Collectivités territoriales

Guide pratique du **numérique**

MAIF

assureur militant

Sommaire

pages

📖 Termes renvoyant aux lexique.

Les données, un potentiel à protéger

Les collectivités locales recourent de façon croissante au numérique pour gérer les services dont elles ont la compétence : état civil, listes électorales, inscriptions scolaires, action sociale, gestion foncière et urbanisme, facturation de taxes et redevances, etc. La divulgation ou la mauvaise utilisation des informations collectées est susceptible de porter atteinte aux droits et aux libertés des personnes ou à leur vie privée. Afin que les usagers aient confiance, les services numériques doivent répondre aux exigences de protection des données. Les collectivités ont l'obligation de se mettre en conformité avec le règlement européen sur la protection des données (RGPD), applicable depuis mai 2018.

Les différentes **données**

Les données personnelles

Les données personnelles sont définies par l'article 2 de la loi Informatique et libertés du 6 janvier 1978 : *« Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »* Sont donc visées des informations relatives à l'état de la personne, mais aussi à sa situation économique, sa vie sociale, etc.

Données individuelles	Nom, prénom, date de naissance, nationalité, adresse postale, téléphone(s), courriel...
Données d'état civil	Données individuelles + naissance, mariage (témoins, professions..., Pacs, filiation, décès
Données familiales	Aides sociales, Caf, relations familiales et liens de famille, inscription en établissement scolaire, données de patrimoine
Données biométriques	Empreintes digitales, photo
Données médicales	Numéro de Sécurité sociale, fiche médicale fournie par la famille, certificat médical, régime alimentaire, handicap
Données RH	CV, position, ancienneté, statut, absences, arrêts maladies, accidents de travail, sanctions, type de véhicule, situation de santé des conjoints ou enfants en vue d'ouverture de droits
Données financières	RIB, dettes, non-valeur
Données fiscales	Revenus fiscaux, quotient familial, données de redevance d'enlèvement des ordures ménagères
Données d'urbanisme	Propriété des parcelles, location, études foncières
Données concession	Lieu de concession funéraire, places disponibles
Données police municipale	Suivi de délinquance, infractions, verbalisation, pièces d'identité, n° d'immatriculation du véhicule, contrat d'assurance

Le croisement de toutes ces données peut aboutir à un profil précis d'une personne ainsi que de toute sa famille et son environnement.
Pour rappel : les agents publics ont un devoir de réserve et de secret sur les données qu'ils utilisent.

Les données sensibles

Les données sensibles sont *« les données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci »* (art. 8 loi I&L).
Elles font l'objet d'un régime de protection renforcée. Sauf exception légale, il est par principe interdit de les collecter.

Les données sensibles eu égard à la loi :

> les données médicales pour un Ehpad avec un dossier contenant les maladies, un projet d'accompagnement individuel, etc. ;

> le dossier « enfant » avec une partie médicale contenant des informations sur sa prise en charge dans le milieu éducatif ou par la mairie avant et après les horaires péri ou extrascolaires ;

> les données RH des agents : appartenance syndicale, données médicales (état de santé) ;

> les données utiles pour les demandes d'aide au logement en lien avec le handicap. Même si elles ne tombent pas sous la définition légale d'une donnée sensible, certaines données doivent être traitées avec prudence ;

> les données sociales qui rentrent dans l'intimité de la personne : famille d'accueil, parent ou fratrie en prison, addiction ;

> le dossier « enfant » avec une partie sociale : comportement inadapté ou violent, environnement radicalisé, trafic de drogues, etc. ;

> les infractions présentes dans le casier judiciaire, même si celui-ci ne rentre pas dans cette catégorie ;

> les sanctions disciplinaires dans le cadre du travail ;

> l'indication « fiché S » ;

> le mariage entre personnes d'un même sexe. Si l'orientation sexuelle est une donnée sensible, le mariage homosexuel n'en est pas une, puisqu'il est rendu public.

