deuxième condition signifie que le délégué bénéficie d'une liberté dans les analyses et actions qu'il décide d'entreprendre, et qu'il ne doit pas recevoir d'instruction dans l'exercice même de ses missions (par exemple sur le sens des avis qu'il rend, sur l'orientation des conseils qu'il donne, etc.).
Il ne peut donc pas faire l'objet d'une sanction ou d'une mesure préjudiciable du seul fait de leur accomplissement (en cas de désaccord avec le responsable de traitement sur une analyse par exemple).

• **être à l'abri des conflits d'intérêts.**
La condition relative au conflit d'intérêts – ne pas se retrouver à la fois juge et partie – constitue une garantie d'indépendance importante. Ainsi, lorsque le délégué est amené à exercer d'autres fonctions, elles ne doivent pas le conduire à décider des finalités et/ou des moyens de mise en œuvre des traitements de données personnelles.

Cette question doit être étudiée au cas par cas, notamment au regard de la taille, de la structure organisationnelle et de l'objet des activités parallèles. Par exemple, la fonction de directeur général des services apparaît particulièrement problématique à cet égard.

Dans les petites collectivités, les secrétaires de mairie sont souvent pressentis pour occuper la fonction de DPO. Or, leur désignation peut parfois se heurter à des difficultés : manque de temps à consacrer au sujet et risque de conflits d'intérêts. Ainsi, avant de procéder à la désignation et pour éviter un risque de conflit d'intérêt, il faudra s'assurer qu'ils ne prennent pas part au circuit de décision concernant les fichiers mis en œuvre dans leur collectivité (objectifs et conditions de mise en œuvre, données traitées, destinataires, durées de conservation, mesures de sécurité, etc.). Dans le cas contraire, leur désignation ne sera pas possible.

Les conseillers municipaux (dont le maire) ne peuvent pas quant à eux être désignés délégués. En effet, en tant que membres de l'assemblée délibérante, ils prennent directement part au processus de décision.

Les différentes formes de délégués

• **Le délégué interne**
Le délégué peut être un agent titulaire ou contractuel de la collectivité.
Lorsqu'elle est possible, une désignation interne répond parfaitement au besoin de proximité du délégué vis-à-vis des personnes qui mettent en œuvre les traitements (solide connaissance des métiers, grande réactivité). La désignation d'un DPO interne n'empêche pas la collectivité de s'appuyer ponctuellement, et de façon complémentaire, sur l'expertise d'un prestataire externe.

• **Le délégué externe**
Les collectivités ont la possibilité de recourir à un délégué externe, personne physique ou morale, par exemple un avocat ou un cabinet de consultants spécialistes des questions Informatique et Libertés. Un contrat de prestation de service relevant des règles de la commande publique devra alors être conclu.
L'avantage d'une telle solution est de permettre aux collectivités de bénéficier d'une expertise en matière de protection des données, ainsi que d'outils et procédures ayant fait leur preuve dans d'autres organismes.

• **La mutualisation de la désignation**

La mutualisation peut permettre de limiter les coûts et de bénéficier de professionnels disposant des compétences et de la disponibilité nécessaires. Le délégué pourra intervenir selon plusieurs modalités de mutualisation, par exemple :

- **la mise à disposition d'agents** par une collectivité territoriale ou un établissement public, voire un centre de gestion, au profit d'une autre collectivité ou d'un établissement public, pour y exercer des missions de DPO ;

- **la prestation de services :** le DPO peut intervenir dans le cadre d'une convention de prestation de services conclue entre une collectivité et un établissement public dans les conditions prévues par le CGCT (Code général des collectivités territoriales). Une telle prestation est soumise au droit de la commande publique ;

- **la mise en place d'un service unifié** entre des collectivités territoriales et leurs groupements, au sein duquel le DPO exercera sa mission au profit de tous les cocontractants ;

- **la mise en place d'un service commun** entre des communes, leur établissement public de coopération intercommunale à fiscalité propre et leurs établissements publics rattachés, au sein desquels le DPO exercera sa mission au profit de tous les cocontractants.

La convention de mutualisation pour les organismes publics

Les collectivités territoriales, les établissements publics administratifs locaux et les personnes morales de droit privé gérant un service public qui optent pour la mutualisation ont l'obligation de conclure une convention de mutualisation.

Cette convention définit les conditions dans lesquelles s'exerce cette mutualisation, en particulier s'agissant des moyens alloués au délégué afin que son action soit effective au sein de chaque collectivité.

La désignation

Vous devez obligatoirement notifier à la CNIL la désignation de votre délégué en utilisant le téléservice https://www.cnil.fr/designation-dpo.

Pour toute modification, vous pouvez envoyer un courriel à servicedpo@cnil.fr.

POUR ALLER PLUS LOIN

Consulter :

• La rubrique DPO

• Le Guide des coopérations à l'usage des collectivités locales et de leurs groupements de la DGCCL

COMMENT ASSURER VOTRE CONFORMITÉ AVEC UN PLAN D'ACTION EN 4 ÉTAPES ?

La démarche de conformité RGPD ne doit pas être perçue que comme une contrainte technique ou juridique. C'est avant tout l'occasion de faire le point sur l'utilisation des services numériques dans la collectivité et de s'assurer que la protection des données personnelles a bien été prise en compte.
La mise en conformité au RGPD passe par plusieurs étapes successives et certaines de ces actions doivent perdurer dans le temps pour être efficaces (formation, évolution des procédures, etc.). Il s'agit d'une démarche active et en continu.

Étape 1 > Recensez les traitements

Le RGPD impose au responsable de traitement de tenir un registre listant les traitements de données. Il vous permet d'avoir une vision claire et globale des activités de la collectivité qui nécessitent la collecte et le traitement de données personnelles.

La tenue du registre est l'occasion de sensibiliser les services aux enjeux de la protection des données. Dans les faits, ce registre est souvent tenu par le DPO.

Dans votre registre, créez une fiche par activité recensée, en précisant :

- **le nom et les coordonnées** du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
- **le ou les objectifs poursuivis par chaque traitement** (finalité(s) du traitement ex : tenue de l'état civil) ;
- **les catégories de personnes concernées et de données** utilisées (ex : nom, nationalité, adresse, etc.) ;
- **qui a accès aux données** (personnes habilitées – ex : service RH pour la paie) et à qui elles seront communiquées (les destinataires - ex : les services des impôts) ;
- **les durées de conservation** de ces données (durée d'utilité et durée de conservation en archive) ;
- **les mesures de sécurité** envisagées (ex : politique des mots de passe, etc.) ;
- le cas échéant, **les transferts de données** à caractère personnel en dehors de l'Union européenne ou à une organisation internationale.

Pour avoir un registre exhaustif et à jour, il est nécessaire d'être en contact régulier avec toutes les personnes de la collectivité susceptibles de traiter des données personnelles.

