

Guide pratique RGPD

Pour les collectivités territoriales

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Version 2026

Table des matières

3 Avant-propos

5 Qu'implique le respect du RGPD pour les collectivités ?
7 Quel est le rôle de la CNIL ?

8 Protection des données personnelles : de quoi parle-t-on ?

8 Qu'est-ce qu'une donnée personnelle ?
9 Qu'est-ce qu'un « traitement de données personnelles » ?

12 Désignez un délégué à la protection des données (DPO)

12 Les missions
13 Les compétences
13 Le statut
15 Les différentes formes de délégués
17 La désignation

19 Comment assurer votre conformité avec un plan d'action en 4 étapes ?

19 Étape 1 – Recensez les traitements
21 Étape 2 – Faites le tri dans les données
23 Étape 3 – Respectez les droits des administrés
25 Étape 4 – Sécurisez les données
28 Que faire en cas de violation de données ?

29 Comment travailler avec un sous-traitant ?

31 Comment identifier les traitements à risque ?

33 Adoptez les 6 bons réflexes

35 Mettre en place des dispositifs vidéo conformes

45 Lexique RGPD

47 Exemples de traitements pouvant être mis en œuvre par les collectivités

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 vidéoprotection, 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.

Aussi, afin d'accompagner les collectivités territoriales dans leur mise en conformité au RGPD, la CNIL a élaboré un guide pratique. 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.

En complément, la CNIL met à disposition de nombreuses ressources sur son site web ainsi qu'un cours en ligne gratuit sur le RGPD, dont un module spécifique pour les collectivités.

Toujours soucieuse d'accompagner toutes les collectivités dans leur mise en conformité au RGPD, la CNIL continue de dialoguer avec les différents acteurs territoriaux. À ce titre, 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) avec lesquels la CNIL échangent régulièrement et qui avaient accepté de relire et d'enrichir la première version de ce guide.

Pour aller plus loin

- **Dossier collectivités territoriales**
  www.cnil.fr/fr/collectivites-territoriales
- **MOOC de la CNIL, formation en ligne gratuite sur le RGPD, comprenant un module dédié aux collectivités territoriales.**
  https://atelier-rgpd.cnil.fr

Qu'implique le respect du RGPD pour les collectivités ?

Avec le RGPD, 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. Depuis l'entrée en application du RGPD, les déclarations à la CNIL sont supprimées.

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.

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.

Pour aller plus loin

- **La responsabilité des acteurs dans le cadre de la commande publique (guide)**
  www.cnil.fr/sites/default/files/2024-03/guide_responsabilite_des_acteurs_dans_le_cadre_de_la_commande_publique.pdf

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 françaises. 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.

Ses missions :

- 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. Elle s'appuie en particulier sur 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 par exemple).

Pour aller plus loin

- **Mieux connaitre la chaîne répressive de la CNIL**
  www.cnil.fr/fr/la-chaine-repressive-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 ».

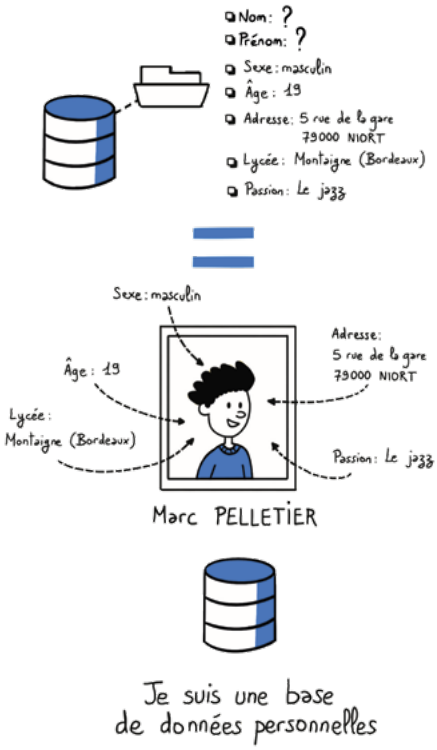
Une personne physique peut être identifiée :

- 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).

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.



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 : 19 ans, garçon, classe Terminale, redoublement dans tel lycée de telle ville.

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

Un « traitement de données personnelles » est une opération, ou un 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.