Ce qui incombe **aux collectivités**

Les obligations

Un certain nombre d'obligations normatives s'appliquent aux collectivités.

- La loi Informatique et libertés du 6 janvier 1978 a pour principal objectif de protéger les informations concernant une personne enregistrée dans des fichiers. Cette loi a un champ d'application très large.
- Le référentiel général de sécurité (RGS), applicable depuis mai 2013, pose une obligation spécifique en ce qui concerne les certificats électroniques, afin de protéger le système d'information.
- La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (dite loi Lemaire) adapte la législation française au nouveau monde numérique.
- Le règlement général de protection des données (RGPD), applicable depuis mai 2018.

> La dématérialisation

Le programme Action publique 2022 vise la dématérialisation de 100 % des démarches d'ici 2022 :

- de la chaîne comptable et financière grâce au programme PES, protocole d'échange avec le Trésor public pour la transmission des pièces comptables et des justificatifs, ainsi que la signature électronique des documents ;
- des marchés publics tels que mise en place par l'ordonnance n° 2015-899 du 23 juillet 2015 et les décrets d'applications de 2016 ;
- et de la chaîne budgétaire *via* @CTES, Aide au contrôle de légalité dématérialisé, le programme de développement du système d'information de transmission des actes soumis au contrôle de légalité et au contrôle budgétaire.

> L'ouverture des données publiques *(Open data)*

Une donnée est considérée comme ouverte quand elle peut être consultée, utilisée et partagée par tous. C'est le principe de l'accessibilité des données ou *Open data*. Dans un souci de transparence de l'action publique, la loi pour une République numérique du 7 octobre 2016 impose aux collectivités :

- l'accès électronique aux informations publiques relatives au territoire pour celles de plus de 3 500 habitants (ou plus de 50 agents) : rapports, études, statistiques, codes sources, permis de construire, correspondances, etc. ;
- la diffusion des comptes-rendus de conseil municipal pour celles disposant d'un site internet ;
- la mise à disposition, de manière permanente et gratuite, des délibérations du conseil municipal et des actes réglementaires pris par les autorités départementales ou régionales.

Cette loi permet d'établir un socle commun de données à ouvrir en priorité : les budgets, les résultats électoraux, le plan local d'urbanisme…

Par ailleurs, les documents administratifs doivent être transmis sous format électronique *« dans un standard ouvert, aisément réutilisable et exploitable par un système de traitement automatisé »* (article 3 de la loi pour une République numérique).

En juin 2019, seules 10 % des collectivités qui en ont l'obligation publiaient leurs données. Les collectivités peuvent se regrouper et déposer leurs données sur un portail commun. Elles peuvent également utiliser, comme 23 % d'entre elles, la plateforme gratuite de l'État (**data.gouv.fr.**)

En savoir

Observatoire OpenData des territoires :
> observatoire-opendata.fr
> data.gouv.fr

La mise en œuvre

> La protection des données

Le RGPD encadre le traitement des données personnelles de tout organisme amené à gérer des données. Il uniformise les principes de protection de la vie privée déjà contenus dans la loi Informatique et libertés : une finalité déterminée et légitime, des données pertinentes et non excessives, une durée de conservation limitée à la durée nécessaire à la poursuite de la finalité, la sécurité des données collectées, le droit d'accès aux données des personnes concernées, celui de les faire rectifier en cas d'inexactitude, de s'opposer au traitement pour motif légitime. Grâce à lui, l'usager peut renforcer le contrôle de l'utilisation de ses données personnelles.