POUR ALLER PLUS LOIN

Pour aider les responsables de traitements, des modèles de registre de traitement sont disponibles sur le site de la CNIL.

Étape 2 > Faites le tri dans les données

Chaque fiche du registre vous permet de vérifier :

- que les données traitées sont bien pertinentes et nécessaires à l'objectif poursuivi (principes de pertinence et de minimisation).

EXEMPLE DE PERTINENCE

Pour l'inscription à l'école élémentaire, il est légitime de demander un livret de famille, un justificatif de domicile et un document attestant que l'enfant a reçu les vaccinations obligatoires pour son âge.

Lors d'une inscription scolaire, il n'est en revanche pas pertinent de demander le numéro de sécurité sociale du ou des représentants légaux ou encore la copie de leur carte Vitale. Pour la gestion de la cantine scolaire, il suffit d'enregistrer uniquement les informations relatives au régime alimentaire et aux aliments à proscrire pour un élève plutôt que d'inscrire son état de santé (ex : « diabétique ») ou de mentionner sa religion.

- la nature des données traitées afin d'adopter des mesures de sécurité adaptées aux risques spécifiques associés aux données.

EXEMPLE DE MESURE DE SÉCURITÉ

Les établissements scolaires et périscolaires sont amenés à collecter des données relatives à la santé des mineurs qu'ils accueillent dans le cadre des projets d'accueil individualisé (PAI). Dans la mesure où ces informations sont sensibles, elles doivent faire l'objet de mesures de protection particulières (rangement sécurisé, etc.).

- que seuls les agents habilités ont accès aux données dont ils ont besoin.

EXEMPLE DE DESTINATAIRES

Dans le cadre des demandes d'actes d'état civil, l'accès aux informations nécessaires à l'instruction de ces demandes doit être limité aux seuls agents chargés de cette activité.

- que les données ne sont pas conservées au-delà de ce qui est nécessaire en fixant précisément la durée de conservation et d'archivage des données (principe de durée limitée de **conservation** des données).

EXEMPLE DE DURÉE DE CONSERVATION

Dans le cadre d'un fichier de prévention de la délinquance mis en œuvre par une mairie, les données sur une personne peuvent être conservées pendant le temps du suivi. Les données peuvent ensuite être conservées en archive durant 3 ans après la fin du suivi.
En tout état de cause, dans la mesure où dans le cadre des programmes de prévention de la délinquance, les personnes concernées ne peuvent être suivies que jusqu'à 25 ans, aucune donnée ne doit être conservée au-delà de cette limite d'âge.

POUR ALLER PLUS LOIN

Voir en fin de guide la fiche n°4 relative aux durées de conservation et à l'archivage

Étape 3 > Respectez les droits des administrés

Le nombre toujours croissant de plaintes reçues par la CNIL témoigne de la sensibilité accrue des personnes concernant la protection de leurs données personnelles. En 2018, près de 74 % des plaintes reçues concernent l'exercice pratique des droits : absence de réponse de la part des organismes ou refus non motivé, absence de procédure en ligne pour exercer ses droits, etc.

• **Informez les personnes dont vous traitez les données**

Chaque fois que des données personnelles sont recueillies, que ce soit sur un formulaire, par l'intermédiaire d'un téléservice ou par oral, vous devez informer en toute transparence les personnes concernées des conditions d'utilisation de leurs données et de leurs droits, en particulier :

- vos coordonnées (le nom et les coordonnées du responsable du traitement) ;
- pourquoi vous collectez ces données (l'objectif de la collecte des données, par exemple pour gérer l'état civil) ;
- ce qui vous autorise à traiter ces données (l'exécution d'une mission de service public, le consentement de la personne concernée, etc.) ;
- qui a accès aux données (les services internes compétents, un prestataire, etc.) ;
- combien de temps vous conservez les données (la durée de conservation) ;
- comment les personnes peuvent exercer leurs droits (via leur espace personnel ou par un message adressé au DPO) ;
- si vous transférez les données hors de l'Union européenne (notamment par le biais d'un sous-traitant, le pays et l'encadrement juridique qui maintient le niveau de protection des données doivent être précisés).

Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, vous pouvez, par exemple, donner un premier niveau d'information en fin de formulaire et renvoyer à une politique de confidentialité/page vie privée sur votre site web.

• **Organisez et facilitez l'exercice des droits des administrés et des agents**

Les personnes (agents, administrés, prestataires, etc.) ont des droits sur leurs données. Vous devez permettre aux personnes d'exercer effectivement et le plus simplement possible leurs droits :
- **droit d'accès :** la personne accède à toutes les informations détenues sur elle ;
- **droit de rectification :** la personne modifie des informations détenues sur elle ;
- **droit d'opposition :** la personne refuse l'utilisation des informations détenues sur elle ;
- **droit d'effacement :** la personne demande la suppression des informations détenues sur elle ;
- **droit à la portabilité :** la personne récupère dans un format ouvert et lisible par machine les informations détenues sur elle ;
- **droit à la limitation :** la personne demande à « geler » l'utilisation des informations détenues sur elle.

Ces droits comprennent chacun des exceptions et des limitations spécifiques, en fonction de la base légale du traitement ou de son contexte. Par exemple, le droit d'opposition ne s'applique pas aux traitements dont la base légale est le respect d'une obligation légale (fichiers d'état civil ou fiscal).

BONNE PRATIQUE

Si vous disposez d'un site web, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée. Si vous proposez un compte en ligne, donnez aux administrés la possibilité d'exercer leurs droits à partir de leur compte.

Mettez en place, par l'intermédiaire du DPO, un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois maximum).

POUR ALLER PLUS LOIN

- Des exemples de mentions d'information sont disponibles sur le site web de la CNIL
- Respecter les droits des personnes

Étape 4 > Sécurisez les données

Vous devez mettre en place des mesures techniques et organisationnelles pour garantir la sécurité des données. En fonction de leur sensibilité, des mesures spécifiques sont nécessaires en cohérence avec les risques pour les droits et libertés des personnes concernées (ex : usurpation d'identité).

Trois types de risques sont ainsi à considérer : l'accès illégitime à des données, leur modification non désirée et leur disparition. Ces risques ne sont pas théoriques. Tous les jours, la CNIL reçoit des notifications de violation de données qui témoignent des faiblesses de la sécurisation de nombreux systèmes d'information. Ces incidents peuvent avoir des conséquences très préjudiciables pour les personnes dont les données sont concernées et des répercussions réputationnelles très importantes pour les organismes.

BONNE PRATIQUE

Les agents disposent d'un identifiant propre avec un mot de passe personnel, complexe, et régulièrement mis à jour. Leurs accès aux fichiers sont définis en fonction de leurs besoins réels en lien avec l'exercice de leur mission et leurs comptes informatiques sont clos à la fin de leur contrat. Les armoires sont fermées à clé. Les mots de passe sont changés régulièrement et ils sont suffisamment complexes.