Exemple de traitement

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 « au cas où », lorsque l'on ne sait pas quel usage en faire. Par ailleurs 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 public, 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 ?**
  www.cnil.fr/fr/cnil-direct/question/reglement-europeen-le-consentement-est-il-obligatoire

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. Celui-ci 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 responsable 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 page 45.**
- **Une liste non exhaustive des traitements de données le plus souvent mis en œuvre par les collectivités vous est proposée en annexe page 47.**

Désignez un délégué à la protection des données (DPO)

Il est obligatoire pour 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.). Pour les petites communes ayant peu de moyens, il est possible de faire appel à un DPO mutualisé entre différents responsables de traitement.

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.


Le délégué informe et conseille la collectivité

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 ?


Le délégué contrôle le respect du réglement

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.


Le délégué est le point de contact pour l'exercice des droits

Pour aller plus loin

- **Le guide pratique RGPD – Délégués à la protection des données**
www.cnil.fr/sites/default/files/atoms/files/guide_pratique_rgpd_-_delegues_a_la_protection_des_donnees.pdf

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

La CNIL met à disposition un cours en ligne gratuit (MOOC) sur le site **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. Il comprend un module dédié aux collectivités territoriales.

Pour aller plus loin

- **Consulter les référentiels de compétences du DPO**
  www.cnil.fr/fr/la-certification-des-competences-du-delegue-la-protection-des-donnees

Le statut

Le délégué doit pouvoir :

- **rendre compte au niveau le plus élevé de la hiérarchie ;**
  Quelle que soit effectivement sa position précise dans l'organigramme, le délégué doit avoir accès et doit pouvoir rendre compte effectivement 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.

! Attention

Dans les petites collectivités, les secrétaires de mairie sont souvent pressentis pour occuper la fonction de DPO. Or, leur désignation apparaît problématique et se heurte souvent 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'intérêts, 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 leurs preuves dans d'autres organismes.



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 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.

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.

Quelle que soit la forme choisie, il existe des solutions adaptées à chaque type de commune. N'hésitez pas à vous rapprocher des différentes associations (AMF, AMRF, Départements de France…), des partenaires locaux (centre de gestion, EPCI, OPSN …) ou institutionnelles (direction générale des collectivités locales, ANCT, préfectures…) pour connaître l'offre proposée dans vos territoires.

La désignation

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

Avant de désigner en ligne votre délégué à la protection des données, vérifiez qu'il dispose du statut, des compétences et des moyens nécessaires à l'exercice de ses missions. Assurez-vous en particulier que ces **3 conditions sont réunies** :

1. **Le délégué détient les compétences requises**
2. **Le délégué dispose de moyens suffisants**
3. **Le délégué a la capacité d'agir en toute indépendance**

La désignation d'un DPO, son remplacement ou la déclaration de la fin de ses missions se font exclusivement depuis le téléservice dédié :

https://connexion.pro.cnil.fr/login

Il existe **3 formulaires** en fonction de ce que vous souhaitez faire.

Formulaire « Désigner un DPO »

- Désigner un DPO (personne physique ou morale) pour la première fois ou suite à une fin de mission.

Formulaire « Mettre fin à la désignation ou remplacer mon DPO »

- Mettre fin à la mission de votre DPO sans procéder à son remplacement.
- Remplacer votre DPO actuel par un nouveau délégué (personne physique ou morale).

Formulaire « Mettre à jour la désignation d'un DPO »

- Modifier le contact et les coordonnées de l'organisme renseignés au moment de la désignation (point d'attention : ce formulaire permet également de modifier les coordonnées du DPO. Si vous souhaitez modifier l'identité du DPO, vous devez utiliser le formulaire « remplacer votre DPO »).

Pour aller plus loin

- **FAQ - Gérer vos désignations de DPO**
  www.cnil.fr/fr/faq-gerer-vos-designations-de-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 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) ;
- l**es 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.**
  www.cnil.fr/fr/RGPD-le-registre-des-activites-de-traitement

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 mesure 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.



Étape 3 – Respectez les droits des administrés

Le nombre toujours croissant de plaintes adressées à la CNIL témoigne de la sensibilité accrue des personnes concernant la protection de leurs données personnelles. En 2025, une grande partie des plaintes reçues concernait l'exercice des droits, notamment le droit d'accès (demande d'accès à des images de vidéoprotection), le droit d'opposition (absence d'information du droit d'opposition à la conservation des empreintes digitales dans le fichier des titres électroniques sécurisés (TES) lors d'un renouvellement de pièce d'identité), ou le droit d'effacement (demande d'effacement de données contenues dans des documents municipaux diffusés en ligne par erreur).