Le traitement des données concerne toutes les opérations et utilisations portant sur les données personnelles, quelle que soit la technique utilisée, et notamment la collecte, l'enregistrement, la conservation, la modification, l'extraction, la consultation, la communication, le transfert, l'interconnexion, mais aussi le verrouillage, l'effacement ou la destruction. Les collectivités peuvent s'appuyer sur l'ensemble des outils mis à disposition par la Commission nationale de l'informatique et des libertés (Cnil) pour se mettre en conformité. En particulier :

– le modèle de registre des traitements ;
– l'outil en *open source* permettant de réaliser des analyses d'impact suivant un chemin clair et détaillé, complété par un catalogue de bonnes pratiques ;
– le guide relatif à l'encadrement des opérations sous-traitées ;
– le guide dédié à la sécurité des données personnelles ;
– et des modèles/trames de mentions d'information et de recueil de consentements, etc.

En savoir

Guide de sensibilisation au RGPD, Cnil, septembre 2019 :
> bit.ly/2m42GBe

Détail des actions dans la fiche MAIF « Le RGPD, qui est concerné ? »
> maif.fr/associationsetcollectivites/associations/guides-fonctionnement/rgpd.html

> Le responsable du traitement des données

Le responsable du traitement des données est la personne morale (collectivité, etc.) incarnée par son représentant légal (président, maire, etc.) qui détermine les finalités et les moyens du traitement des fichiers. Ainsi, le maire est responsable des traitements informatiques et de la sécurité des données personnelles qu'ils contiennent. En cas de non-respect, sa responsabilité, notamment pénale, peut être engagée.

Pour rappel
Il convient de distinguer le responsable du traitement du prestataire de services (ou « sous-traitant »). Ce dernier intervient pour le compte du responsable du traitement selon les objectifs qui lui ont été assignés, définis dans le contrat de prestation de service. Par exemple, l'éditeur de logiciels auquel la collectivité locale fait appel est un prestataire de services. La responsabilité du traitement en incombe à la collectivité.

En savoir

Fiche « Responsable de traitement des données », Cnil :
> bit.ly/2ouBNI1

> Le délégué à la protection des données

Toutes les collectivités ont l'obligation de désigner un délégué à la protection des données (DPD) ou *Data Protection Officer*/DPO. Son rôle est d'accompagner et de conseiller les services et les agents dans les traitements des données personnelles, et de garantir la conformité de ceux-ci au RGPD. Référent de la politique de protection des données physiques, il peut être interne ou externe, mutualisé ou non entre plusieurs collectivités.

Recommandations
L'externalisation et le recours à un prestataire extérieur peut répondre aux besoins d'une collectivité qui n'effectue que des traitements de base sur les données personnelles concernant une population limitée et qui n'aurait, en tout état de cause, ni la nécessité ni les moyens de disposer d'un DPD à temps complet. Attention cependant aux prestataires peu scrupuleux qui proposent des prestations de conformité soi-disant labellisées Cnil. Les collectivités sont invitées à examiner soigneusement les références et à contacter la commission en cas de doute.

> L'apparition de nouveaux

métiers

De nouveaux métiers sont apparus avec le numérique. La collectivité s'est ainsi ouverte à des professionnels chargés d'animer des communautés d'usagers (*Community managers*), de piloter la gestion des bases de données 🕮 (*Chief data officer)* ou encore de définir la stratégie digitale du territoire (*Chief digital officer.*) Quatre-vingts métiers, liés à l'informatique, sont aujourd'hui référencés.

En savoir

Les métiers de la data :
> bit.ly/2JD2nV4

> Les opportunités de mutualisation

La collaboration autour de projets informatiques est nécessaire pour les collectivités de petite taille, afin de leur permettre de fournir des services qu'elles ne peuvent pas mettre en place seules. La mutualisation est pertinente pour développer ces nouvelles expertises en partageant les coûts.

> La formation des personnels

Les données des citoyens sont non diffusables et leur protection nécessite une sensibilisation et une formation adaptée et différenciée des personnels. La mise en place de règles de conduite simples à adopter au quotidien limite le risque d'attaque.