• **Voici quelques vérifications que vous pouvez déjà effectuer :**

- ✓ Les accès aux locaux sont-ils sécurisés ?
- ✓ Les armoires et coffre-fort sont-ils fermés à clés systématiquement ?
- ✓ Les comptes utilisateurs sont-ils protégés par des mots de passe d'une complexité suffisante ? Sont-ils clos à la fin des contrats des agents ?
- ✓ Des profils distincts sont-ils prévus selon les besoins des utilisateurs pour accéder aux données ?
- ✓ Les postes de travail sont-ils sécurisés (ex : verrouillage automatique de session, antivirus et logiciels à jour) ?
- ✓ Le personnel est-il sensibilisé à la protection de la vie privée ? Une charte informatique est-elle signée ?
- ✓ Des mobiles multifonctions (smartphone), ordinateurs portables ou clé USB sont-ils utilisés ? Leur usage est-il encadré ?
- ✓ Des procédures de sauvegardes régulières et de récupération des données en cas d'incident sont-elles mises en place ?

POUR ALLER PLUS LOIN

- Recommandation de la CNIL sur les mots de passe et conseils pratiques
- Guide des bonnes pratiques de l'informatique réalisé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la Confédération des petites et moyennes d'entreprises (CPME).
- Guide sécurité des données personnelles sur le site web de la CNIL

Le site gouvernemental www.cybermalveillance.gouv.fr vous propose de l'aide en ligne ainsi qu'une liste de prestataires approuvés.

Que faire en cas de violation de données ?

Des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées (courriels transmis à des mauvais destinataires, équipement perdu ou volé, publication involontaire de données sur internet, etc.) ? Cet incident constitue une « violation de données ».

Si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées, vous devez la signaler à la CNIL dans les 72 heures. Cette notification s'effectue en ligne sur le site web de la CNIL :
https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Si ces risques sont élevés pour ces personnes, vous devrez les en informer.
Plus d'informations sur : https://www.cnil.fr/fr/les-violations-de-donnees-personnelles

COMMENT TRAVAILLER AVEC UN SOUS-TRAITANT ?

Le sous-traitant, au sens du RGPD, est la personne physique ou morale (entreprise ou organisme public) qui traite des données pour le compte d'un autre organisme (le responsable de traitement), dans le cadre d'un service ou d'une prestation.

Vous êtes concerné, en qualité de responsable de traitement, si vous choisissez de confier le traitement des données à des prestataires qui seront vos sous-traitants (exemple : hébergeurs de données, prestataires de services, etc.).

Le RGPD consacre une logique de responsabilisation de tous les acteurs impliqués dans un traitement de données personnelles en y incluant les sous-traitants.

Ceux-ci doivent vous aider, dans une démarche active et permanente de mise en conformité de vos traitements.

EXEMPLE DE SOUS-TRAITANCE

Une collectivité peut décider de confier la maintenance informatique à une société.
La société est alors le sous-traitant de la collectivité au sens du RGPD.

Quelles sont les obligations des sous-traitants ?

Les obligations suivantes doivent être précisées dans un contrat :

- une obligation de transparence et de traçabilité : vos instructions sur le traitement doivent être recensées par écrit, le sous-traitant doit tenir un registre qui recense les traitements effectués pour votre compte, votre autorisation doit être demandée s'il souhaite faire appel lui-même à un sous-traitant et il doit mettre à votre disposition toutes les informations nécessaires pour démontrer le respect de vos obligations et pour permettre la réalisation d'audits ;
- la prise en compte des principes de protection des données dès la conception et par défaut ;
- une obligation de garantir la sécurité des données traitées ;
- une obligation d'assistance, d'alerte et de conseil (par exemple une procédure de notification des violations de données personnelles doit être fixée).

Comment intégrer les obligations des sous-traitants dans les marchés publics ?

Les marchés publics conclus avec des sous-traitants doivent comprendre les clauses obligatoires prévues par le RGPD (article 28). Pour les marchés en cours avant le 25 mai 2018, des avenants doivent procéder à l'ajout de celles-ci.

Il est recommandé aux acheteurs publics d'insérer dans leurs contrats publics les clauses adéquates en se référant au clausier type élaboré par la CNIL dans le guide « RGPD : Guide du sous-traitant ».

BONNE PRATIQUE

Si les modalités d'exercice des droits ne sont pas prévues clairement dans les clauses, un sous-traitant pourrait demander à facturer l'extraction de données en vue de répondre au droit d'accès d'une personne concernée

POUR ALLER PLUS LOIN

- Guide RGPD pour les sous-traitants
- La Direction des affaires juridiques du ministère de l'Économie, des Finances, de l'Action et des Comptes publics propose des contenus dédiés à la commande publique

COMMENT IDENTIFIER LES TRAITEMENTS À RISQUE ?

La grande majorité des traitements mis en œuvre quotidiennement par les communes ne présentent pas de risques particuliers. Cependant, certaines données ou certains types de traitements, comme par exemple les fichiers gérés par le centre communal d'action sociale, nécessitent une vigilance particulière de votre part.

Quand peut-on parler de traitement à risque ?

Quand vous traitez certains types de données (dites « données sensibles ») :

- révélant l'origine prétendument raciale ou ethnique ;
- portant sur les opinions politiques, philosophiques ou religieuses ;
- relatives à l'appartenance syndicale ;
- concernant la santé (exemple : handicap) ou l'orientation sexuelle ;
- génétiques ou biométriques.

Les données d'infraction ou de condamnation pénale font également l'objet de règles particulières. Ces données – données sensibles et données d'infraction ou de condamnation - ne peuvent être traitées que sous certaines conditions strictement encadrées. Dans l'hypothèse où le traitement envisagé reposerait sur la collecte de ce type de données, prenez tout conseil utile, notamment auprès de votre délégué à la protection des données et auprès de la CNIL.

Quand votre traitement présente de forts enjeux pour la vie privée des personnes, notamment lorsqu'il a pour objet ou pour effet :

- l'évaluation d'aspects personnels (exemple : fichier du CCAS) ;
- une prise de décision automatisée (exemple : attribution d'une prime ou d'une aide sociale) ;
- la surveillance systématique de personnes (exemple : télésurveillance des agents) ;
- le traitement de données sensibles (exemple : médecine préventive, contrôle d'accès biométrique aux cantines scolaires, etc.) ;
- le traitement de données concernant des personnes vulnérables (exemple : les agents des collectivités ou les employés des entreprises sont considérés comme des personnes vulnérables du fait de leur lien de subordination, les enfants) ;
- le traitement à grande échelle de données personnelles ;
- le croisement d'ensembles de données ;
- des usages innovants ou l'application de nouvelles technologies (exemple : reconnaissance faciale) ;
- l'exclusion du bénéfice d'un droit, d'un service ou contrat (exemple : liste de « mauvais payeurs »).