Pour aller plus loin

- **Le rapport annuel 2025**
  https://www.cnil.fr/sites/default/files/2026-07/rapport_annuel_2025.pdf

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).



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**
  www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation
- **Respecter les droits des personnes**
  www.cnil.fr/fr/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 :

1. l'accès illégitime à des données ;
2. leur modification non désirée ;
3. 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.

Focus sur les violations

12 %

du volume total de violations reçues par la CNIL proviennent des collectivités territoriales

1 182

violations reçues en 2025

+ 50 %

des violations sont des attaques sur les systèmes d'information et sur les messageries

1/4

de ces violations sont consécutives à une erreur d'un utilisateur ou à un dysfonctionnement informatique.



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.

Pour aller plus loin

- **Le guide *Obligations et responsabilités des collectivités locales en matière de cybersécurité* (Cybermalveillance.gouv.fr – CNIL)**
  www.cybermalveillance.gouv.fr/medias/2022/07/220630_FranceRelance_Guide-1-1.pdf
- **L'étude sur la maturité cyber des collectivités de Cybermalveillance.gouv.fr**
  www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/etude-cybersecurite-collectivites-moins-de-25000-habitants
- **Mémento sur la cybersécurité pour les communes rurales de l'AMF**
  https://www.amf.asso.fr/arbo-cybersecurite/496

Réduire les risques avec l'authentification multifacteur

En plus du mot de passe, il est désormais essentiel de mettre en place une authentification multifacteur (également appelée « MFA » ou « double authentification »).

L'authentification multifacteur : de quoi parlons-nous ?

L'authentification multifacteur (MFA) est un processus qui ajoute une vérification pour confirmer l'identité de la personne qui se connecte, en plus du mot de passe.

Généralement, l'étape supplémentaire permettant une confirmation peut s'appuyer sur :

- quelque chose que vous connaissez comme un mot de passe, une clé d'accès, un code PIN ou une question de sécurité ;
- quelque chose que vous possédez, par exemple un appareil mobile, une carte à puce ou un jeton matériel ;
- ou quelque chose qui vous définit telles que des données biométriques (empreinte digitale, reconnaissance faciale ou vocale).

La MFA permet de réduire le risque d'usurpation de compte, dans l'éventualité où l'identifiant et le mot de passe auraient été volés.

Les vérifications à effectuer

- ☑ Les accès aux locaux sont-ils sécurisés ?
- ☑ Les armoires et coffres-forts sont-ils fermés à clé 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 ?
- ☑ Une authentification multi facteur est-elle mise en place ?
- ☑ 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**
  www.cnil.fr/fr/mots-de-passe-des-recommandations-de-securite-minimales-pour-les-entreprises-et-les-particuliers

- **Guide sécurité des données personnelles sur le site web de la CNIL**
  www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

- **Le site** Messervices.cyber.gouv.fr

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 ».

Attention

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 :

www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Si ces risques sont élevés pour ces personnes, vous devrez les en informer.

Pour aller plus loin

- **Violations de données personnelles : les règles à suivre**
  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**
  www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants
- **Guide -** ***La responsabilité des acteurs dans le cadre de la commande publique***
  www.cnil.fr/sites/cnil/files/2024-03/guide_responsabilite_des_acteurs_dans_le_cadre_de_la_commande_publique.pdf
- **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 :** www.economie.gouv.fr/daj

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 des 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**
  www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-pia
- **Consultez la liste des traitements pour lesquels une analyse de risque est obligatoire**
  www.cnil.fr/sites/default/files/atoms/files/liste-traitements-avec-aipd-requise-v2.pdf
- **Téléchargez le logiciel gratuit pour réaliser une AIPD**
  www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

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.

Mettre en place des dispositifs vidéo conformes

Les caméras de vidéoprotection sur la voie publique.

Les caméras peuvent être installées notamment 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 aussi permettre de constater des infractions aux règles de la circulation et au dépôt d'ordures sauvage, de réguler les flux de transport, de protéger des bâtiments et installations publics et leurs abords, de prévenir des risques naturels ou technologiques, de faciliter le secours de personnes ou encore de lutter contre les incendies.

Qui peut filmer la voie publique ?

En principe, **seules les autorités publique**s, telles que les mairies, peuvent filmer la voie publique. Les écoles ou musées, par exemple, peuvent également filmer les abords immédiats de leurs installations dans les lieux susceptibles d'être exposés à des actes de terrorisme.