Pour sensibiliser et former

– La mise en place d'un **outil de *e-learning*** dédié à la sensibilisation et à la formation aux questions de sécurité.
– La rédaction d'une **Charte informatique** pour les élus et les collaborateurs qui indique les droits et les devoirs de chacun vis-à-vis de l'information en énumérant les principes essentiels et les comportements attendus en interne. Elle peut aussi préciser la politique d'habilitation concernant les droits d'accès aux données 🕮.

Quelques règles de base

– Pour la messagerie électronique : face au *phishing* 🕮 et aux *ransomwares* 🕮, il est important de faire comprendre qu'il faut analyser le contenu et la provenance d'un e-mail avant de l'ouvrir.
– Afin de respecter la confidentialité : verrouiller les postes de travail dans le cas d'une absence prolongée avec un mot de passe qui sera changé régulièrement.

En savoir

Centre national de la fonction publique territoriale (CNFPT) : cnfpt.fr/

Club de la sécurité de l'information en réseau (Clusif) : clusif.fr/clusir/

ANSSI : ssi.gouv.fr/

Les mesures organisationnelles

L'organisation du stockage et de la protection des données personnelles est liée aux modes de fonctionnement propres à chaque collectivité. Il n'existe pas de règles imposées. En général, la gestion des données collectées suit la même organisation de stockage des données que pour les dossiers papier : un stockage dans la mairie (le serveur 🕮 s'y trouve la plupart du temps), des sauvegardes par métier et par direction et un double archivage (papier et numérique *via* le *cloud*). Deux choix de stockage répondant à des stratégies d'investissement différentes sont possibles : investir dans un *datacenter* de proximité ou migrer vers des solutions *cloud*, plus souples.

À titre d'exemple, en mai 2019, la ville de Paris a inauguré un datacenter *municipal implanté dans le nord de la capitale afin d'avoir la totale maîtrise sur ses données.*

> Le *cloud computing* 🕮

La collectivité peut stocker les données numériques de ses citoyens sur un *cloud computing* (ou l'informatique en nuage). Le principal inconvénient de ce service est que la collectivité n'a pas la maîtrise sur ses données. Elles seront difficilement localisables, stockées sur des serveurs distants à l'étranger et dépendant juridiquement du pays hébergeur.

> Le *cloud* souverain

L'État encourage les collectivités à adopter une solution de *cloud* souverain, c'est-à-dire de souscrire à un prestataire soumis au droit français, hébergeant l'ensemble des données 🕮 dans un *datacenter* localisé en France. Les données du *cloud* sont alors entièrement stockées et traitées sur le territoire français, à l'exemple de *CloudWatt* et *Numergy,* issus d'un partenariat entre l'État et des opérateurs privés.

En savoir

> cloudwatt.com/fr

> hlogin.numergy.com

> Les relations avec les sous-traitants

Une collectivité qui confie ses données à un prestataire hébergeur doit pouvoir disposer :

– d'une garantie technique, sur le niveau de sécurité offert par le prestataire et ses sous-traitants pour garantir la protection et la confidentialité des informations (dispositifs anti-intrusion) ;
– et d'une garantie juridique concernant, d'une part, l'absence d'utilisation des données et, d'autre part, le non-accès aux données par un tiers.

Tous ces éléments doivent pouvoir être contractualisés et vérifiés auprès des différents fournisseurs, d'où l'importance de labels et de certifications reconnus.

> Les labels de confiance

La qualification ***SecNumCloud,*** label de confiance de l'Agence nationale de la sécurité des systèmes d'information (Anssi) s'impose comme la référence en matière de sécurité numérique. Son référentiel couvre les produits livrés en tant que services en ligne, les infrastructures (bureaux et *datacenters*) sur lesquels ils s'appuient, et les procédures d'exploitation, de gestion et de fonctionnement. Une liste des prestataires est fournie sur le site de l'Anssi.

Depuis janvier 2019, Oodrive a décroché ce label. OVH, Cheops Technology, Idnomic, Orange, Outscale, Vendôme Solutions et Worldline sont aujourd'hui candidats pour l'obtenir.