Si vos traitements de données répondent à au moins 2 de ces 9 critères listés ci-dessus, vous devez, en principe, conduire une analyse d'impact sur la protection des données (AIPD), avant de commencer les opérations de traitement.

Cette analyse d'impact sur la vie privée vous permettra d'identifier les risques pour les personnes concernées et de déterminer les mesures appropriées pour protéger leurs données personnelles.

Le délégué à la protection des données pourra conseiller la collectivité sur la réalisation de cette analyse et en vérifier l'exécution.

Dans le cas où il existe un doute, la CNIL recommande la réalisation d'une analyse d'impact.

POUR ALLER PLUS LOIN

- Consultez le dossier complet sur l'analyse d'impact sur la protection des données
- Consultez la liste des traitements pour lesquels une analyse de risque est obligatoire
- Téléchargez le logiciel gratuit pour réaliser une AIPD

ADOPTEZ LES 6 BONS RÉFLEXES

Ces 6 réflexes reprennent des notions ou principes déjà abordés précédemment dans d'autres parties de ce guide mais de façon plus synthétique. Ils peuvent vous être utiles pour sensibiliser les agents au sein de votre collectivité.

1 NE COLLECTEZ QUE LES DONNÉES VRAIMENT NÉCESSAIRES POUR ATTEINDRE VOTRE OBJECTIF

Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.
Le principe de finalité limite la manière dont vous pourrez utiliser ou réutiliser ces données dans le futur et évite la collecte de données « au cas où ».
Le principe de minimisation limite la collecte aux seules données strictement nécessaires à la réalisation de votre objectif.

2 SOYEZ TRANSPARENT

Les administrés doivent conserver la maîtrise des données qui les concernent. Cela suppose qu'ils soient clairement informés de l'utilisation qui sera faite de leurs données dès leur collecte. Les données ne peuvent en aucun cas être collectées à leur insu. Les personnes doivent également être informées de leurs droits et des modalités d'exercice de ces droits.

3 ORGANISEZ ET FACILITEZ L'EXERCICE DES DROITS DES ADMINISTRÉS

Vous devez organiser des modalités permettant aux administrés d'exercer leurs droits et répondre dans les meilleurs délais à ces demandes de consultation ou d'accès, de rectification ou de suppression des données, voire d'opposition, sauf si le traitement répond à une obligation légale (par exemple, un administré ne peut s'opposer à figurer dans un fichier d'état civil). Ces droits doivent pouvoir s'exercer par voie électronique à partir d'une adresse dédiée.

4 FIXEZ DES DURÉES DE CONSERVATION

Vous ne pouvez pas conserver les données indéfiniment.
Elles ne sont conservées en « base active », c'est-à-dire la gestion courante, que le temps strictement nécessaire à la réalisation de l'objectif poursuivi. Elles doivent être par la suite détruites, anonymisées ou archivées dans le respect des obligations légales applicables en matière de conservation des archives publiques.

5 SÉCURISEZ LES DONNÉES ET IDENTIFIEZ LES RISQUES

Vous devez prendre toutes les mesures utiles pour garantir la sécurité des données : sécurité physique ou sécurité informatique, sécurisation des locaux, armoires et postes de travail, gestion stricte des habilitations et droits d'accès informatiques. Cela consiste aussi à s'assurer que seuls les tiers autorisés par des textes ont accès aux données. Ces mesures sont adaptées en fonction de la sensibilité des données ou des risques qui peuvent peser sur les personnes en cas d'incident de sécurité.

6 INSCRIVEZ LA MISE EN CONFORMITÉ DANS UNE DÉMARCHE CONTINUE

La conformité n'est pas gravée dans le marbre et figée.
Elle dépend du bon respect au quotidien par les agents, à tous les niveaux, des principes et mesures mis en œuvre. Vérifiez régulièrement que les traitements n'ont pas évolué, que les procédures et les mesures de sécurité mises en place sont bien respectées et adaptez-les si besoin.

1 COMMUNIQUER DES RENSEIGNEMENTS SUR LES ADMINISTRÉS, À QUI ET À QUELLES CONDITIONS ?

En principe, les collectivités territoriales ne sont pas habilitées à communiquer à des tiers les données personnelles qu'elles détiennent. Néanmoins, vous devez communiquer certaines de ces données à des « tiers autorisés » à leur demande, notamment d'autres autorités publiques ou certains auxiliaires de justice (par exemple les huissiers) quand la loi les y autorise ou l'impose expressément.

À quelles conditions pouvez-vous communiquer des données ?

La communication de renseignements sur les administrés à des « tiers autorisés » est possible dès lors qu'elle est permise par un texte ou nécessaire au respect d'une obligation légale. La multiplicité des acteurs susceptibles d'être considérés comme tiers autorisés ne permet pas d'en proposer une liste exhaustive dans ce guide. En revanche, il est possible de rappeler un certain nombre de principes communs.

Pour chaque demande, vous devez vérifier les éléments ci-dessous :

- la demande de communication doit être écrite et préciser son fondement légal. La collectivité saisie de la requête doit s'assurer de sa conformité aux textes invoqués et peut toujours, en cas de doute, interroger la CNIL (à titre d'exemple une simple demande par téléphone sans vérification particulière ne peut donner lieu à une transmission de données) ;
- elle doit être présentée par une personne ayant qualité pour agir en application du texte fondant le droit de communication (la présentation d'un document formel n'est pas systématiquement obligatoire, celui-ci doit être exigé par le responsable de traitement lorsque le texte le prévoit) ;
- la fréquence et le périmètre de la demande de communication (nature des données, personnes concernées et type de traitement notamment) ne pourront dépasser les limites éventuellement prévues par le texte législatif précité (ex. respect du secret médical) ;
- les modalités de transmission de la demande doivent être sécurisées afin de veiller à la confidentialité des données personnelles (ex. remise en main propre, utilisation du chiffrement en cas de transmission par voie informatique, etc.) ;

- seules les informations strictement nécessaires à la satisfaction de la demande pourront être transmises ;
- la demande et la réponse doivent faire l'objet en interne d'une traçabilité permettant de justifier la transmission en cas d'éventuel contentieux (ex. copie de la demande, identification de l'agent ou du service demandeur, périmètre des données transmises).

Les collectivités peuvent être tentées de diligenter des enquêtes pour répondre à des demandes d'organismes extérieurs, puis de conserver les renseignements obtenus sur leurs administrés.
La CNIL rappelle qu'aucune disposition législative ne permet aux mairies de diligenter de telles enquêtes, même à la demande de tiers autorisés.

Quels sont les exemples de tiers autorisés à obtenir ponctuellement des données personnelles sur des personnes détenues par les collectivités locales ?