Attention

Les caméras ne doivent pas permettre de voir l'intérieur des immeubles d'habitation, ni 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.





Comment obtenir l'autorisation préfectorale obligatoire ?

Les dispositifs de vidéoprotection sur voie publique doivent être **autorisés préalablement par la préfecture du département (préfet de police à Paris)**.

L'autorisation est valable **5 ans et est 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 à l'adresse **www.televideoprotection.interieur.gouv.fr**

Qui peut consulter les images enregistrées ?

Uniquement les personnes habilitées par l'autorisation préfectorale, et dans le cadre de leurs fonctions. Elles doivent être formées et sensibilisées aux règles de mise en œuvre d'un système de vidéoprotection. **Les personnes filmées ont un droit d'accès** aux images sur lesquelles elles apparaissent, sous réserve du respect des droits des tiers, ce qui peut nécessiter le masquage ou le « floutage » d'une partie des images.

Combien de temps conserver les images ?

L'arrêté préfectoral d'autorisation précise la durée de conservation des données. Cette durée doit être adaptée à l'objectif du dispositif : en règle générale, quelques jours suffisent pour effectuer des vérifications. Par principe, cette durée de conservation ne peut pas excéder un mois.

Comment informer les personnes filmées ?

Les personnes filmées doivent en être informées **par des panneaux affichés en permanence et de façon visible, dans les lieux concernés**. Un certain nombre de mentions obligatoires doivent figurer sur ces panneaux.

Des informations complémentaires sont également à publier sur un autre support, par exemple le site web de la mairie.

Pour aller plus loin

- **La vidéosurveillance - vidéoprotection sur la voie publique sur cnil.fr**
  www.cnil.fr/fr/la-videoprotection

Vos administrés souhaitent installer des caméras pour sécuriser leur domicile ?

Les particuliers ne peuvent filmer que **l'intérieur de leur propriété** : l'intérieur de la maison ou de l'appartement, le jardin, le chemin d'accès privé. **Ils n'ont pas le droit de filmer la voie publique**, y compris pour assurer la sécurité de leur véhicule garé devant leur domicile.





La vidéoverbalisation

Un agent verbalisateur peut consulter en direct les images de caméras de vidéoprotection depuis le centre de supervision urbaine (CSU).

Ce dispositif permet de verbaliser, à distance, certaines infractions aux règles de la circulation (par exemple, l'usage du téléphone et le port d'écouteurs au volant, le stationnement gênant) et les infractions relatives au dépôt d'ordures sauvage.

Attention

En l'état actuel de la réglementation, les communes **ne sont pas autorisées à conserver la photographie du véhicule et de sa plaque d'immatriculation** à des fins de preuve. La constatation de l'infraction doit se faire en temps réel avec l'établissement du PV depuis le CSU.

Les caméras individuelles ou « piéton »

Les agents (police municipale, sapeurs-pompiers et gardes-champêtres) peuvent en être équipés pour l'enregistrement audiovisuel de leurs interventions en cas d'incident. Ces dispositifs peuvent permettre de prévenir et constater des infractions.

- L'emploi des caméras individuelles est soumis à autorisation du préfet ;
- l'existence d'une convention de coordination des interventions de la police municipale et des Forces de Sécurité Intérieure (FSI) est nécessaire ;
- la retransmission en temps réel des images des caméras individuelles à leur poste de commandement est possible lorsque leur sécurité ou celle des biens et des personnes est menacée.

Combien de temps conserver les images ?

Les durées de conservation sont variables mais **ne peuvent pas excéder 6 mois**.

Comment informer les personnes filmées ?

Les caméras sont portées **de façon apparente** et un **signal visuel spécifique** indique si la caméra enregistre. **L'enregistrement est déclenché par l'agent qui en informe les personnes filmées**, sauf si les circonstances l'interdisent (par exemple, l'état d'ébriété de la personne).

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

Peut-on filmer dans un domicile privé ?

Oui, une intervention peut avoir lieu dans un domicile privé pour certains agents (la police municipale et les services d'incendie et de secours notamment). Dans ce cas, la collecte d'images doit être strictement limitée.

Les drones

La police municipale ne peut pas recourir à des drones dans l'exercice de ses missions de prévention des atteintes à l'ordre public.