En savoir

Liste des produits et services certifiés par l'Anssi :
> bit.ly/2mcZ2FM

Le numérique dans la vie de la collectivité

Le numérique impose aux collectivités de revoir le mode d'accès à leurs services.

Ce que **l'État met à la disposition** des collectivités

Etalab

La mission **Etalab** fait partie de la Direction interministérielle du numérique et du système d'information et de communication de l'État (Dinsic). Ce service accompagne l'ouverture des données 🕮 de toutes les administrations publiques. Il anime la plateforme ouverte des données publiques **data.gouv.fr** qui met en relation des producteurs et des utilisateurs de données. Pour les collectivités qui n'auraient pas de budget dédié, leurs données peuvent y être hébergées gratuitement.

En savoir

Etalab : > etalab.gouv.fr
> data.gouv.fr

demarches-simplifiees.fr

Demarches-simplifiees.fr est hébergé par la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC). Il s'adresse aux agents des services publics de l'État, des collectivités et fonctionne comme un générateur de formulaires. Sa spécificité est de mutualiser pour éviter la multiplication d'outils spécifiques.

service-public.fr

service-public.fr propose un accompagnement et des fonctionnalités pour aider les mairies, de toutes tailles, dans l'amélioration continue des services aux usagers. Par exemple, l'inscription sur les listes électorales, le recensement de jeunes citoyens, l'obtention d'un acte d'état civil ou la consultation des offres de marché public est ainsi accessible. Le raccordement d'une commune au dispositif est simple, sécurisé, gratuit et rapide. Près de 8 000 mairies l'utilisent déjà.

franceconnect.gouv.fr

franceconnect.gouv.fr permet aux internautes de s'identifier sur un service en ligne local par l'intermédiaire d'un compte déjà existant (impots.gouv.fr, ameli.fr, La Poste, etc.) sans création d'un nouvel identifiant ou mot de passe pour l'usager.

opendatafrance.net

opendatafrance.net soutient les collectivités dans leurs démarches d'ouverture de leurs données. Cet organisme recense les réutilisations de données locales, propose des dossiers thématiques (agenda, foncier, déchets…) illustrés de témoignages de réutilisateurs, qu'il s'agisse de collectivités territoriales, d'associations ou d'entreprises.

La ville **intelligente**

Le numérique au cœur de l'aménagement du territoire

Les collectivités sont invitées à devenir des « villes intelligentes » ou *smart cities*. Cette réflexion sur l'introduction des technologies dans la ville doit leur permettre d'offrir de nouveaux usages et de nouvelles manières de gérer les services aux usagers.

Cette tendance s'applique à de nombreux sujets comme :
- des transports plus performants ;
- une meilleure gestion du stationnement ;
- une meilleure gestion de l'électricité et de l'eau ; l'optimisation du ramassage des ordures, de la gestion de la voirie ;
- la simplification de la gestion du parc immobilier de la collectivité.

Exemples d'applications pour usagers

L'application géolocalisée **« DK'CL! »** de la communauté urbaine de Dunkerque est destinée à améliorer le cadre de vie en permettant de signaler un problème de voirie, un accès inadapté, de consulter les travaux en mode carte, etc.

« Dansmarue » de la ville de Paris permet à l'utilisateur de signaler directement les anomalies qu'il aurait constatées et de soumettre ses propositions de végétalisation dans les rues ou les parcs de Paris, depuis son smartphone, aux services concernés.

« Nantes dans ma poche » permet de nombreux services personnalisables pour les usagers (lignes de transports, parkings, services de proximité, etc.) et utilise un ensemble d'outils numériques déjà existants sur la métropole nantaise (sites institutionnels, e-démarches, *open data*, etc.).

Savoir où se garer, trouver des parcs pour se promener, connaître les jours et les horaires des marchés, les événements de son quartier… Voici des exemples de services pratiques proposés par **« Bordeaux en poche »,** une application lancée par la ville et la métropole de Bordeaux.