Peuvent par exemple obtenir des renseignements relatifs aux administrés :
- les autres administrations autorisées par une disposition législative ou réglementaire, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication à obtenir des données à caractère personnel (par exemple les services en charge de la gestion de l'allocation de solidarité aux personnes âgées pour le contrôle de l'état civil des demandeurs dans le respect des dispositions du code de la sécurité sociale) ;
- la direction générale des finances publiques et celle des douanes pour l'établissement de l'assiette, le contrôle et le recouvrement des impôts ;
- les comptables publics pour le recouvrement des amendes et condamnations pécuniaires qui ne sont pas de nature fiscale et pour le recouvrement des créances des collectivités locales et de leurs établissements publics ;
- les organismes de sécurité sociale, dans le cadre de la lutte contre la fraude, et ceux en charge du RSA ;
- les juges d'instruction, les procureurs de la République et les officiers de police judiciaire agissant dans le cadre de leurs pouvoirs (prévus notamment par le code de procédure pénale) ;
- les huissiers de justice dans le cadre des procédures civiles d'exécution.

Quelles sont les limites au droit de communication des tiers autorisés ?

Dans le cadre des demandes de renseignement, vous ne pouvez pas :
- constituer des fichiers spécifiques dans le but de faciliter la gestion des demandes ;
- utiliser des fichiers que vous ne détenez pas en propre pour répondre aux demandes ;
- collecter, à l'occasion de démarches, des données sans lien avec la finalité du fichier et permettant uniquement de répondre aux demandes.

Comment articuler le droit de communication des tiers autorisés avec le droit d'accès aux documents administratifs ?

Le droit de communication de renseignements concernant des personnes ne doit pas être confondu avec le droit d'accès aux documents administratifs tel que prévu par le code des relations entre le public et l'administration (CRPA) ou par des régimes de communication spéciaux (tel que le régime d'accès aux procès-verbaux du conseil municipal, aux budgets et aux comptes de la commune organisé par le code général des collectivités territoriales).

L'exercice du droit de communication par des tiers autorisés leur permet d'accéder à certaines catégories d'informations dans le cadre d'une procédure légale tandis que le droit d'accès aux documents administratifs permet à toute personne (des particuliers, des entreprises ou d'autres administrations) d'accéder aux documents détenus par l'administration.

Par ailleurs, si les documents administratifs peuvent parfois contenir des informations relatives aux personnes physiques, les dispositions du CRPA protègent certains secrets (par exemple les mentions relatives à la vie privée ou à la santé) qui ne seront communicables qu'aux seuls intéressés.

EXEMPLE DE LA LISTE ÉLECTORALE

Le code électoral permet à tout électeur, tout candidat et tout parti ou groupement politique de prendre communication et copie de la liste électorale, à condition de s'engager à ne pas en faire un usage commercial (utilisation par une agence de publicité, par une entreprise commerciale ou par un agent immobilier en vue de démarches de prospection, par exemple).

Après avoir vérifié que le demandeur entre bien dans une des catégories prévue par la loi, les services municipaux peuvent donc délivrer copie de la liste électorale. Si cette délivrance est faite sur support informatique, cette facilité doit être offerte à tous les demandeurs et facturée de façon identique, si elle implique un coût pour la commune.

La Commission d'accès aux documents administratifs (CADA) est seule compétente pour examiner les questions relatives à l'accès aux listes électorales.

2 COMMENT COMMUNIQUER EN LIGNE ?

Dans un contexte d'évolution des relations entre l'administration et le public et de dématérialisation croissante des services publics, les collectivités sont amenées à être de plus en plus présentes en ligne : sur leur site institutionnel, les réseaux sociaux ou encore en mettant en œuvre des téléservices. Intégrez les bonnes pratiques vous garantissant une présence en ligne en conformité avec le RGPD.

Votre collectivité utilise un site web et des comptes sociaux pour communiquer ?

Vérifiez si vous protégez suffisamment les données personnelles des personnes qui visitent votre site et vos réseaux sociaux.
Le caractère viral des plateformes comme Facebook, Twitter, LinkedIn ou Instagram mérite d'attacher un soin particulier à protéger les données des publics qui vous suivent.

À la clé : moins de risques de piratage et de fuites de données et une réputation en ligne préservée !

Vous avez un site institutionnel ?

Votre site présente votre collectivité, vos activités et vos actualités. Vous proposez un formulaire de contact et éventuellement l'inscription à un bulletin d'information.

Sur un site institutionnel, quelques réflexes de base sont à retenir. Prévoyez au minimum :

- Des « mentions CNIL » en bas des formulaires de contact et d'abonnement. Des modèles sont proposés par la CNIL sur son site web.
- Un moyen de contact pour que les personnes puissent exercer leurs droits par voie électronique.
- Des mentions légales identifiant l'éditeur du site.

POUR EN SAVOIR PLUS

Quelles sont les mentions obligatoires sur un site internet ?

Votre site dépose des cookies ou des traceurs publicitaires ?

Lors de la consultation de votre site web vous pouvez déposer des cookies et autres traceurs sur les outils utilisés par les internautes (ordinateur, tablette, smartphone, etc.) pour analyser leur navigation et leurs habitudes de consultation.

Selon l'objectif du traceur que vous utilisez sur votre site, il est nécessaire, **soit d'informer** l'internaute de son existence (exemple : cookie de session pour un téléservice), **soit d'obtenir son consentement** avant de déposer ou de lire un traceur sur son terminal.

Si votre site utilise des fonctionnalités offertes par d'autres sites (exemples : solutions de statistiques, boutons sociaux, vidéos provenant de plateformes tierces telles que Google, YouTube, Facebook, etc.), **vous devez obtenir le consentement des visiteurs**.

Vous mettez en place des téléservices ?

Un téléservice constitue le « guichet d'accueil » numérique proposé par une collectivité permettant aux usagers d'accomplir certaines démarches ou formalités administratives : demande de permis de construire, inscription au ramassage scolaire, demande de logement social, demande de pièces extraites de l'état civil, etc.

Un site web diffusant des informations sur la commune ou l'inscription à un bulletin municipal ne constitue pas un téléservice.

Les téléservices qui reposent sur la collecte de données personnelles constituent des traitements soumis à la réglementation sur la protection des données personnelles.

La collectivité, et son sous-traitant, doivent respecter **des principes essentiels pour garantir le respect de la vie privée des usagers** :

La pertinence et la proportionnalité
Le téléservice permet de faire transiter des données entre les usagers et les « applications métiers », les informations collectées et enregistrées doivent être pertinentes et strictement nécessaires à l'accomplissement de la démarche concernée.