En revanche, **les agents environnementaux des communes et les sapeurs-pompiers peuvent y recourir** afin d'assurer le secours aux personnes, la prévention de risques naturels ou technologiques (incendies, niveaux d'eaux et crues, activité volcanique etc.).
Quelles données peuvent être collectées ?

Les images captées par les caméras installées sur des drones, avec le jour, la plage horaire d'enregistrement, le lieu ou la zone géographique concernée. Néanmoins, le déclenchement de l'enregistrement ne peut intervenir que dans des conditions strictes. Le son n'est pas capté.

Comment informer les personnes filmées ?

Elles doivent être informées, sauf urgence. Cette information peut se faire par tout moyen. Il est recommandé de la délivrer **sur le lieu de l'opération en cours via des dispositifs sonores ou physiques**, comme des barrières.

Peut-on filmer dans un domicile privé et selon quelles conditions ?

Oui. Néanmoins, seuls les services d'incendie et de secours y sont autorisés lorsque cela est strictement nécessaire aux finalités poursuivies. Les images non supprimées sont conservées **au maximum pendant 7 jours**.

Pour les agents de l'État (police et gendarmerie nationales, militaires et douanes), lorsque l'interruption de l'enregistrement à l'intérieur d'un domicile ou son entrée n'a pu avoir lieu, celui-ci est **supprimé à l'issue de l'intervention et au plus tard dans un délai de 48 heures**. Le besoin de signalement à l'autorité judiciaire peut constituer une exception.

Les dispositifs LAPI

Le LAPI désigne tout algorithme permettant la **l**ecture **a**utomatisée d'une **p**laque d'**i**mmatriculation. Il peut être fixe ou mobile et être utilisé dans différents cas.

Le LAPI utilisé à des fins de sécurité

Les collectivités peuvent-elles financer ces dispositifs LAPI ?

Oui, via les conventions de prestation de matériel passées avec le ministère de l'Intérieur. Les conditions sont strictes : aucun accès aux données du dispositif LAPI par la police munipale, ni transfert de responsabilité vers cette dernière.

Seules les douanes, la police et la gendarmerie nationales peuvent installer des LAPI à **des fins de sécurité des personnes et des biens** (terrorisme, criminalité organisée, vol de véhicules, etc.).
La police municipale n'est pas autorisée à utiliser un dispositif LAPI permettant de collecter, pour la constitution préalable d'une base de données, l'ensemble des plaques des véhicules filmées par les caméras de vidéoprotection dans le seul but de répondre à d'éventuelles réquisitions judiciaires.

Le LAPI utilisé pour le stationnement payant

Certaines collectivités recourent à des dispositifs LAPI pour **renforcer leurs procédures de contrôle du paiement du stationnement sur voirie**. Ces dispositifs de gestion et de suivi du stationnement, dépénalisés depuis 2018, sont soumis au règlement général sur la protection des données (RGPD).

Le constat de l'absence ou de l'insuffisance de paiement doit toujours être réalisé par un agent chargé des contrôles (sur place ou à distance, dans un délai raisonnable après le pré-contrôle LAPI).

Quelles sont les données collectées et pour quelles durées de conservation ?

Les dispositifs LAPI peuvent collecter les numéros de plaques d'immatriculation, l'horodatage et la géolocalisation des véhicules. Ces données sont supprimées automatiquement dès constat de la régularité du stationnement.

Il est possible de collecter des photographies de l'environnement du véhicule en cause, sous certaines conditions (dont le floutage irréversible et sans intervention humaine des plaques d'immatriculation des véhicules à proximité, à l'exception de celle du véhicule concernée), seulement pour :

- la constatation de l'irrégularité à distance par l'agent en charge du contrôle. Les photographies sont supprimées dès constat que le véhicule est en règle ;
- la gestion des contestations des administrés, dans la limite des délais de recours applicables.

Les personnes peuvent-elles exercer leur droit d'opposition ?

En principe oui, mais les collectivités ont la possibilité d'exclure le droit d'opposition par délibération de leur conseil municipal, pour le motif d'intérêt général de bonne gestion et du contrôle du stationnement payant sur la voie publique.

Comment les personnes sont-elles informées ?

Par les horodateurs et le site web des collectivités qui en disposent. Elles peuvent aussi s'assurer de la bonne information des personnes en faisant appel à la presse locale ou aux offices de tourisme.

Le LAPI utilisé pour la circulation des véhicules sur la voie publique

Comment ces dispositifs peuvent-ils être utilisés ?