La ville de Cahors a déployé l'outil **« Tell my city »** pour les signalements. En 2017, les 430 signalements ont concerné principalement la propreté, la voirie, la circulation, les espaces verts et les jardins.

Choisir la bonne application

Le guide *Le numérique va-t-il hacker la démocratie locale ?* présente une méthodologie pour choisir son outil numérique de participation citoyenne (élaborée à partir de cinq questions clefs). Des fiches « démarches » sur la consultation des citoyens, l'organisation d'une concertation, la préparation d'un budget participatif... décrivent les différentes étapes d'un projet type et les facteurs de réussite. À la fin du guide, une liste des applications existantes est proposée.

En mars 2019, la mission Etalab a publié un guide en ligne sur l'usage des **algorithmes** 🕮 publics, conçu comme un outil évolutif. C'est une ressource précieuse pour toute collectivité qui veut développer sa propre application.

En savoir

***Le numérique va-t-il hacker la démocratie locale ?,* mai 2018 : bit.ly/2oxx5JI**

Guide sur l'usage des algorithmes publics, accessible sur Github : bit.ly/2HJirHo

Lexique 🕮

Algorithme
Désigne un ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur.

Authentification
Action qui consiste à prouver son identité à un système informatique, le plus souvent grâce à un mot de passe. La phase d'authentification intervient après la phase d'identification.

Big data
Concept qui englobe toutes les technologies et pratiques destinées à une gestion et analyse massive de données. Plus que l'amas de données, *Big data* fait référence aux activités créées comme l'analyse des données, leur stockage, la valeur qu'elles peuvent créer, le gain de temps si on les analyse plus rapidement, etc.

Cloud computing
(informatique dans les nuages)
Désigne l'utilisation de serveurs distants pour traiter ou stocker l'information. Le *cloud*, par exemple Dropbox, Skydrive ou Google drive, permet de travailler sur un même fichier depuis des ordinateurs ou appareils mobiles.

Donnée (data)
Toute représentation de faits, d'idées ou d'instructions de manière formalisée permettant sa communication, son traitement et/ou son stockage par un cerveau humain ou une machine.

Dématérialisation
Processus remplaçant la transmission, le stockage et l'archivage d'actes papier par des actes numériques.

Identification
Action qui consiste à établir l'identité de l'utilisateur d'un système. Se fait grâce à un identifiant (parfois appelé *login*), unique dans le système, et attribué individuellement à chaque utilisateur. Cette action est très souvent suivie d'une phase d'authentification 🕮.

Phishing
(filoutage ou hameçonnage)
Technique qui a pour but de manipuler un individu pour qu'il révèle des informations confidentielles sur Internet. Par ce biais, un cybercriminel peut obtenir une fausse identité ou bien vider un vrai compte bancaire.

Ransomware (rançongiciel)
Logiciel informatique malveillant, prenant en otage les données.

Serveur
Ordinateur dont les informations peuvent être consultées à distance par d'autres ordinateurs.

Principaux textes législatifs

> Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

> Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique

> Loi n° 2004-809 du 13 août 2004 relative aux libertés et aux responsabilités locales

> Ordonnance n° 2014-1330 du 6 novembre 2014 relative au droit des usagers de saisir l'administration par voie électronique

> Règlement n° 2016/679, dit règlement général sur la protection des données (RGPD)

> Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique

Notes

MAIF protège les élus et les collectivités territoriales avec la même expertise et qualité qui ont fait son succès auprès des associations, des établissements publics et des particuliers.

Découvrez nos solutions dédiées sur

MAIF.FR

ou au **05 49 73 89 89** (prix d'un appel local).

MAIF - société d'assurance mutuelle à cotisations variables - CS 90000 - 79038 Niort cedex 9.
Entreprise régie par le Code des assurances.

10/2019 - Réalisation : Johanna Candidat pour le Studio de création MAIF.