EXEMPLE DE PERTINENCE ET PROPORTIONNALITÉ

Ne pas imposer une authentification préalable de l'usager si celle-ci n'est pas strictement nécessaire à l'accomplissement d'une démarche ou d'une formalité administrative (la création d'un compte utilisateur pour se voir délivrer la copie d'un acte de mariage) et ne pas recueillir des données
supplémentaires qui ne seraient pas strictement nécessaires (demander le numéro de carte d'identité pour la délivrance d'un extrait d'acte d'état civil).

La pluralité des identifiants
Pour mettre en œuvre un téléservice, la CNIL recommande l'utilisation d'un identifiant par service public proposé.

EXEMPLE D'IDENTIFIANT

Une collectivité qui propose un téléservice permettant d'accomplir différentes démarches administratives devra générer un identifiant par service public : état civil, permis de construire, etc.

Vous pouvez également utiliser le service « FranceConnect » pour gérer l'identification de vos usagers dans les démarches. Ce service est développé par la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) pour simplifier les démarches en ligne.

Le cloisonnement des données des différentes sphères administratives
Le responsable de traitement doit maintenir un cloisonnement des informations personnelles collectées en fonction de la finalité de leur collecte, qui est garanti par une politique de gestion des droits des personnes habilitées à accéder aux données en fonction de leurs missions.

La sécurité des données
Les mesures de sécurité décrites dans le Guide de la sécurité des données personnelles de la CNIL, avec une attention particulière aux questions relatives à la sécurisation des sites web, constituent un socle de bonnes pratiques à respecter pour mettre en œuvre un téléservice.

En matière de téléservice, la CNIL rappelle qu'une analyse de risque de la sécurité des systèmes d'informations est requise pour l'homologation du Référentiel Général de Sécurité (RGS). Des conseils méthodologiques sont disponibles.

BONNE PRATIQUE

Le délégué à la protection des données (DPO) doit être associé à la mise en œuvre des téléservices.

POUR ALLER PLUS LOIN

- Téléservices et protection des données.
- Le service FranceConnect

Les différents téléservices doivent être inscrits au registre des activités de traitement tenu par le responsable du traitement.

3 COMMENT METTRE EN PLACE LES DIFFÉRENTS DISPOSITIFS VIDÉO ?

De plus en plus de collectivités souhaitent mettre en place des dispositifs « vidéo ». Il peut s'agir de vidéoprotection sur la voie publique, de caméras mobiles équipant les agents de police municipale, de dispositifs dans le cadre du stationnement payant ou encore d'enregistrement de séances du conseil municipal.

Quelles sont les règles à respecter si vous installez des caméras de vidéoprotection sur la voie publique ?

Des caméras peuvent être installées sur la voie publique pour prévenir des actes de terrorisme, des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants.

Ces dispositifs peuvent permettre de constater des infractions aux règles de la circulation, réguler les flux de transport, protéger des bâtiments et installations publics et leurs abords, prévenir des risques naturels ou technologiques, faciliter le secours aux personnes ou encore lutter contre les incendies et assurer la sécurité des installations accueillant du public dans les parcs d'attraction.

Comment obtenir l'autorisation préfectorale obligatoire ?
Selon les textes en vigueur (code de la sécurité intérieure), les dispositifs de vidéoprotection installés sur la voie publique doivent faire l'objet d'une demande d'autorisation préalable auprès de la préfecture du département (préfet de police à Paris). L'autorisation est valable 5 ans et renouvelable. Le formulaire peut être retiré auprès des services de la préfecture du département ou téléchargé sur le site web du ministère de l'Intérieur.

Il peut également être rempli en ligne sur le site :
https://www.televideoprotection.interieur.gouv.fr

Qui peut consulter les images ?
Seules les personnes habilitées par l'autorisation préfectorale, et dans le cadre de leurs fonctions (par exemple : les agents du centre de supervision urbain d'une commune), peuvent visionner les images enregistrées. Ces personnes doivent être particulièrement formées et sensibilisées aux règles de mise en œuvre d'un système de vidéoprotection.

Combien de temps les images sont-elles conservées ?
Par principe, la durée de conservation des images ne doit pas excéder un mois.

Comment informer les personnes ?
Les personnes filmées doivent être informées, au moyen de panneaux affichés de façon visible :
- de l'existence du dispositif ;
- de son responsable ;
- des modalités concrètes d'exercice de leur droit d'accès aux enregistrements visuels les concernant.

Ces panneaux sont affichés en permanence dans les lieux concernés et doivent être compréhensibles par tous les publics.

BONNE PRATIQUE

Les caméras installées sur la voie publique ne doivent pas permettre de visualiser l'intérieur des immeubles d'habitation ni, de façon spécifique, leurs entrées. Des procédés de masquage irréversible de ces zones doivent être mis en œuvre et il est nécessaire de régulièrement contrôler leur bon fonctionnement.

Quelles sont les règles à respecter si vous souhaitez équiper les agents de police municipale de caméras mobiles ?

Comment obtenir l'autorisation préfectorale obligatoire ?
Le maire doit présenter au préfet de département une demande d'autorisation pour la mise en œuvre de ce dispositif.
Cette demande d'autorisation doit notamment être accompagnée de l'engagement de conformité dit « RU-065 » effectué auprès de la CNIL.

Dans quels cas les caméras piéton peuvent-elles être utilisées ?
Les enregistrements peuvent être effectués pour trois raisons :
- la prévention des incidents au cours des interventions des agents de la police municipale ;
- le constat des infractions et la poursuite de leurs auteurs par la collecte de preuves ;
- la formation et la pédagogie des agents de police municipale.

Comment les enregistrements sont-ils transmis et combien de temps sont-ils conservés ?
Lorsque les agents de police municipale ont procédé à l'enregistrement d'une intervention, les données enregistrées par les caméras individuelles doivent être transférées sur un support informatique sécurisé dès leur retour au service. Il ne peut pas y avoir d'accès à distance en temps réel. Il ne peut pas y avoir d'accès direct des personnels aux enregistrements auxquels ils procèdent au moyen des caméras individuelles qui leur sont fournies. Les enregistrements doivent être automatiquement effacés au bout de six mois.

Comment les personnes filmées sont-elles informées ?
Les caméras sont portées de façon apparente par les agents et un signal visuel spécifique indique si la caméra enregistre. Le déclenchement de l'enregistrement fait l'objet d'une information des personnes filmées, sauf si les circonstances l'interdisent.

Enfin, une information générale du public est délivrée sur le site web de la commune ou, à défaut, par voie d'affichage en mairie.

Quelles sont les règles à respecter si vous mettez en place un dispositif de lecture automatisée des plaques d'immatriculation (LAPI) dans le cadre du stationnement payant ?

Certaines collectivités recourent à des dispositifs de lecture automatisée de plaques d'immatriculation (LAPI) pour renforcer leurs procédures de contrôle du paiement du stationnement sur voirie.