Les collectivités peuvent recourir à des dispositifs LAPI afin de verbaliser le non-respect des règles de circulation liées aux **voies de circulation réservées** aux véhicules de transport en commun, aux taxis, aux véhicules utilisés pour le covoiturage, ou aux véhicules à très faibles émissions.

Combien de temps les données sont-elles conservées ?

Les données sont **supprimées dès qu'il est constaté que le véhicule est en règle**. À défaut, elles peuvent être conservées **8 jours ouvrés maximum** à compter de leur collecte. En cas d'infraction, les photographies du véhicule, les données relatives à l'infraction et le numéro d'identification de la détection peuvent être conservés 3 ans maximum à titre de preuve pour les besoins de la procédure.

Les caméras embarquées

Comment ces dispositifs peuvent-ils être utilisés et comment les personnes sont-elles informées ?

Des caméras peuvent être installées dans les véhicules utilisés par les services d'incendie et de secours. Elles permettent un enregistrement des interventions à des fins de sécurité, uniquement sur la voie publique ou les lieux ouverts au public en cas d'incident. Le son ne peut pas être collecté. Le public est informé par **une signalétique spécifique apposée sur le moyen de transport, sauf dérogations. L'enregistrement est déclenché par l'agent et un signal visuel ou sonore spécifique** indique si un enregistrement est en cours, sauf urgence ou si les circonstances de l'intervention l'interdisent (par exemple, les véhicules banalisés).

Caméras augmentées, reconnaissance faciale : de quoi parle-t-on ?

Les caméras augmentées

Une caméra augmentée est constituée d'un logiciel de traitement automatisé de l'image couplé à une caméra. Elle permet de filmer et d'analyser les personnes, objets, véhicules ou autres éléments présents à l'image, afin d'en déduire certaines informations, et données personnelles.

La CNIL considère que le code de la sécurité intérieure (CSI) ne permet pas, à lui seul, d'utiliser de
telles technologies sur les caméras de vidéoprotection. L'utilisation d'un tel dispositif sur la voie
publique **doit, la plupart du temps, être encadrée par une loi ou un décret**.

La **loi sur les Jeux Olympiques et Paralympiques 2024** a autorisé, par exemple, à titre expérimental jusqu'au 31 mars 2025, le recours aux caméras augmentées pour assurer la sécurité de certains grands évènements sportifs, récréatifs et culturels, pour certains cas d'usage (détection de la présence d'une personne au sol à la suite d'une chute, d'un départ de feu, etc.) sous réserve de respecter certaines conditions précises.

Cette expérimentation vient d'être prolongée jusqu'en 2030 et élargie aux bâtiments et lieux ouverts au public en cas de menace terroriste ou de risque d'atteinte grave à la sécurité des personnes (loi « RIPOST » n°2026-798).

Il est aussi déjà possible de mettre en œuvre ces dispositifs à des fins statistiques, par exemple pour mesurer le nombre de vélos circulant sur la voie publique à des fins d'aménagement ultérieur du territoire.

Pour aller plus loin

- **Les caméras « augmentées » ou algorithmiques dans l'espace public**
  www.cnil.fr/fr/cameras-augmentees-espaces-publics



La reconnaissance faciale

La reconnaissance faciale implique d'utiliser des données biométriques. Il s'agit de données sensibles dont la collecte et l'utilisation sont, sauf exceptions, **interdites par le RGPD**.

De manière générale, la reconnaissance faciale doit être prévue par une loi, ou un décret, après avis de la CNIL. Dans tous les cas, tout projet d'y recourir devra faire l'objet d'une analyse d'impact relative à la protection des données (AIPD).

Attention

Avant de mettre en œuvre les dispositifs ci-dessous, **il faudra effectuer une déclaration** (www.cnil.fr/fr/declarer-un-fichier) **de conformité en ligne auprès de la CNIL à l'un des règlements uniques (RU) suivants** :

Vidéoprotection

RU-074

(Traitements mis en œuvre par une autorité compétente et pour le compte de l'État).

Vidéoverbalisation

RU-009

RU-074

Caméra embarquée

RU-080

Drones

Agents de la sécurité civile

RU-067

Caméras piétons

Police Municipale **RU-065**

Sapeurs-Pompiers **RU-066**

Gardes-Champêtres **RU-069**

Annexes

Lexique RGPD



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
75 007 Paris
Tél. 01 53 73 22 22

www.cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS