CYBERACTU'

Le magazine du service « Protection des données » du Centre de gestion du Gard

Juillet 2025

Petites communes et RGPD
Une conformité sous contrainte

Dossier page 16

Le point archives : Les documents numériques

Les conseils du DPO : Les caméras piéton

Cybersécurité : Les bénéfices économiques du RGPD

CDG 30 CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD

CENTRE DE GESTION
DU GARD

Contactez-nous

04 66 38 86 86
cdg30@cdg30.fr

CDG 30 CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD

Contactez-nous

CDG 30 CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD

Contactez-nous

CDG 30 CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD

Contactez-nous

CDG 30 CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD

SOMMAIRE

ÉDITO

Dans un monde où la digitalisation des services publics s'accélère, la cybersécurité est devenue un enjeu incontournable pour les collectivités territoriales. Dans ce numéro, notre dossier spécial se concentre sur ces petites collectivités, souvent démunies face à la complexité de la mise en conformité avec le RGPD. Comment ces structures, aux moyens parfois limités, peuvent-elles garantir la protection des données personnelles tout en maintenant la qualité de leurs services ? Quelles stratégies et quels accompagnements sont à leur disposition pour relever ce défi ? À travers des retours d'expérience, des analyses et des solutions pratiques, ce numéro vise à éclairer les élus et les agents territoriaux sur les bonnes pratiques à adopter. La cybersécurité n'est pas seulement une obligation légale : elle est une opportunité pour renforcer la confiance des citoyens envers leurs institutions. Construisons ensemble un avenir numérique plus sûr pour nos territoires !

Pierre BONANNI – Ana VEGA

Sidonie HOURS – Sarah ROMAN

Contacts

Service « Protection des données »

☎ : 04 66 38 86 86

@ : dpd@cdg30.fr

CDG 30 CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD

RENTRÉE SCOLAIRE : PROTÉGER LES DONNÉES PERSONNELLES LORS DE L'AFFICHAGE DES LISTES DE CLASSES

À l'approche de la rentrée scolaire, l'affichage des listes de classes est une pratique courante dans les écoles pour informer élèves et parents. Cependant, cette démarche, bien que pratique, soulève des enjeux de cybersécurité et de protection des données personnelles, comme le rappelle la CNIL. Voici les bonnes pratiques à adopter pour concilier organisation et respect du RGPD.

Des objectifs éducatifs et organisationnels

Publier les listes de classes permet de faciliter l'organisation des familles et d'aider les élèves à se projeter dans leur nouvelle année scolaire. Cependant, lorsque ces listes sont affichées à l'extérieur des établissements, elles peuvent révéler des informations sensibles, comme le nom, le prénom ou la localisation d'un élève pendant l'année scolaire. Dans certains cas, cela peut poser des risques, notamment en cas de harcèlement ou de situations familiales complexes, comme une déchéance de l'autorité parentale.

Les recommandations de la CNIL

Pour limiter ces risques, la CNIL propose plusieurs bonnes pratiques :

- **Informer en amont :** Les parents doivent être prévenus de l'affichage des listes et avoir la possibilité de s'y opposer. Les coordonnées du délégué à la protection des données (DPD) ou du responsable de l'établissement doivent être communiquées.
- **Minimisation des données :** Seules les informations strictement nécessaires (prénom, initiale du nom, classe) doivent apparaître. Les données comme la date de naissance ou des prénoms supplémentaires ne doivent être incluses qu'en cas d'homonymie.
- **Vigilance face aux fraudes :** La CNIL met en garde contre les plateformes frauduleuses qui promettent un accès anticipé aux listes de classes, souvent dans le but de collecter des données personnelles.

Un traitement encadré par le RGPD

L'affichage des listes constitue un traitement de données personnelles, soumis à la loi Informatique et Libertés et au RGPD. Les établissements doivent s'appuyer sur les conseils de leur DPD pour garantir la conformité. En cas d'opposition d'un parent, les modalités doivent être claires et accessibles, bien que l'exercice de ce droit puisse être complexe si l'affichage est déjà effectué.

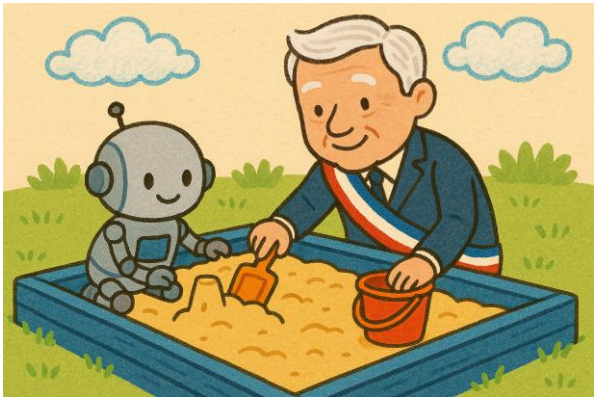
Protéger la vie privée des élèves tout en assurant une rentrée fluide est un équilibre à trouver. En adoptant ces bonnes pratiques, les établissements scolaires peuvent limiter les risques liés à la diffusion des données personnelles et renforcer la confiance des familles. Pour plus d'informations, consultez les ressources de la CNIL.

BILAN DU BAC À SABLE IA : ACCOMPAGNER LES SERVICES PUBLICS DANS L'INNOVATION RESPONSABLE

La CNIL a récemment publié le bilan de son dispositif « bac à sable IA », lancé en 2023 pour soutenir les acteurs publics dans le développement de solutions d'intelligence artificielle conformes au RGPD. Ce programme, axé sur la protection des données personnelles, a permis d'accompagner plusieurs projets innovants dans le secteur public, tout en renforçant la cybersécurité et la confiance numérique.

Un cadre pour innover en respectant le RGPD

Le bac à sable IA vise à aider les organismes publics à concevoir des outils d'IA respectueux des droits des citoyens. En 2023, cinq projets ont été sélectionnés, couvrant des domaines variés comme la lutte contre la fraude, la gestion des données administratives ou l'amélioration des services aux usagers. Ces initiatives ont bénéficié d'un accompagnement personnalisé par les experts de la CNIL, garantissant la conformité avec les exigences européennes en matière de protection des données.



Des enseignements clés pour la cybersécurité

Le bilan met en lumière plusieurs bonnes pratiques :

- **Minimisation des données :** Les projets doivent limiter la collecte de données personnelles au strict nécessaire, réduisant ainsi les risques d'exposition en cas de cyberattaque.
- **Transparence et consentement :** Les usagers doivent être informés de l'utilisation de leurs données et, lorsque nécessaire, donner leur consentement explicite.
- **Sécurisation des systèmes :** Les outils d'IA doivent intégrer des mesures robustes de cybersécurité, comme le chiffrement et des audits réguliers, pour protéger les données sensibles.

Un impact concret pour les services publics

Parmi les projets accompagnés, certains ont permis d'optimiser les processus administratifs tout en renforçant la protection des données. Par exemple, des solutions basées sur l'IA ont amélioré la détection de fraudes tout en garantissant l'anonymisation des données traitées. Ces avancées montrent qu'innovation et respect de la vie privée peuvent aller de pair.

Vers une IA éthique et sécurisée

Ce premier bilan du bac à sable IA confirme l'engagement de la CNIL à promouvoir une intelligence artificielle éthique et sécurisée dans le secteur public. En 2025, le dispositif se poursuivra avec de nouveaux appels à projets, ouverts aux acteurs publics souhaitant innover tout en respectant les principes du RGPD. Pour en savoir plus, rendez-vous sur le site de la CNIL.

Nouveau module du MOOC de la CNIL : travail et données personnelles

La CNIL enrichit son MOOC dédié à la protection des données avec un nouveau module consacré à la gestion des données personnelles dans le cadre professionnel. Disponible gratuitement, ce module s'adresse aux agents, employeurs et professionnels des RH, et met l'accent sur les enjeux de cybersécurité et de conformité au RGPD en milieu de travail.

L'ATELIER RGPD

Un contenu adapté au monde du travail

Ce module explore les défis liés à la collecte, au traitement et à la sécurisation des données personnelles dans l'environnement professionnel. Il aborde des thématiques clés telles que :

- **La collecte de données RH :** Comment limiter les informations collectées (CV, évaluations, données de santé) au strict nécessaire, conformément au principe de minimisation du RGPD.
- **La surveillance des agents :** Les règles encadrant les outils de contrôle (vidéosurveillance, géolocalisation, monitoring des emails) pour respecter la vie privée.
- **La cybersécurité au travail :** Les bonnes pratiques pour protéger les données contre les cyberattaques, comme le chiffrement des fichiers sensibles ou la sensibilisation des employés aux risques de phishing.

Un apprentissage interactif et accessible

Conçu pour être accessible à tous, ce module propose des vidéos, quiz et cas pratiques pour mieux comprendre les obligations légales et les droits des agents. Par exemple, il explique comment un agent peut exercer son droit d'accès à ses données ou s'opposer à un traitement excessif. Les employeurs y trouveront également des conseils pour mettre en place des politiques de protection des données conformes.

Un enjeu majeur pour les collectivités

Dans un contexte où les violations de données sont en hausse, ce module souligne l'importance de former les équipes aux bonnes pratiques de cybersécurité. Une gestion responsable des données personnelles renforce non seulement la conformité, mais aussi la confiance des agents et des usagers.

Comment y accéder ?

Le MOOC est disponible sur la plateforme de la CNIL, sans prérequis. Ce nouvel ajout s'inscrit dans une démarche d'éducation numérique, essentielle pour naviguer dans un monde où les données sont omniprésentes. Pour découvrir ce module et approfondir vos connaissances, rendez-vous sur le site de la CNIL.


FRAUDE FIGHTCLUB

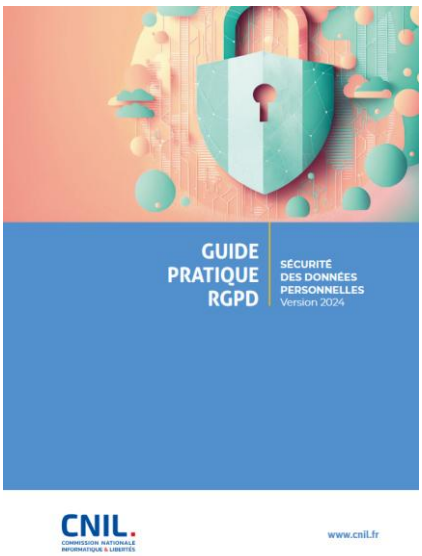
PROTÉGEZ VOS PROCHES CONTRE LA FRAUDE

REJOIGNEZ LE @FRAUDEFIGHTCLUB SUR INSTAGRAM

Avec le soutien de

LES CONTRÔLES DE LA CNIL EN 2025 : PRIORITÉS ET ENJEUX POUR LA CYBERSÉCURITÉ

La CNIL a dévoilé ses priorités pour les contrôles de conformité au RGPD en 2025, mettant l'accent sur des thématiques clés liées à la protection des données et à la cybersécurité. Ces contrôles, qui concernent aussi bien les entreprises que les organismes publics, visent à garantir le respect des droits des citoyens tout en répondant aux défis numériques actuels.



En 2025, la CNIL concentrera son effort sur :

- **La collecte de données par le biais des applications mobiles**
- **La cybersécurité des collectivités territoriales**
- **Les données traitées par l'administration pénitentiaire**
- **Le respect du droit à l'effacement**

Un renforcement de la cybersécurité

Les contrôles mettront un accent particulier sur les mesures de sécurité mises en place par les collectivités. Cela inclut l'utilisation du chiffrement, la gestion des accès et la formation des employés pour prévenir les cyberattaques, comme les ransomwares ou les fuites de données. La CNIL vérifiera également si les responsables de traitement informent correctement les utilisateurs et respectent leurs droits (accès, opposition, suppression). L'application des mesures recommandées par la CNIL dans son guide sur la sécurité des données est donc requise !

Une approche pédagogique et répressive

Si la CNIL privilégie l'accompagnement pour encourager la conformité, elle n'hésitera pas à sanctionner les manquements graves. En 2024, plusieurs amendes ont été prononcées pour des violations liées à l'absence de consentement ou à des failles de sécurité. En 2025, elle poursuivra cette double approche, tout en sensibilisant les acteurs aux bonnes pratiques.

Les contrôles de la CNIL en 2025 soulignent l'importance d'une gestion rigoureuse des données personnelles dans un monde numérique en constante évolution. Les organisations sont invitées à anticiper ces vérifications en renforçant leur cybersécurité et en se conformant au RGPD. Pour plus de détails, consultez le site de la CNIL.

Rapport annuel 2024 de la CNIL : un bilan au cœur des enjeux de cybersécurité

Le rapport annuel 2024 de la CNIL dresse un panorama de ses actions pour protéger les données personnelles dans un contexte numérique en pleine mutation. Avec une attention particulière portée à la cybersécurité, la CNIL a renforcé ses efforts pour garantir la conformité au RGPD et répondre aux défis posés par l'essor des technologies comme l'IA.

En 2024, la CNIL a enregistré une augmentation significative de ses interventions. Plus de 400 contrôles ont été réalisés, ciblant notamment les applications de santé, les réseaux sociaux et les pratiques de collecte de données par l'IA.

Près de 16 000 plaintes ont été déposées, souvent liées à des violations de données ou à des publicités ciblées non consenties.

Enfin, 45 sanctions ont été prononcées, pour un total de plusieurs millions d'euros d'amendes, principalement pour des failles de sécurité ou des manquements au consentement.

Le rapport met en lumière l'importance de mesures robustes pour protéger les données personnelles. Les cyberattaques, comme les ransomwares, restent une menace majeure. La CNIL a ainsi sensibilisé les organisations à l'adoption de pratiques telles que le chiffrement des données sensibles, la mise en place de politiques d'accès strictes ou encore la formation des agents pour contrer les risques de phishing.

La protection des données des mineurs, notamment sur les réseaux sociaux et les plateformes éducatives, a été une priorité, avec des recommandations pour limiter les collectes abusives.

Au-delà des sanctions, la CNIL a poursuivi sa mission pédagogique en publiant des guides, en lançant de nouveaux modules de son MOOC et en accompagnant des projets innovants via son « bac à sable IA ». Ces initiatives visent à aider les entreprises et les administrations à intégrer la protection des données dès la conception de leurs outils.

Le rapport 2024 de la CNIL illustre son rôle central dans la défense des droits numériques face aux enjeux de cybersécurité. En combinant contrôles, sanctions et sensibilisation, elle encourage une gestion responsable des données personnelles. Pour consulter le rapport complet et découvrir ses recommandations, rendez-vous sur le site de la CNIL.

Nos félicitations du premier semestre 2025 pour la commune de Chamborigaud !

Située au nord de notre département, la commune de Chamborigaud (886 habitants), connue pour son viaduc ferroviaire impressionnant et ses paysages cévenols relaxants, a adhéré au service protection des données au cours de l'année 2019.

Ayant une volonté de se mettre rapidement en conformité, la commune a ainsi entamé de nombreux changements.

Suite à l'arrivée d'une nouvelle Secrétaire générale, un nouvel audit de sécurité a ainsi été mené en juin 2025. Celui-ci a démontré que la commune remplissait toutes les exigences de sécurité préconisées par la CNIL !

Nous ne pouvons que féliciter l'équipe pour son engagement envers la protection des données de ses citoyens et l'exemple qu'ils peuvent inspirer pour les autres collectivités gardoises.

Viaduc de Chamborigaud

CYBERSÉCURITÉ : LES BIENFAITS DU RGPD EN MATIÈRE ÉCONOMIQUE ET D'ATTRACTIVITÉ DU TERRITOIRE

Le RGPD, souvent perçu comme une contrainte, offre des avantages économiques non négligeables pour les collectivités territoriales, comme le souligne la CNIL dans un récent article. En renforçant la cybersécurité, il permet aux communes, départements et régions de protéger leurs données tout en optimisant leurs ressources et leur image.

Renforcer la confiance des citoyens

En respectant le RGPD, les collectivités garantissent une gestion sécurisée des données personnelles des administrés (état civil, services sociaux, inscriptions scolaires). Des mesures comme le chiffrement ou des accès restreints réduisent les risques de cyberattaques, telles que les ransomwares, qui peuvent paralyser les services publics. Cette transparence et cette sécurité renforcent la confiance des citoyens, un atout précieux pour la légitimité des institutions locales.

Réduire les coûts des incidents et des cyberattaques

Les violations de données peuvent engendrer des coûts importants : amendes, frais juridiques, perturbations des services. En 2024, les collectivités conformes au RGPD ont évité des pertes financières majeures en prévenant les fuites de données ou en limitant leur impact grâce à des notifications rapides, comme l'exige le règlement. Investir dans des formations ou des audits de cybersécurité s'avère bien moins onéreux que gérer une crise.

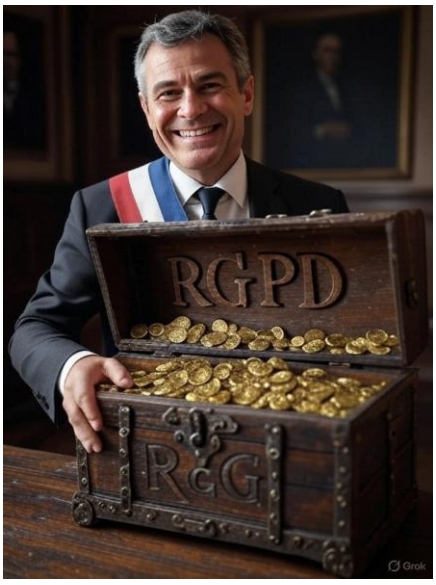
Un levier pour l'attractivité territoriale

Une collectivité qui protège efficacement les données personnelles de leurs usagers gagne en attractivité. Les entreprises, notamment dans les secteurs technologiques ou de la santé, privilégient les territoires respectueux des normes RGPD pour leurs implantations. De plus, une conformité rigoureuse facilite l'accès à des financements européens ou nationaux, souvent conditionnés à des standards élevés de protection des données.

L'accompagnement de la CNIL

La CNIL soutient les collectivités avec des outils pratiques, comme des guides et des modules de formation (MOOC), pour intégrer le RGPD dès la conception des projets numériques (privacy by design). Ces diverses ressources permettent d'optimiser les budgets en évitant des coûts de mise en conformité tardive tout en renforçant la résilience face aux cybermenaces.

Pour les collectivités territoriales, le RGPD est un investissement stratégique. En améliorant la cybersécurité, il protège contre les risques financiers, renforce la confiance citoyenne et booste l'attractivité. Pour découvrir les outils et recommandations de la CNIL, rendez-vous sur leur site.



Les décisions des autorités chargées de la protection des données

29 avril 2025 : Italie – 30 000 €

La CNIL italienne a infligé une amende de 30 000 euros à l'Ordine degli psicologi della Lombardia, l'Ordre des psychologues de la région de Lombardie. Le responsable du traitement a subi une violation de données **en raison de l'insuffisance des mesures techniques et organisationnelles** visant à prévenir les violations de données, et notamment l'absence de double authentification, ou encore de mise à jour des serveurs.

23 avril 2025 : Suède – 9 200 €

L'autorité suédoise de protection de la vie privée a infligé une amende de 9 200 euros au *Diskrimineringsombudsmannen*, le Médiateur suédois pour l'intégration. Le responsable du traitement n'a pas pris les mesures de sécurité suffisantes, ce qui a entraîné la divulgation non autorisée de données sensibles.

15 avril : Pologne – 7 800 €

L'autorité polonaise de protection des données a infligé une amende de 7 800 euros à un salon funéraire de la commune de Pulawy (Est de la Pologne), qui n'a pas mis en place une sécurité organisationnelle et technique appropriée pour les données personnelles dans les documents relatifs aux enterrements. Il y a eu une perte de données du fait de ces négligences.

24 MARS 2025 : ESPAGNE – 2 000 €

L'autorité espagnole de protection des données a infligé une sanction de 2 000 euros à l'encontre du parti politique catalan « *Independents de Vallromanes* ».

Le parti est accusé d'avoir **publié sur les réseaux sociaux** une décision de justice incluant des données personnelles n'étant pas nécessaires compte tenu du message que souhaitait faire passer le parti politique dans sa publication, allant à l'encontre du principe de minimisation des données.

24 MARS 2025 : POLOGNE – 17 600 €

L'autorité polonaise de protection des données a infligé une amende de 17 600 euros au commandant en chef de la police polonaise. Au cours d'une conférence de presse, le commandant en chef de la police a divulgué les données personnelles et médicales d'une personne qui avait subi un avortement qui avait fait l'objet d'une enquête de la part de la police polonaise. La divulgation était suffisamment précise pour permettre à un tiers d'identifier la personne. Il en a résulté un risque spécifique de discrimination, de perte de réputation et de perte de contrôle sur leurs propres données.

17 MARS 2025 : POLOGNE – 23 500 €

L'autorité polonaise de protection des données a infligé une amende de 23 500 euros au Ministre polonais des affaires numériques. Le Ministre a traité illégalement des données personnelles de citoyens polonais dans une base de données et les a utilisé pour effectuer de la propagande électorale pour son propre parti, dans le cadre du vote postal prévu lors de l'élection présidentielle de 2020.

17 mars 2025 : Pologne – 6 300 000 €

En lien avec la sanction du Ministre des affaires numériques (voir page précédente), l'autorité polonaise de la protection des données a infligé une lourde amende à la Poste polonaise pour avoir utilisé les données d'une base nationale de données pour envoyer de la propagande électorale pour le compte du parti du Ministre dans le cadre de l'organisation des élections présidentielles de 2020.

13 mars 2025 : Italie – 50 000 €

La CNIL italienne a infligé une amende de 50 000 euros à l'agence régionale pour le développement et les services dans le domaine de l'agriculture. Le responsable du traitement a traité les données géographiques de ses agents sans base juridique suffisante. Le responsable du traitement n'a pas non plus fourni suffisamment d'informations dans ses documents internes concernant la protection des données, a enfreint les principes de base de la légalité, de l'équité, de la transparence et de la limitation des finalités et n'a pas procédé à une évaluation de l'impact sur la protection des données.

21 janvier 2025 : Lituanie – 9 000 €

L'agence lituanienne de protection des données a infligé une amende de 9 000 euros au service de l'emploi relevant du Ministère de la sécurité sociale et du travail de la République de Lituanie. À la suite d'une fuite de données faisant intervenir les données de 292 usagers, l'autorité a constaté que le Ministère n'avait pas mis en œuvre des mesures techniques et organisationnelles suffisantes pour prévenir de tels incidents.

Et si l'Histoire avait été bouleversée par de mauvaises pratiques cyber?

Christophe Colomb, Napoléon, Marie-Antoinette...

Pour (re)découvrir l'Histoire et adopter les bons réflexes,
rendez-vous sur **cybermois.gouv.fr**
du 1er au 31 octobre 2025

Visuels réalisés avec l'IA

CYBER MOIS
CYBERMOIS.GOUV.FR

NÉCROLOGIE

LES DERNIÈRES VICTIMES DE CYBERATTAQUES*

Mathieu
21 février 2025

Loon-Plage
04 avril 2025

Bain de Bretagne
24 février 2025

Métropole du Grand-Paris
07 mars 2025

Département des Hauts-de-Seine
19 mai 2025

Lorient
10 mars 2025

Ostheim
17 mars 2025

Merlevenez
27 mars 2025

Thaon les Vosges
08 avril 2025

Ardon
16 avril 2025

Département de la Côte d'Or
12 mars 2025

SDIS 86
20 février 2025

Berson
21 février 2025

Pont de Claix
1er février 2025

Centre d'Urgence Cyber
0 800 71 13 13
Soutenu par RÉPUBLIQUE FRANÇAISE
Numéro gratuit
Cyber'Occ délivre un service gratuit d'assistance, en cas de cyber-incident, aux TPE, PME, ETI, collectivités et associations d'Occitanie.
csirt@cyberocc.fr

** Sur les six derniers mois*

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

3 GESTES POUR SÉCURISER VOTRE ESPACE NUMÉRIQUE

Premier ministre
Secrétariat d'État chargé du numérique
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique
CHAMBRE DE COMMERCE ET D'INDUSTRIE
cpme CONFÉDÉRATION DES PME
ORDRE DES EXPERTS-COMPTABLES

PETITES COMMUNES ET RGPD : UNE CONFORMITÉ SOUS CONTRAINTE, PORTÉE PAR LES DPO MUTUALISÉS

Depuis l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) le 25 mai 2018, toutes les organisations, publiques comme privées, sont tenues de se conformer à des exigences strictes en matière de protection des données personnelles. Ce cadre réglementaire, bien que conçu pour garantir la sécurité et la confidentialité des données des citoyens européens, s'applique de manière universelle, sans distinction de taille ou de moyens. En France, les petites communes, y compris celles de moins de 200 habitants, n'échappent pas à cette obligation. Avec environ 35 000 communes en France, dont près de 20 % comptent moins de 200 habitants selon l'Insee (données 2023), ces collectivités rurales se retrouvent face à un défi de taille : comment assurer une mise en conformité au RGPD avec des ressources humaines et financières souvent limitées, et un accès restreint aux outils numériques modernes ?

Centre-bourg de Rochefourchat – Source : France 3 Auvergne Rhône-Alpes

Dans ces petites structures, où le secrétariat de mairie est parfois assuré par un élu bénévole ou un employé à temps partiel, la gestion des données personnelles – qu'il s'agisse des registres d'état civil, des listes électorales ou des demandes de subventions – repose sur des moyens souvent rudimentaires. Par exemple, une commune comme Rochefourchat, dans la Drôme, qui compte officiellement un seul habitant (Insee, 2023), doit théoriquement respecter les mêmes obligations qu'une métropole comme Lyon. Cette situation particulière soulève une problématique centrale : par quels procédés des collectivités aux moyens parfois dérisoires peuvent-elles répondre aux exigences techniques et juridiques du RGPD, telles que la tenue d'un registre des traitements, la sécurisation des données ou la gestion des demandes de droits de ses citoyens ?

Face à ce paradoxe, les Délégués à la Protection des Données (DPO) mutualisés, souvent portés par les centres de gestion de la fonction publique territoriale, émergent comme une solution clé. Ces structures, comme le Centre de Gestion de la Fonction Publique Territoriale (CDG) du Gard, qui accompagne plus de 140 collectivités locales dans leurs démarches RGPD, permettent de mutualiser les compétences et les coûts.

En mettant à disposition des DPO formés, ces centres offrent un appui indispensable pour cartographier les traitements de données, former les agents communaux et répondre aux éventuelles inspections de la CNIL. Cette mutualisation, bien que perfectible, apparaît comme un levier stratégique pour concilier les contraintes des petites communes avec les impératifs de conformité, garantissant ainsi la protection

des données des citoyens tout en allégeant le fardeau administratif des élus locaux.

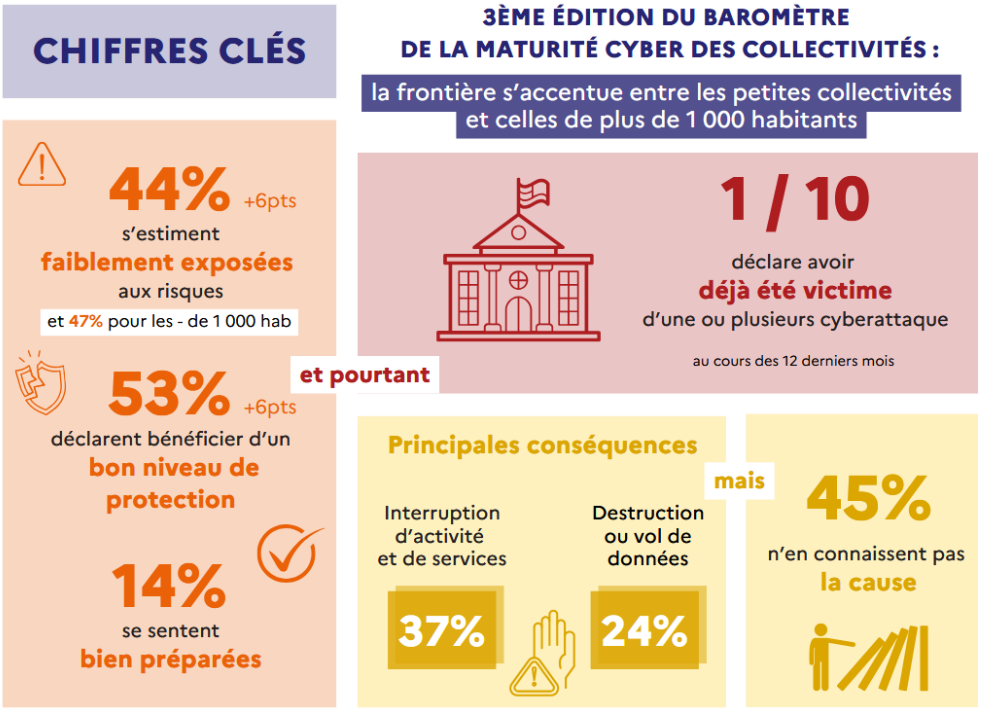
Un cadre juridique unique, des réalités très diverses

Le RGPD, entré en vigueur le 25 mai 2018, impose un cadre juridique uniforme à toutes les organisations et administrations traitant des données personnelles au sein de l'Union européenne, qu'il s'agisse de multinationales, d'associations ou de collectivités territoriales. En France, cela inclut les 34 955 communes recensées par l'Insee en 2023, des métropoles comme Paris aux hameaux de quelques dizaines d'habitants, comme Causse-Bégon, dans notre département (25 habitants, Insee 2022). Cette application universelle, bien que garante d'une égalité de protection pour les citoyens, ignore les disparités criantes en termes de moyens humains, financiers et techniques entre les collectivités, plaçant les petites communes rurales face à des défis disproportionnés pour atteindre une totale conformité.

Les obligations imposées par le RGPD sont claires et exigeantes. Ainsi, toute collectivité, quelle que soit sa taille, doit désigner un DPO, chargé de superviser la conformité. Elle doit également recenser les traitements de données personnelles dans un registre dédié, garantir leur sécurisation (par exemple, via le chiffrement ou des sauvegardes sécurisées), informer les personnes concernées de leurs droits (accès, rectification, oubli, suppression, etc.) et mettre en place des procédures pour gérer les violations de données dans un délai de 72 heures auprès de la CNIL. Selon un rapport de la CNIL de 2024, 85 % des collectivités territoriales françaises avaient désigné un DPO à fin 2023, mais seules 60 % des communes de moins de 500 habitants disposaient d'un registre des traitements à jour, signe d'une mise en œuvre inégale.

Dans les petites communes rurales, souvent définies comme celles de moins de 200 habitants, ces obligations se heurtent à des réalités bien spécifiques. Les traitements de données, bien que peu nombreux, sont souvent sensibles. Par exemple, une commune comme Vaudelnay (Maine-et-Loire, 1 200 habitants) gère des données d'état civil (naissances, mariages, décès), des informations scolaires pour les inscriptions ou les transports, des données électorales pour les scrutins, ou encore des données liées à l'urbanisme pour les permis de construire. Ces données, bien que limitées en volume, nécessitent une vigilance accrue en raison de leur caractère personnel et parfois confidentiel. Une erreur dans la gestion d'un registre d'état civil ou une fuite de données électorales peut avoir des conséquences graves, tant sur le plan juridique que pour la confiance des administrés.

Pourtant, ces communes opèrent souvent avec des moyens humains et techniques très restreints. Dans de nombreuses collectivités de moins de 200 habitants, comme Saint-Germain-de-Pasquier (Eure, 130 habitants), l'administration repose sur un unique agent administratif polyvalent, souvent à temps partiel, ou sur des élus bénévoles. Selon une étude de l'Association des Maires de France (AMF, 2022), 68 % des communes de moins de 500 habitants n'ont pas d'agent dédié à la gestion numérique, et 45 % utilisent



Source : cybermalveillance.gouv.fr

encore des fichiers papier ou des tableurs non sécurisés pour gérer leurs données. Cette faible culture numérique, couplée à un manque de formation, rend la compréhension des exigences du RGPD particulièrement ardue. Par exemple, dans la commune de Fontanès-de-Sault (Aude, 12 habitants), le maire, qui cumule les fonctions administratives, a déclaré en 2023 lors d'une enquête de l'AMF : « *Le RGPD, c'est un jargon incompréhensible pour nous. On n'a ni le temps ni les moyens de s'en occuper*. »

En outre, l'accès limité aux outils numériques modernes aggrave ces difficultés. Selon le rapport 2024 de la Direction Générale des Collectivités Locales (DGCL), 30 % des communes de moins de 200 habitants ne disposent pas d'une connexion Internet haut débit fiable, ce qui complique la mise en œuvre de solutions comme les logiciels de gestion sécurisée des données.

Cette fracture numérique, combinée à un budget communal souvent inférieur à 50 000 euros par an (DGCL, 2023), limite les investissements dans des équipements ou des formations adaptés. Ainsi, tandis que le RGPD impose un cadre juridique rigoureux et universel, les réalités des petites communes rurales révèlent un fossé entre les exigences réglementaires et les capacités opérationnelles, rendant la mise en conformité particulièrement complexe sans un accompagnement structuré.

Le DPO mutualisé : une réponse adaptée, mais sous tension

Face aux défis posés par la conformité au RGPD dans les petites communes rurales, où les moyens humains et financiers sont souvent limités, le modèle du DPO mutualisé s'impose comme une solution pragmatique.

Porté principalement par les CDG, ce dispositif permet à plusieurs collectivités de partager les services d'un même DPO, offrant ainsi un accompagnement spécialisé à des structures qui n'auraient pas les ressources pour recruter un expert en interne. En 2024, selon la FNCDG, plus de 70 % des communes de moins de 500 habitants en France s'appuyaient sur un DPO mutualisé via leur CDG, illustrant l'ampleur de ce modèle. Par exemple, le CDG de l'Allier accompagne près de 300 collectivités, dont des villages comme Limoise (150 habitants), dans leurs démarches de mise en conformité.

Le recours à un DPO mutualisé présente plusieurs atouts majeurs pour les petites communes. Tout d'abord, il garantit l'accès à une expertise juridique et technique pointue, souvent hors de portée pour des collectivités aux budgets restreints. Les DPO des CDG, formés aux subtilités du RGPD et des réglementations nationales, maîtrisent les obligations légales et savent traduire ces exigences en actions concrètes. Par exemple, dans la commune de Saint-Cirgues (Haute-Loire, 120 habitants), le DPO du CDG 43 a aidé en 2023 à identifier et sécuriser les traitements de données liés aux inscriptions scolaires, un domaine où la mairie manquait de compétences internes.

Ensuite, ce modèle permet une externalisation et une gestion des responsabilités complexes. La gestion des violations de données, la rédaction de mentions d'information ou la réponse aux demandes des citoyens (comme le droit d'accès) sont des tâches

chronophages et techniques. En les déléguant à un DPO mutualisé, les élus et agents communaux peuvent se concentrer sur leurs missions quotidiennes. Selon un rapport de la CNIL (2024), les collectivités ayant un DPO mutualisé sont 40 % moins susceptibles de faire l'objet de sanctions pour non-conformité que celles sans accompagnement structuré.

Enfin, la mutualisation des coûts rend ce dispositif financièrement viable. Recruter un DPO à temps plein peut coûter entre 40 000 et 60 000 euros par an (selon les estimations de l'AMF, 2023), une somme prohibitive pour une commune comme Montfroc (Drôme, 80 habitants), dont le budget annuel ne dépasse pas 45 000 euros (DGCL, 2023). En revanche, les services d'un DPO mutualisé, facturés via une cotisation annuelle au CDG (souvent entre 500 et 2 000 euros selon la taille de la commune), permettent de répartir les frais entre plusieurs collectivités, rendant la conformité plus accessible.

Malgré ses atouts, le modèle du DPO mutualisé n'est pas exempt de contraintes, qui mettent le dispositif sous tension. Premièrement, la charge de travail des DPO est souvent considérable. Un seul DPO peut être amené à suivre des dizaines, voire des centaines de collectivités. Par exemple, le CDG de la Creuse, qui couvre 250 communes, dispose de seulement deux DPO pour l'ensemble de ses adhérents (rapport d'activité CDG 23, 2024). Cette surcharge limite le temps consacré à chaque commune, rendant parfois l'accompagnement beaucoup moins approfondi qu'espéré. Dans des villages comme La Villedieu (Creuse, 50 habitants), les élus déplorent un suivi épisodique, souvent réduit à des échanges par courriel.

Deuxièmement, la visibilité limitée sur le terrain constitue un frein. Les DPO mutualisés, basés dans les locaux des CDG, réalisent la majorité de leurs missions à distance, via des outils numériques ou des réunions virtuelles. Cette approche, bien que pratique, peut compliquer la compréhension des enjeux locaux. Par exemple, à Saint-Priest-la-Marche (Cher, 200 habitants), le maire a signalé en 2023 que les recommandations du DPO, bien que pertinentes, semblaient déconnectées des réalités matérielles de la commune, comme l'absence de connexion Internet fiable pour mettre en place des outils de sauvegarde sécurisés.

Enfin, la difficulté à adapter le discours et les outils à chaque contexte local représente un défi. Les petites communes présentent des niveaux de maturité numérique et des besoins très variables. Un DPO mutualisé peut proposer des modèles de registres ou de mentions légales standardisés, mais ces outils ne sont pas toujours adaptés aux spécificités d'une commune. Par exemple, une commune comme Roquesteron (Alpes-Maritimes, 190 habitants), qui gère des données liées à des activités touristiques saisonnières, peut nécessiter des conseils spécifiques que les solutions génériques peinent à couvrir. Selon une enquête de l'AMF de 2022, 55 % des maires de communes de moins de 200 habitants estiment que les outils proposés par les DPO mutualisés sont « trop techniques » ou « mal adaptés » à leur quotidien. Ainsi, bien que le modèle du DPO mutualisé offre une réponse structurée et économiquement viable aux exigences du RGPD, il reste confronté à des tensions structurelles qui limitent son efficacité. Ces défis soulignent la nécessité d'un accompagnement encore plus personnalisé et de moyens renforcés pour les CDG, afin de garantir une conformité durable dans les petites communes.

Une conformité progressive, entre théorie et pragmatisme

Dans les petites communes rurales, la mise en conformité avec le RGPD s'apparente à un marathon plutôt qu'à un sprint. Avec des ressources limitées et une faible culture numérique, ces collectivités, souvent de moins de 200 habitants, progressent lentement mais sûrement vers une gestion plus sécurisée des données personnelles. Selon une étude de l'Association des Maires de France (AMF, 2023), 65 % des communes de moins de 500 habitants ont amorcé des démarches de conformité RGPD, mais seules 40 % estiment être pleinement conformes, signe d'un processus graduel. Par exemple, la commune de La Bâtie-des-Fonds (Drôme, 10 habitants), qui s'appuie sur le Centre de Gestion de la Drôme (CDG 26), a mis plus de deux ans pour établir un registre des traitements de base, illustrant la lenteur mais aussi la persévérance de ces petites structures.

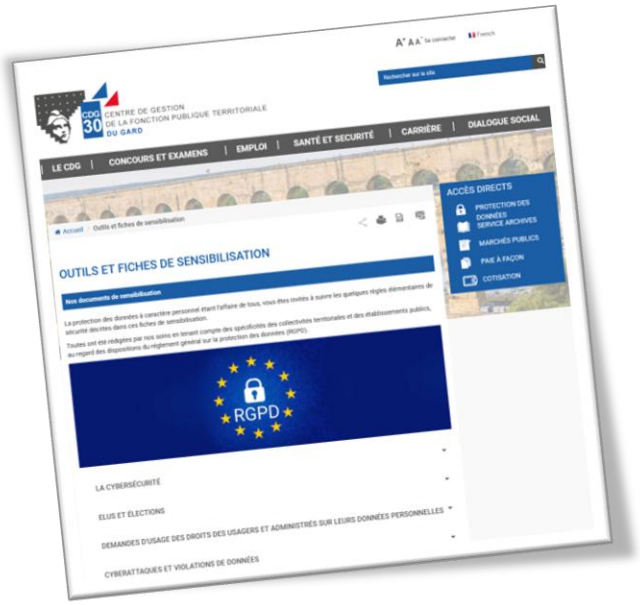
Pour faciliter cette progression, les petites communes s'appuient largement sur des modèles-types proposés par les CDG ou la CNIL. Ces outils, comme les registres préremplis, les fiches de traitement ou les mentions d'information standardisées, permettent de poser des bases solides sans exiger une expertise juridique approfondie.

Par exemple, la CNIL a publié en 2022 un kit RGPD spécifique aux collectivités locales, téléchargé plus de 12 000 fois par des communes de moins de 1 000 habitants (rapport d'activité CNIL, 2024). Dans la commune de Saint-Maurice-de-Rotherens (Savoie, 180 habitants), le CDG 73 a fourni en 2023 un modèle de registre adapté aux traitements courants (état civil, élections, urbanisme), permettant à la mairie de formaliser ses obligations en quelques mois.

Ces modèles, bien que standardisés, sont très bien adaptés aux petites communes, où les traitements de données sont peu nombreux mais sensibles. Ils réduisent le temps et les coûts nécessaires à la mise en conformité, tout en garantissant une certaine homogénéité dans les pratiques. Selon la FNCDG, près de 80 % des communes accompagnées par un CDG utilisent ces outils comme point de départ, ce qui a permis à des villages comme Saint-Julien-de-l'Herms (Isère, 140 habitants) de se doter d'un cadre RGPD minimal sans engager de dépenses importantes.

Malgré ces avancées, la conformité RGPD est souvent perçue comme une charge administrative supplémentaire dans les petites communes, où le personnel est réduit à l'extrême. Dans des collectivités comme Montbrun (Lozère, 70 habitants), où un seul agent administratif à temps partiel gère l'ensemble des tâches communales, l'ajout de démarches RGPD – comme la rédaction d'un registre ou la formation à la cybersécurité – peut sembler écrasant. L'enquête de l'AMF de 2022 révèle que 72 % des maires de communes de moins de 200 habitants considèrent le RGPD comme « *une grande contrainte bureaucratique* », et 60 % estiment manquer de temps pour s'y consacrer pleinement. Cette perception est exacerbée par la polyvalence des agents, qui jonglent entre des missions variées, de la gestion des cimetières à l'organisation des élections.

Cette charge est d'autant plus pesante que les bénéfices du RGPD ne sont pas toujours évidents pour les élus et les agents. Par exemple, à La Chapelle-Geneste (Haute-Loire, 110 habitants), le maire a déclaré en 2023 lors d'une réunion avec le CDG 43 : « *On comprend l'importance de protéger les données, mais pour une commune comme la nôtre, où tout le monde se connaît, ça semble démesuré*. » Cette réticence reflète un décalage entre les exigences réglementaires européennes et les réalités d'un tissu communal rural, où les pratiques administratives restent souvent informelles. Dans ce contexte, le DPO mutualisé joue un rôle crucial en adaptant les exigences du RGPD aux contraintes du terrain, sans pour autant les vider de leur substance. Cette démarche pragmatique consiste à prioriser les actions à fort impact, comme la sécurisation des données sensibles ou la sensibilisation des agents, tout en accompagnant les communes dans une montée en compétences progressive. Par exemple, à Saint-Front (Charente, 150 habitants), le DPO du CDG 16



Le site internet du CDG 30 propose lui-même de nombreux modèles et outils adaptés à une utilisation par les petites collectivités

a conseillé en 2024 de commencer par verrouiller les ordinateurs communaux avec des mots de passe et de former l'agent administratif à repérer les tentatives d'hameçonnage, avant d'aborder des tâches plus complexes comme l'analyse d'impact.

Cette approche nécessite un équilibre délicat : le DPO doit simplifier le discours et les outils sans compromettre les obligations légales. Selon un rapport de la CNIL de 2024, les DPO mutualisés ont permis à 75 % de l'ensemble petites communes accompagnées de respecter les exigences minimales du RGPD, mais 20 % d'entre elles restent en retard sur des aspects comme la gestion des violations de données, faute d'outils adaptés. Pour pallier ces écarts, certains CDG organisent des ateliers pratiques pour les élus, où des scénarios concrets (par exemple, une fuite de données électorales) sont simulés pour rendre le RGPD plus tangible.

Ainsi, la conformité RGPD dans les petites communes rurales s'inscrit dans une dynamique progressive, mêlant recours à des outils standardisés, efforts d'adaptation des DPO et gestion d'une charge administrative souvent mal accueillie. Ce pragmatisme, bien que perfectible, permet à ces collectivités de s'aligner peu à peu sur les exigences réglementaires, tout en préservant leurs capacités opérationnelles limitées.

Les établissements publics : un maillon souvent oublié mais concerné

Si les petites communes rurales sont au cœur des enjeux de

conformité au RGPD, les établissements publics de coopération intercommunale (EPCI), comme les syndicats intercommunaux, constituent un maillon souvent négligé, bien que tout aussi concerné par les exigences réglementaires.

Parmi ceux-ci, les syndicats de regroupement pédagogique (SIRP), qui organisent la scolarisation dans plusieurs communes rurales, illustrent parfaitement les défis spécifiques liés à la gestion des données personnelles dans un cadre intercommunal. Ces structures, bien que modestes, traitent des données sensibles et doivent naviguer dans un environnement complexe où la coordination entre collectivités membres est essentielle.

Selon la Direction Générale des Collectivités Locales (DGCL, 2024), environ 1 500 SIRP sont actifs en France, regroupant souvent des communes de moins de 500 habitants, ce qui souligne leur importance dans le paysage rural. Les SIRP, créés pour mutualiser la gestion des écoles primaires entre plusieurs petites communes, collectent et traitent une variété de données personnelles, souvent sensibles.

Par exemple, le SIRP de la Vallée du Lot, qui regroupe cinq communes dans le Lot (totalisant environ 600 habitants), gère des données sur les élèves (noms, dates de naissance, dossiers médicaux pour les allergies ou handicaps), organise les transports scolaires (horaires, adresses des familles) et maintient des relations avec les parents (courriers, inscriptions aux activités périscolaires). Ces traitements, bien que limités en volume, impliquent des informations protégées par le RGPD en raison de leur caractère personnel et de leur lien avec des mineurs.

La spécificité des SIRP réside dans le partage des traitements entre les communes membres et le syndicat lui-même. Par exemple, une commune comme Saint-Vincent-du-Pendit (Lot, 180 habitants), membre du SIRP de la

Vallée du Lot, fournit des données sur ses élèves au syndicat pour l'organisation des transports, tandis que le SIRP centralise les dossiers scolaires et les échanges avec les familles. Cette répartition soulève des questions complexes : qui est le responsable du traitement au sens du RGPD ? Qui tient le registre des traitements ? Quelles mesures de sécurité doivent être appliquées, et par qui ? Selon un rapport de la CNIL (2024), 55 % des SIRP audités en 2023 présentaient des lacunes dans la définition des responsabilités entre le syndicat et ses communes membres, ce qui expose ces structures à des risques juridiques.

La coordination représente un défi majeur. Dans des SIRP comme celui des Coteaux du Tarn (Tarn, regroupant quatre communes pour 400 habitants), les élus rapportent des difficultés à harmoniser les pratiques. Par exemple, une commune peut conserver des fichiers papier non sécurisés, tandis qu'une autre utilise un logiciel numérique, créant des incohérences dans la gestion des données. Une enquête de l'Association des Maires de France (AMF, 2023) indique que 60 % des SIRP de moins de 1 000 habitants ne disposent pas d'un registre des traitements, et 45 % n'ont pas formalisé d'accord clair sur la répartition des responsabilités RGPD.

Dans ce contexte, le DPO mutualisé, souvent rattaché à un CDG, joue un rôle d'interface cruciale entre les communes membres et le SIRP. Sa mission, déjà exigeante dans une seule

commune, se complexifie ici en raison de la nécessité de coordonner plusieurs entités aux pratiques et aux moyens hétérogènes. Par exemple, le CDG de la Haute-Vienne accompagne le SIRP de la Basse-Marche, qui regroupe six communes (environ 800 habitants), en clarifiant les rôles : le SIRP est désigné comme responsable principal des traitements liés à la scolarisation, tandis que les communes sont co-responsables pour les données qu'elles collectent. En 2023, ce travail a permis de rédiger un registre commun et de former les agents des six mairies aux bonnes pratiques.

Cependant, cette mission reste sous tension. Un DPO mutualisé, déjà chargé de suivre des dizaines de collectivités, doit jongler avec des agendas multiples et des priorités divergentes. Selon la FNCDG, un DPO mutualisé consacre en moyenne 10 % de son temps aux structures intercommunales comme les SIRP, ce qui limite sa capacité à intervenir de manière plus approfondie. À titre d'exemple, dans le SIRP du Val d'Allier (Puy-de-Dôme, cinq communes, 700 habitants), le DPO du CDG 63 a été sollicité en 2024 pour résoudre un différend entre deux communes sur la sécurisation des données des transports scolaires, une tâche qui a nécessité plusieurs réunions pour aligner les pratiques.

Pour surmonter ces défis, une gouvernance claire et un partage d'information entre les collectivités membres sont indispensables. Cela implique de formaliser des conventions précisant les responsabilités de chaque acteur, de mettre en place des outils communs (comme des registres partagés) et de sensibiliser les élus et agents à l'importance de la coopération. La CNIL recommande, dans son guide pour les collectivités (2023), l'adoption d'accords au niveau intercommunal pour définir les obligations RGPD, une pratique encore rare : seuls 30 % des SIRP de moins de 1 000 habitants disposent d'un tel document (CNIL, 2024).

Des initiatives émergent pour répondre à ces enjeux. Par exemple, le CDG des Landes a lancé en 2024 un programme pilote pour les SIRP de son territoire, proposant des formations conjointes pour les élus et agents des communes membres, ainsi qu'un logiciel mutualisé pour gérer les données scolaires en conformité avec le RGPD. Ce projet, qui concerne une dizaine de SIRP (environ 2 000 habitants au total), a permis de réduire de 50 % les écarts de conformité signalés par la CNIL

lors de contrôles. Ainsi, les établissements publics comme les SIRP, bien que souvent oubliés dans le débat sur le RGPD, sont pleinement concernés par les exigences de protection des données. Leur fonctionnement intercommunal complexifie la mise en conformité, mais le rôle d'interface du DPO mutualisé, combiné à une gouvernance renforcée, offre des perspectives pour une gestion plus cohérente et sécurisée des données personnelles.

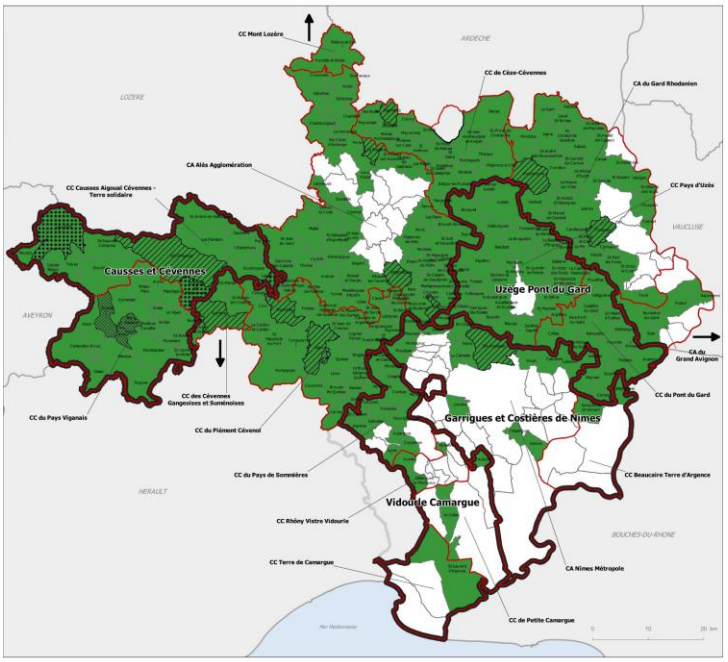
Une meilleure reconnaissance du rôle de DPO mutualisé

Dans le paysage des petites communes rurales et des structures intercommunales comme les SIRP, le DPO mutualisé, souvent rattaché aux CDG, s'impose comme un maillon essentiel.

Il représente fréquemment le seul lien entre les obligations complexes du RGPD et leur mise en œuvre concrète dans des collectivités aux ressources limitées. Par exemple, dans la commune de Saint-Bonnet-le-Bourg (Puy-de-Dôme, 170 habitants), le DPO du CDG 63 a permis en 2024 de sécuriser les données électorales en remplaçant des fichiers papier par un système numérique protégé, une transition que la mairie n'aurait jamais pu entreprendre seule. Selon la FNCDG, 75 % des communes de moins de 500 habitants dépendent de leur DPO mutualisé pour répondre aux exigences de la CNIL. Pourtant, ce rôle stratégique reste sous tension en raison de contraintes logistiques et financières. Pour pérenniser et optimiser ce modèle, plusieurs pistes d'amélioration émergent, visant à renforcer la reconnaissance et l'efficacité des DPO mutualisés.

L'une des principales limites du modèle actuel réside dans la faible présence physique des DPO sur le terrain, les interventions se limitant souvent à des échanges à distance. Pour répondre aux besoins spécifiques des petites communes, un temps de présence sur site renforcé est une proposition clé. Une visite régulière du DPO permettrait de mieux comprendre les réalités locales, d'identifier les failles de sécurité (comme des ordinateurs non protégés) et de renforcer la confiance des élus et agents. Par exemple, le CDG de la Haute-Saône a expérimenté en 2023 une série de visites trimestrielles dans des communes comme La Voivre (90 habitants), ce qui a permis de réduire de 30 % les incidents de sécurité signalés, selon le rapport d'activité du CDG 70 (2024). Selon une enquête de l'AMF réalisée en 2023, 68 % des maires de communes de moins de 200 habitants souhaitent des interventions physiques plus fréquentes de leur DPO pour un accompagnement plus concret.

Les secrétaires de mairie, souvent seuls à gérer les tâches administratives dans les petites communes, jouent un rôle crucial dans la conformité RGPD, mais manquent fréquemment de formation adaptée. Proposer des formations spécifiques à ces agents polyvalents permettrait de les outiller pour gérer les bases du RGPD au quotidien, comme la rédaction de mentions d'information ou la détection de violations de données. Par exemple, le CDG de l'Ain a lancé en 2024 un cycle de formations courtes (trois heures) pour les secrétaires de mairie de communes comme Saint-Maurice-de-Rémens, village de 150 habitants, axé sur des cas pratiques comme la sécurisation des registres d'état civil. Ce



Carte des communes reconnues comme « rurales » au sens de l'INSEE (ici, en vert), soit 81% des communes du département (Source : INSEE 2023)

programme a formé plus de 200 agents en un an, augmentant de 40 % le taux de registres à jour dans les communes concernées (rapport CDG 01, 2024). La CNIL estime dans son rapport 2024 que former les agents administratifs pourrait réduire de moitié les erreurs de conformité dans les petites collectivités.

Le modèle du DPO mutualisé, bien que moins coûteux qu'un DPO interne, représente une charge significative pour les petites communes, dont les budgets annuels dépassent rarement 50 000 euros (DGCL, 2023). Un soutien financier de l'État ou des régions pourrait alléger cette pression et permettre aux CDG de recruter davantage de DPO ou d'améliorer leurs outils. Par exemple, en Nouvelle-Aquitaine, un fonds régional expérimental lancé en 2024 a subventionné à hauteur de 50 % les cotisations RGPD pour 100 communes de moins de 200 habitants, permettant au CDG 24 (Dordogne) d'embaucher un DPO supplémentaire. Cette initiative a permis d'accompagner 20 % de communes supplémentaires dans la région (rapport régional, 2024). Un tel soutien pourrait également financer des outils numériques adaptés, comme des logiciels de gestion des données sécurisés, réduisant la fracture numérique dans les zones rurales.

Enfin, une simplification des obligations RGPD pour les petites communes et structures intercommunales apparaît comme une piste incontournable. Si le RGPD s'applique uniformément, certaines exigences, comme l'analyse d'impact pour chaque traitement ou la gestion complexe des violations de données, peuvent être disproportionnées pour des collectivités traitant un volume limité de données.

La CNIL a déjà adapté certaines recommandations, proposant en 2023 un modèle de registre simplifié pour les communes de moins de 1 000 habitants, adopté par 15 000 collectivités (CNIL, 2024). Une démarche similaire pourrait être étendue, par exemple en dispensant les petites structures de certaines formalités pour les traitements à faible risque, comme les listes électorales dans une commune de 50 habitants. À Rochefourchat (Drôme, 1 habitant), où le volume de données est quasi nul, une approche allégée serait plus réaliste tout en maintenant la protection des citoyens.

Ces propositions, si elles étaient mises en œuvre, renforceraient la capacité des DPO mutualisés à accompagner efficacement les petites communes et leurs structures intercommunales. Elles nécessitent toutefois une volonté politique et des moyens accrus, tant au niveau national que local. Le rôle du DPO mutualisé, pivot de la conformité RGPD dans les territoires ruraux, mérite une reconnaissance accrue, non seulement comme un exécutant technique, mais comme un acteur stratégique de la modernisation administrative. En 2024, la FNCDG a lancé une campagne de sensibilisation auprès des élus pour valoriser ce rôle, avec des ateliers dans 20 départements, touchant plus de 1 000 maires de petites communes. Ces initiatives, bien que prometteuses, doivent s'inscrire dans une stratégie pérenne pour garantir une conformité RGPD durable et adaptée aux réalités du terrain.

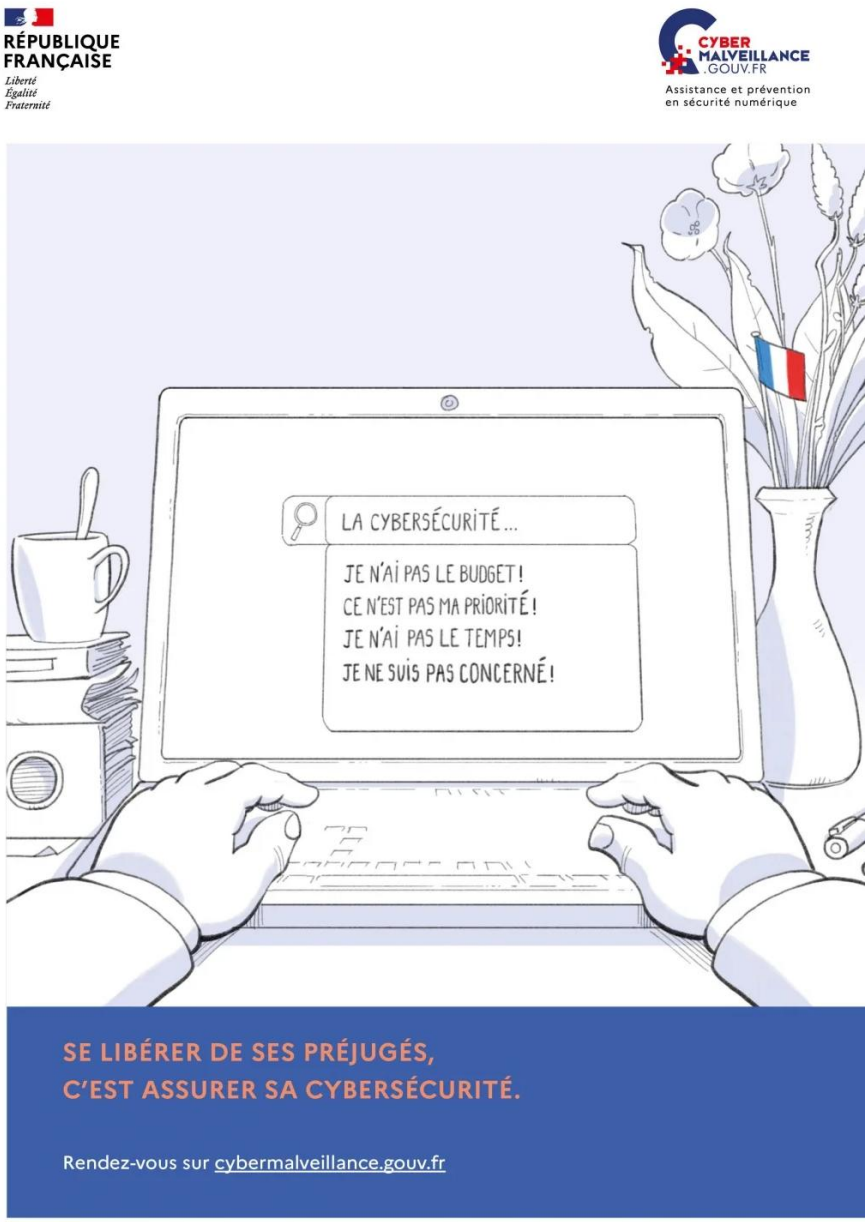
La mise en conformité avec le RGPD dans les petites communes rurales françaises reste un chantier en cours, marqué par des avancées significatives mais freiné par des contraintes structurelles. Avec près de 7 000 communes de moins de 200 habitants en France (Insee, 2023), souvent dotées d'un unique agent administratif polyvalent et d'un accès limité aux outils numériques, l'application d'un cadre réglementaire aussi exigeant que le RGPD représente un défi de taille. Par exemple, une commune comme Fontanès-de-Sault (Aude, 12 habitants) doit théoriquement respecter les mêmes obligations qu'une grande métropole, malgré un budget annuel inférieur à 30 000 euros (DGCL, 2023). Selon un rapport de la CNIL (2024), si 65 % des petites collectivités ont entamé leur mise en conformité, seules 40 % d'entre-elles respectent l'ensemble des exigences, illustrant un processus lent, entravé par le manque de moyens humains et techniques.

Dans ce contexte, le recours aux DPO mutualisés, portés par les CDG, s'est imposé comme une solution efficace pour accompagner ces communes et leurs structures intercommunales, comme les SIRP. En offrant une expertise juridique, des outils standardisés et une mutualisation des coûts, les DPO mutualisés permettent à des collectivités comme une petite commune de l'Eure, Saint-Germain-de-Pasquier (130 habitants), de sécuriser leurs données sensibles, telles que les registres d'état civil, tout en

allégeant la charge administrative des élus. La FNCDG estime que près de 70 % des communes de moins de 500 habitants dépendent de ce modèle pour leur conformité RGPD. Toutefois, les limites actuelles – surcharge des DPO, interventions souvent à distance, outils parfois mal adaptés – soulignent la nécessité d'accorder davantage de moyens et de reconnaissance à ces acteurs clés. Par exemple, le CDG de la Creuse, qui couvre 250 communes avec seulement deux DPO, illustre les tensions auxquelles ce modèle est confronté (rapport CDG 23, 2024).

L'enjeu central reste d'assurer une protection réelle des données personnelles, même dans les territoires les plus ruraux, sans imposer des charges trop lourdes aux collectivités locales. Les données des citoyens – qu'il s'agisse des listes électorales, des dossiers scolaires ou des demandes de permis de construire – méritent une gestion sécurisée, quel que soit le contexte. Malgré ce, la perception du RGPD comme une contrainte trop bureaucratique, exprimée par 72 % des maires de communes de moins de 200 habitants (AMF, 2022), appelle des solutions pragmatiques. Renforcer la présence des DPO sur le terrain, former les secrétaires de mairie, mobiliser des financements publics et simplifier certaines obligations pour les petites structures sont autant de pistes pour concilier protection des données et réalités locales.

En définitive, la conformité RGPD dans les petites communes rurales ne peut être envisagée comme un objectif immédiat, mais comme un processus progressif, soutenu par des DPO mutualisés mieux outillés et une gouvernance adaptée. À l'image de la commune de Labeaume (Ardèche, 180 habitants), qui a progressivement sécurisé ses pratiques et usages grâce à l'accompagnement du CDG 07, ces territoires démontrent qu'une approche assez pragmatique, combinant expertise externe et volonté locale, peut transformer une contrainte réglementaire en une opportunité pour moderniser l'administration. L'avenir de la protection des données dans les zones rurales dépendra de la capacité des acteurs publics à valoriser ce modèle mutualisé, garantissant ainsi un équilibre entre conformité, équité et soutenabilité pour les plus petites collectivités ■



La gestion des documents numériques
une étape préalable essentielle à une bonne conservation des archives

Une archive numérique peut être :

- Un document **numérique natif**, c'est-à-dire qu'il est créé sous forme électronique, et non sur papier :
    - Courriels
    - Documents issus des outils bureautiques (fichier Word, Excel, etc.)
    - Documents et données issus d'applications métiers
    - Documents multimédias
    - Documents et données échangées dans le cadre des téléprocédures
- Un document **numérique de substitution** (document scanné), établi conformément à un protocole de numérisation fidèle, répondant aux normes en vigueur.

Les archives numériques obéissent **aux mêmes règles et aux mêmes principes de gestion que les archives papier**. Elles présentent des particularités techniques qui nécessitent des méthodes de traitement adaptées à leur nature. Toute élimination d'archives numériques doit faire l'objet d'un bordereau d'élimination visé par le directeur des Archives départementales (articles L.214-1 à 10 du code du patrimoine).

Il est important de faire la distinction entre **les documents de travail et les documents validés** : ces derniers sont susceptibles d'engager juridiquement la collectivité. Les documents de travail (brouillons, documents non validés) peuvent être éliminés dès qu'ils ne sont plus utiles, sans bordereau de suppression.

L'archivage électronique est l'ensemble des actions, outils et méthodes mis en œuvre pour réunir, identifier, classer, détruire et conserver des contenus numériques, sur un support sécurisé. Archiver sous forme électronique n'est pas numériser ou dématérialiser. Le but de l'archivage électronique est de pouvoir exploiter les données et les rendre accessibles dans le temps, que ce soit à titre de preuve (en cas d'obligations légales notamment ou de litiges) ou à titre historique.

Conseil de notre archiviste

L'optimisation de la gestion des fichiers et dossiers numériques

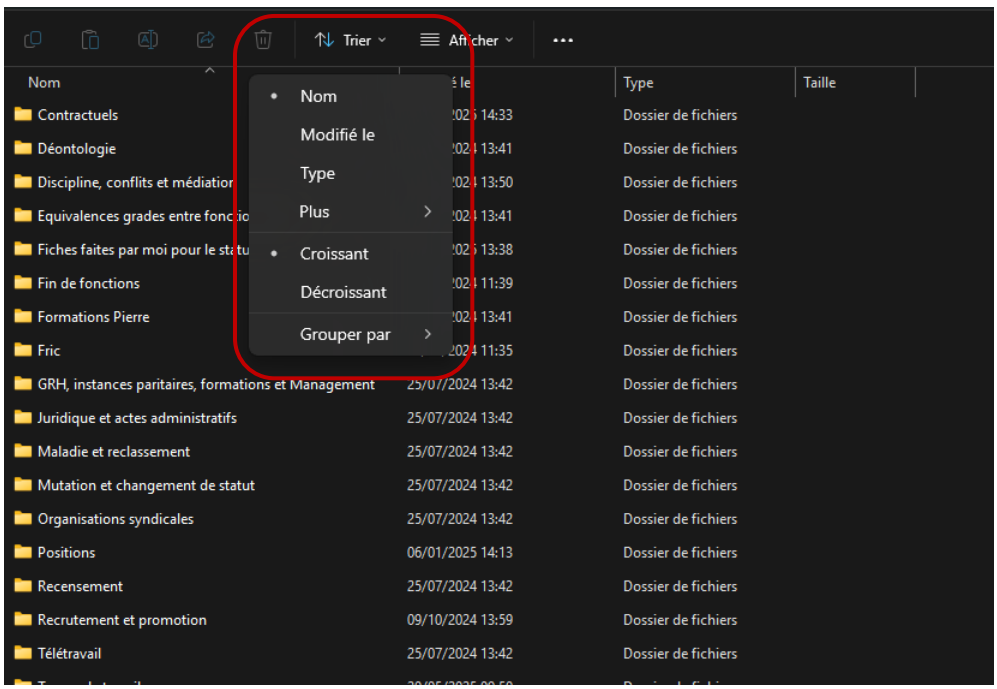
Objectif : optimiser l'organisation, le classement et la gestion des documents numériques afin de faciliter l'accès, la recherche et le traitement des informations.

1 Évaluer le Vrac Numérique

Étapes :

1. **Dresser un inventaire des fichiers :** identifiez les types de fichiers présents dans le vrac (documents, images, vidéos, PDF, etc.). Cela vous permettra de comprendre la diversité des contenus à traiter.
2. **Analyser la volumétrie :** Estimez le nombre de fichiers et la taille des dossiers. Cela vous donnera une idée du temps et des ressources nécessaires pour gérer ce vrac.
3. **Identifier les priorités :** Sélectionnez les fichiers urgents ou importants (par exemple, les documents contractuels, les factures, les rapports, etc.) et traitez-les en priorité.

Conseil : Utilisez des outils de recherche de type « tri par date » ou « tri par type » pour mieux analyser le vrac.



Exemple d'outil de recherche sur un dossier de Windows 11

2 Tri initial et suppression des fichiers inutiles

Étapes :

1. **Supprimer les doublons :** Utilisez des outils pour détecter et supprimer les fichiers en double (par exemple, Duplicate Cleaner ou CCleaner)
2. **Supprimer les fichiers obsolètes ou inutiles :** Vérifiez les fichiers non pertinents, temporaires ou dépréciés (par exemple, les images non utilisées, les fichiers téléchargés et non ouverts)
3. **Organiser les fichiers par type :** Regroupez les fichiers en catégories (documents textes, images, vidéos, etc.) pour une première séparation.

Conseils :

- Avant de supprimer un fichier, assurez-vous qu'il n'est pas nécessaire à long terme (par exemple, pour des archives légales ou fiscales)
- Utilisez des outils comme Archifiltre pour faciliter la détection des doublons

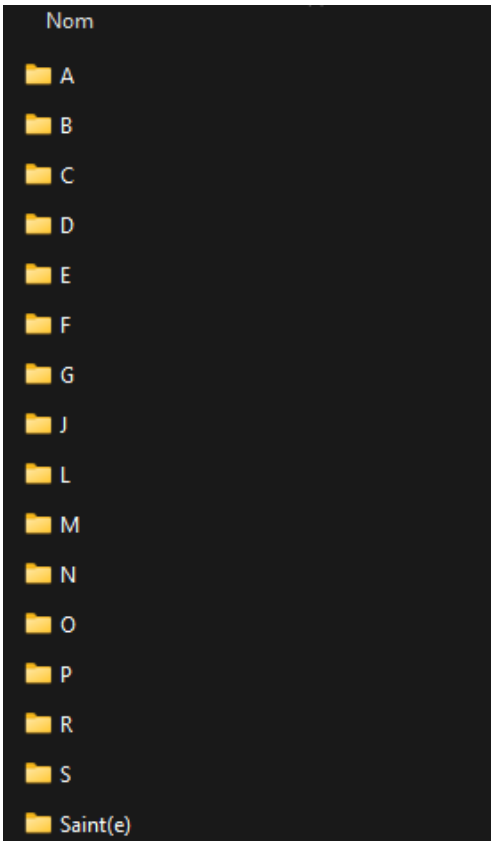
3 Définir une structure hiérarchique claire

Étapes :

1. **Créer des catégories principales :** Organisez les dossiers par thématiques principales (par exemple, « administratif », « projets », « finances », etc.)
2. **Sous-dossiers :** Créez des sous-dossiers spécifiques pour chaque catégorie. Par exemple, dans un dossier « Projets », vous pourriez créer des sous-dossiers par projet (« Projet A », « Projet B », etc.)
3. **Nommer de manière logique :** Utilisez des noms simples, clairs et explicites pour les dossiers et sous-dossiers (par exemple, « Contrats_2025 », ou encore « Factures_janvier », etc.)

Conseils :

- Limitez le nombre de niveaux de dossiers pour éviter la complexité excessive (pas plus de 3 ou 4 niveaux)
- Respectez une nomenclature uniforme



Par exemple, les dossiers de chaque collectivité suivie par le service « Protection des données » du CDG 30 sont classés par types (communes, établissements publics, etc.), puis par ordre alphabétique

4 Choisir un système de nommage des fichiers cohérent

Étapes :

1. **Format standard :** Définissez un format de nommage pour vos fichiers afin d'assurer leur lisibilité et leur traçabilité (par exemple, « type_document_date_version », ce qui donnerait « Facture_2025-01-15_V1.pdf »)
2. **Incorporer des métadonnées :** Lorsque possible, inclure des informations clés dans le nom du fichier (date, auteur, version, etc.)
3. **Éviter les caractères spéciaux :** Utilisez des tirets, des underscores (aussi appelé couramment « tiret du 8 ») ou des espaces pour séparer les mots, mais évitez les autres caractères spéciaux

Conseils :

- Ajoutez des numéros de version ou des dates pour éviter la confusion entre les différentes versions d'un document
- Utilisez des conventions communes au sein de votre équipe

En résumé :

1. **Évaluez et identifiez le vrac numérique**, en analysant les types de fichiers et en définissant les priorités
2. **Supprimez les fichiers inutiles** (doublons) et effectuez un premier tri par type
3. **Organisez la structure des dossiers** de manière logique et simple
4. **Traiter le vrac :** renommez et rangez les fichiers

LE BON GESTE

Par Sidonie HOURS, stagiaire au service « Protection des données »

LES CAMÉRAS-PIÉTONS

Qu'est ce que c'est ?

Une caméra-piéton est un dispositif mobile porté par un agent permettant d'enregistrer des images et du son de ses interactions avec le public, voire des scènes de délits ou de crime.

Cadre légal

Code de la sécurité intérieure (article L.241-2 à L.241-5)
Décret n°2022-605 du 21 avril 2022
Loi n°2018-697 du 3 août 2018

L'utilisation des caméras-piétons est strictement encadrée par la loi et ne peux se faire que dans des situations précises. Elles répondent à 4 finalités principales **: prévenir l'incident, constater des infractions, collecter des preuves, former les agents.**

L'usage des caméras-piétons est soumis à des règles précises afin de garantir le respect des libertés individuelles. Voici les principales conditions à respecter :

- Pas d'enregistrement en continu
- Activation manuelle par l'agent
- Information de la personne concernée

Protection des données personnelles

Les enregistrements sont conservés pour une durée maximale de 6 mois, sauf s'ils sont extraits dans le cadre d'une procédure administrative, disciplinaire ou judiciaire.
Les personnes filmées ne peuvent pas consulter directement les enregistrements. Si elles souhaitent exercer leur droit d'accès, elles doivent passer par un recours indirect auprès de la CNIL (Commission Nationale de l'Informatique et des Libertés), qui agira comme intermédiaire pour vérifier la légitimité de la demande.

TYPES DE DONNÉES	MODALITÉ DE COLLECTE
Images enregistrées par les caméras	**Collecte autorisée** L'enregistrement n'est pas permanent, l'agent doit l'enclencher lorsque se produit ou est susceptible de se produire un incident
Horodatage des enregistrements	**Collecte obligatoire** Lorsque les caméras ne permettent pas d'horodater l'enregistrement, l'agent doit être en mesure de justifier l'information
Lieux d'enregistrement	**Collecte obligatoire** Certaines caméras permettent une géolocalisation des agents, ce suivi ne doit pas être permanent et doit pourvoir être désactivé pendant les temps de pause des agents

Bonnes pratiques pour les agents :

Pour garantir un usage conforme et éthique des caméras-piétons, les agents doivent respecter un certain nombre de bonnes pratiques au quotidien :

- **Activer la caméra uniquement dans les cas prévus par la réglementation**, notamment en cas de tension, de conflit ou de situation à risque.
- **Vérifier systématiquement que l'équipement est en état de fonctionnement** (batterie, mémoire, enregistrement) avant chaque mission.
- **Être capable d'expliquer l'usage de la caméra à toute personne concernée**, dans un cadre de transparence, lorsque les circonstances le permettent.
- **Ne jamais utiliser la caméra à des fins personnelles** ni détourner les enregistrements à des usages non professionnels.

Procédure pour la mise en place de caméras-piétons par un collectivité :

1. Seules certaines autorités publiques qui sont habilités peuvent utiliser les caméras-piétons :
   - Les polices municipales
   - Les agents de surveillance de la voie publique (ASVP) dans certains cas
   - Les agents de sécurité de la SNCF ou de la RATP

2. La mise en place doit faire l'objet d'une autorisation préfectorale qui est valable 5 ans.

3. Cette autorisation est composée d'un dossier administratif et technique comprenant plusieurs pièces, dont un engagement de conformité destiné à la CNIL.

4. Il est nécessaire de prévoir une analyse d'impact relative à la protection des données avec votre DPO.

5. Les agents doivent recevoir une formation sur l'utilisation du dispositif et une note d'information interne est recommandée. Le public doit être informé de l'usage possible de caméras-piétons via un affichage ou une communication claire.

Durée de conservation

DOCUMENT	DURÉE DE CONSERVATION	SORT FINAL
Images enregistrées	1 mois	Destruction automatique*
Registre des accès aux enregistrements et réquisition judiciaire	3 ans	Destruction avec autorisation des archives départementales

*Il est possible de garder les données au-delà d'un mois lorsque les enregistrements sont utilisés à des fins de formation. Toutefois, il faut flouter les images afin de ne plus identifier les personnes

Transmission des données

Les données peuvent être transmises :

- Au maire
- Au président de l'intercommunalité
- Au responsable du service de police municipale
- Aux agents individuellement désignés ou habilités par le maire
- A l'agent auquel la caméra est fournie
- Aux agents en charge de la formation des agents

GOUVERNEMENT
Liberté
Égalité
Fraternité

17 CYBER
Mon assistance en ligne

Un service proposé par

POLICE NATIONALE
Gendarmerie nationale
CYBER MALVEILLANCE .GOUV.FR