À quoi les données collectées par ces dispositifs peuvent-elles servir ?
Les données collectées lors du paiement du stationnement doivent servir uniquement à :
- mettre en œuvre les règles de tarification du stationnement posées par la collectivité (suivi et contrôle du paiement, établissement du forfait de post-stationnement, gestion des contestations), à l'exclusion de toute autre fin ;
- réaliser des pré-contrôles du paiement du stationnement en vue de faciliter le travail des agents de contrôle.

Les dispositifs de LAPI ne peuvent collecter que les numéros de plaque d'immatriculation ainsi que l'horodatage et la géolocalisation du véhicule.

Combien de temps les données sont-elles conservées ?
L'immatriculation des véhicules dont le stationnement a fait l'objet d'un paiement doit être supprimé de la base, une fois que le rapprochement avec le serveur de tickets a permis de constater que le véhicule est en règle.

Lorsqu'il s'avère, après rapprochement, qu'il y a absence ou insuffisance de paiement, l'immatriculation des véhicules suspectés de ne pas être en règle devra être supprimée une fois que le constat par l'agent de contrôle est réalisé et que la procédure de régularisation de forfait de post-stationnement (FPS) est, le cas échéant, initiée. En effet, une fois que la procédure de FPS est initiée, les données collectées par le dispositif de LAPI ne sont plus utiles pour la collectivité.

Comment les personnes sont-elles informées ?
Une information des citoyens peut s'effectuer via les horodateurs et le site web des collectivités qui en disposent. Les collectivités peuvent aussi s'assurer de leur bonne diffusion en faisant appel à la presse locale ou aux offices de tourisme.

BONNE PRATIQUE

Dans de nombreux cas, ces dispositifs sont délégués à un prestataire qui réalise les contrôles pour le compte de la collectivité. Il faut donc prévoir lors de la passation du marché les règles relatives à la protection de la vie privée des citoyens et en contrôler la bonne mise en œuvre.

Quelles sont les règles à respecter si vous enregistrez et diffusez les séances des conseils municipaux ?

La diffusion sur internet d'une séance d'un conseil municipal constitue un traitement de données à caractère personnel.

Les élus membres de l'assemblée ne peuvent pas s'opposer à cet enregistrement, qu'il soit audio ou également visuel, dans la mesure où l'article L2121-18 du code général des collectivités territoriales pose le principe de publicité des séances de conseil municipal.

En revanche, les autres personnes, et notamment le public, peuvent s'opposer à être filmées. Elles doivent donc être informées de cet enregistrement.

4 COMMENT CONCILIER LES DURÉES DE CONSERVATION ET LES ARCHIVES ?

Les données à caractère personnel doivent être conservées pour la durée de leur utilité. Mais une même donnée peut avoir parfois plusieurs utilités successives ce qui implique donc des durées de conservation différentes.

Le cycle de vie des données à caractère personnel peut se décomposer en trois phases successives :

- les données sont en cours d'utilisation (dossier « en cours ») ;
- les données sont mises de côté (le dossier est réglé) ;
- les données sont archivées (le dossier est réglé et archivé).

1ère phase : l'utilisation courante ou « base active » qui correspond à la durée d'utilisation courante (DUC)

C'est la durée d'utilisation courante des données ou, autrement dit, la durée nécessaire à la réalisation de l'objectif du traitement (établissement d'un acte d'état civil, gestion d'un bénéficiaire d'une prestation, inscription aux activités périscolaires, etc.).

Durant cette phase, les données sont généralement accessibles quotidiennement aux agents, selon leurs fonctions, au sein des services opérationnels (chargés de l'état civil, du cadastre, des établissements scolaires, etc.).

Il appartient au responsable du fichier de définir cette durée et de la respecter. Lorsqu'il fait appel à des sous-traitants et qu'il n'a pas directement la main sur les données, cette durée doit être définie contractuellement.

EXEMPLE D'UTILISATION COURANTE

À titre de comparaison avec des dossiers papier, il s'agirait d'un classeur accessible au sein d'un bureau placé dans un tiroir fermé à clé quand il n'est pas utilisé.

2e phase : l'archivage intermédiaire qui correspond à la durée d'utilisation administrative (DUA)

Après leur utilisation, les données personnelles peuvent parfois être conservées dans une base d'archivage intermédiaire, distincte de la base active, avec accès restreint, dans la mesure où :
- il existe une obligation légale de conservation de données pendant une durée fixée ;
- en l'absence d'obligation de conservation, ces données présentent néanmoins un intérêt administratif, notamment en cas de contentieux, justifiant de les conserver le temps des règles de prescription/forclusion applicables.

Il ne s'agit pas de conserver l'intégralité des données mais seulement celles qui sont indispensables ou requises par l'obligation légale.

Ces données ne peuvent plus être utilisées par les services opérationnels : elles sont désormais conservées dans un but précis et ne sont accessibles que de façon restreinte.

Le choix du mode technique d'archivage intermédiaire est laissé à l'appréciation du responsable du fichier. Ces données peuvent par exemple être archivées sur un support de conservation dédié avec des accès restreints aux seules personnes ayant un intérêt à en connaître en raison de leurs fonctions (par exemple le service juridique).

La décision de recourir à un archivage intermédiaire doit être prise dès la sélection du sous-traitant pour une gestion optimale.

EXEMPLE D'ARCHIVAGE INTERMÉDIAIRE

À titre de comparaison avec des dossiers papier, il s'agirait d'un classeur rangé dans une salle d'archivage fermée à clé au sein des bureaux.

3e phase : l'archivage définitif

Certaines données et documents présentant un intérêt historique doivent pouvoir être conservées et archivées, dans les conditions fixées par le code du patrimoine.

Cette mission est celle du service des Archives de France. La décision ainsi que les modalités d'archivage définitif des documents des collectivités « sont définies par accord entre le service, l'établissement ou l'organisme intéressé et le service interministériel des Archives de France de la direction générale des patrimoines » (article R. 212-13 du code du patrimoine).

Il est recommandé de les conserver sur un support physique indépendant n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à les consulter (par exemple, la direction des archives lorsqu'elle existe).

Afin de vous renseigner sur vos obligations en matière d'archivage définitif, vous pouvez vous rapprocher des services d'archives concernés (dans la plupart des cas pour les communes les services d'archives départementales) et consulter le site francearchives.fr.

EXEMPLE D'ARCHIVAGE DÉFINITIF

À titre de comparaison avec des dossiers papier, il s'agirait d'un classeur transmis à un organisme d'archivage.

BONNE PRATIQUE

Les différentes durées de conservation doivent être inscrites dans le registre du délégué à la protection des données pour chacun des traitements concernés.

Dans chacune des phases, le responsable du fichier doit prévoir des mesures techniques et organisationnelles pour protéger les données (destruction, perte, altération, diffusion ou accès non autorisés, etc.). Ces mesures doivent assurer un niveau de sécurité approprié aux risques et à la nature des données considérées. Par exemple, les données des destinataires de la lettre d'information de la collectivité n'appellent pas les mêmes mesures que la gestion des prestations sociales octroyées par la collectivité ou le fichier de gestion des activités de la police municipale).

Une personne qui exerce son droit d'accès doit obtenir la communication de l'intégralité des données qui la concernent, qu'elles soient stockées en base active ou archivées.

Quel que soit le type d'archive, la consultation des données archivées doit être tracée.

POUR ALLER PLUS LOIN

Des préconisations relatives au tri et à la conservation des archives produites par les communes et les structures intercommunales ont été faites dans l'instruction DGP/SIAF/2014/006.

Données personnelles
Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Les données personnelles comprennent, entre autres, les noms, prénoms, numéros de téléphone, plaque d'immatriculation, numéro de sécurité sociale, adresse postale ou courriel, la voix ou l'image.
Par contre, des coordonnées d'entreprises (par exemple, l'entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie1@email.fr ») ne sont pas, en principe, des données personnelles.

Traitement de données personnelles
Toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction...)

Finalité du traitement
La finalité du traitement est l'objectif principal du traitement.

Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial. Ce principe de finalité limite la manière dont le responsable de traitement peut utiliser ou réutiliser ces données dans le futur.

Responsable de traitement
Le responsable de traitement est la personne morale (commune, intercommunalité, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser.

Délégué à la protection des données (DPO)
Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme. Sa désignation est obligatoire pour les collectivités. Le délégué peut être, interne, externe ou mutualisé.

Minimisation
Le principe de minimisation prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Sous-traitant
Le sous-traitant est la personne physique ou morale (entreprise ou organisme public) qui traite des données pour le compte d'un autre organisme (le responsable de traitement), dans le cadre d'un service ou d'une prestation. Les sous-traitants ont des obligations concernant les données personnelles, qui doivent être présentes dans le contrat.

Données sensibles
Les données sensibles forment une catégorie particulière des données personnelles.
Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Le RGPD interdit de recueillir ou d'utiliser ces données, sauf dans certains cas qui sont précisément listés.

Registre des activités de traitement

Le registre des activités de traitement permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que le responsable de traitement fait avec les données personnelles. Il permet notamment d'identifier les parties prenantes, les catégories de données traitées ; à quoi servent ces données, qui y accède et à qui elles sont communiquées, combien de temps les données personnelles sont conservées et comment elles sont sécurisées.

Les bases légales

La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de traiter des données personnelles. On peut également parler de « fondement juridique » ou de « base juridique » du traitement.

Six bases légales sont prévues par le RGPD :

- le consentement ;
- le contrat ;
- l'obligation légale ;
- la sauvegarde des intérêts vitaux ;
- l'intérêt public ;
- les intérêts légitimes.

Violation de données

Une violation de la sécurité se caractérise par la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

Analyse d'impact (AIPD)

Une analyse d'impact sur la protection des données est une étude qui doit être menée lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Certification

C'est une procédure par laquelle un organisme d'évaluation externe appelé également tiers certificateur va donner l'assurance écrite qu'une personne, un produit, un processus ou un service est en conformité avec les exigences données dans un référentiel.

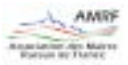
EXEMPLES DE TRAITEMENTS POUVANT ÊTRE MIS EN ŒUVRE PAR LES COLLECTIVITÉS

(liste non exhaustive)

- Alertes de la population en cas de risque naturel ou industriel, plans communaux de sauvegarde
- Cadastre
- Communication politique
- Comptabilité générale
- Conservation d'archives
- Consommations de gaz, d'électricité, d'eau, et redevances d'assainissement facturables
- Contrôles d'accès aux locaux, des horaires et de la restauration administrative
- Dispositifs biométriques de contrôle de l'accès aux locaux sur les lieux de travail (empreintes digitales)
- Dispositifs biométriques pour le contrôle d'accès, la gestion des horaires et de la restauration sur les lieux de travail (contour de la main)
- Enquêtes à des fins statistiques
- Études et actions d'amélioration de l'habitat
- Facturation des consommations d'énergie et d'eau et des redevances d'assainissement, mise en recouvrement de taxes et redevances
- Facturation des services offerts aux parents (gestion des transports et restaurants scolaires, centres aérés et garderies, écoles de musique, crèches municipales)
- Fichier des demandeurs d'emploi
- Géolocalisation des véhicules utilisés par les employés
- Gestion courante des ressources humaines (gestion administrative, mise à disposition d'outils informatiques, organisation du travail, gestion des carrières et de la formation)
- Gestion de l'aide sociale légale et facultative
- Gestion de l'état civil
- Gestion dématérialisée des marchés publics
- Gestion des activités sociales et culturelles par les comités des œuvres sociales ou les délégués du personnel
- Gestion des aires d'accueil des gens du voyage
- Gestion des cimetières
- Gestion des demandes de pièces d'identité et autres documents administratifs
- Gestion des élèves des écoles maternelles, élémentaires, collèges et lycées
- Gestion des fichiers de fournisseurs
- Gestion des listes électorales

- Gestion des ordures ménagères
- Gestion des rémunérations (paie, déclarations fiscales et sociales, tenue des registres obligatoires)
- Gestion foncière, aménagement du territoire
- Information et communication externes
- Logement social
- Lutte contre la vacance des logements
- Observatoire fiscal et aide au recensement des bases d'imposition
- Prêts de livres, disques, documents d'archives publiques
- Recensement de la population (métropole et collectivités d'outre-mer)
- Recouvrement de certaines taxes et redevances (droits de voirie, droits immobiliers, taxes sur le chauffage et éclairage par électricité, taxes et redevances de cimetières, facturation des ordures ménagères...)
- Registres des personnes âgées ou handicapées mis en œuvre dans le cadre du plan d'alerte et d'urgence départemental en cas de risques exceptionnels (« fichiers canicule », grands froids...)
- Rôles des impôts locaux
- Système de vidéosurveillance implanté dans les locaux d'une collectivité non accessibles au public...
- Système de vidéosurveillance installé dans un lieu public ou ouvert au public lorsque les enregistrements sont contenus dans des fichiers
- Systèmes d'information géographique (SIG) ou autres traitements associant données cadastrales, d'urbanisme et/ou des - SPANC (services publics de l'assainissement non collectif)
- Téléservices
- Télétransmission des actes soumis au contrôle de légalité
- Utilisation des services téléphoniques sur les lieux de travail
- Validation des attestations d'accueil

Ce guide a été réalisé par la CNIL avec le concours de :



Commission Nationale
de l'Informatique et des Libertés
3, Place de Fontenoy - TSA 80715
75 334 PARIS CEDEX 07
Tél. 01 53 73 22 22

www.cnil.fr
https://twitter.com/cnil
https://fr-fr.facebook.com/

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr