Réglementation : Conformité de la plateforme

SAISINE PAR VOIE ELECTRONIQUE (SVE)

Principe réglementaire	**Depuis le 7 novembre 2016, tout usager peut saisir les administrations** (services de l'État, mairies, organismes de service public ou de sécurité sociale) **par voie électronique, au lieu de se déplacer ou d'envoyer un courrier. Des exceptions existent pour certaines démarches.**
Pour quelles administrations ?	**Depuis le 7 novembre 2016, toutes les administrations (services de l'État, mairies, organismes de service public) peuvent être saisies par voie électronique*.** **Concernant les administrations de l'État et ses établissements publics, des exceptions existent.** Exemples de motifs : • Défense et sécurité nationale ; • Nécessité de comparution personnelle de l'usager ;
A qui la SVE s'adresse ?	**La SVE est accessible à tous les usagers :** • **Particuliers ;** • **Professionnels ;** • **Entreprises ;** • **Associations, etc.**

POUR QUELLES DEMANDES ?

Sauf exceptions, après s'être identifié auprès de l'administration, l'usager peut :

- Adresser par voie électronique toute demande, déclaration, document ou information à l'administration ;
- Et/ou répondre à l'administration par cette voie, sans que le service concerné ne puisse lui demander de répéter ou confirmer sa saisine par une autre voie qui ne serait pas dématérialisée.

QUELLES SONT LES CONTRAINTES POUR LA COLLECTIVITE ?

- **Mettre à disposition des citoyens un ou plusieurs téléservices** : selon le service concerné, l'usager a à sa disposition soit un téléservice spécifique, soit un formulaire de contact général ou ciblé sur un ensemble défini de sujets, dont chaque requête est orientée vers le service compétent. Il est parfois nécessaire d'accompagner votre demande en ligne de pièces justificatives numérisées.

- Lorsqu'il a mis en place un téléservice dédié à l'accomplissement de certaines démarches administratives, le service concerné n'est régulièrement saisi par voie électronique pour ces démarches que par l'usage de ce téléservice.

- **Envoyer dans les 24 heures un Accusé d'Enregistrement Electronique (AEE)** comportant la date de réception de l'envoi électronique ;

- **Envoyer dans les 10 jours ouvrés un Accusé de Réception Electronique (ARE)** par le service compétent et adressé à l'usager, comportant le nom du service en charge de la demander et l'adresse postale (le cas échéant l'adresse électronique), ainsi que le numéro de téléphone du service chargé du dossier.

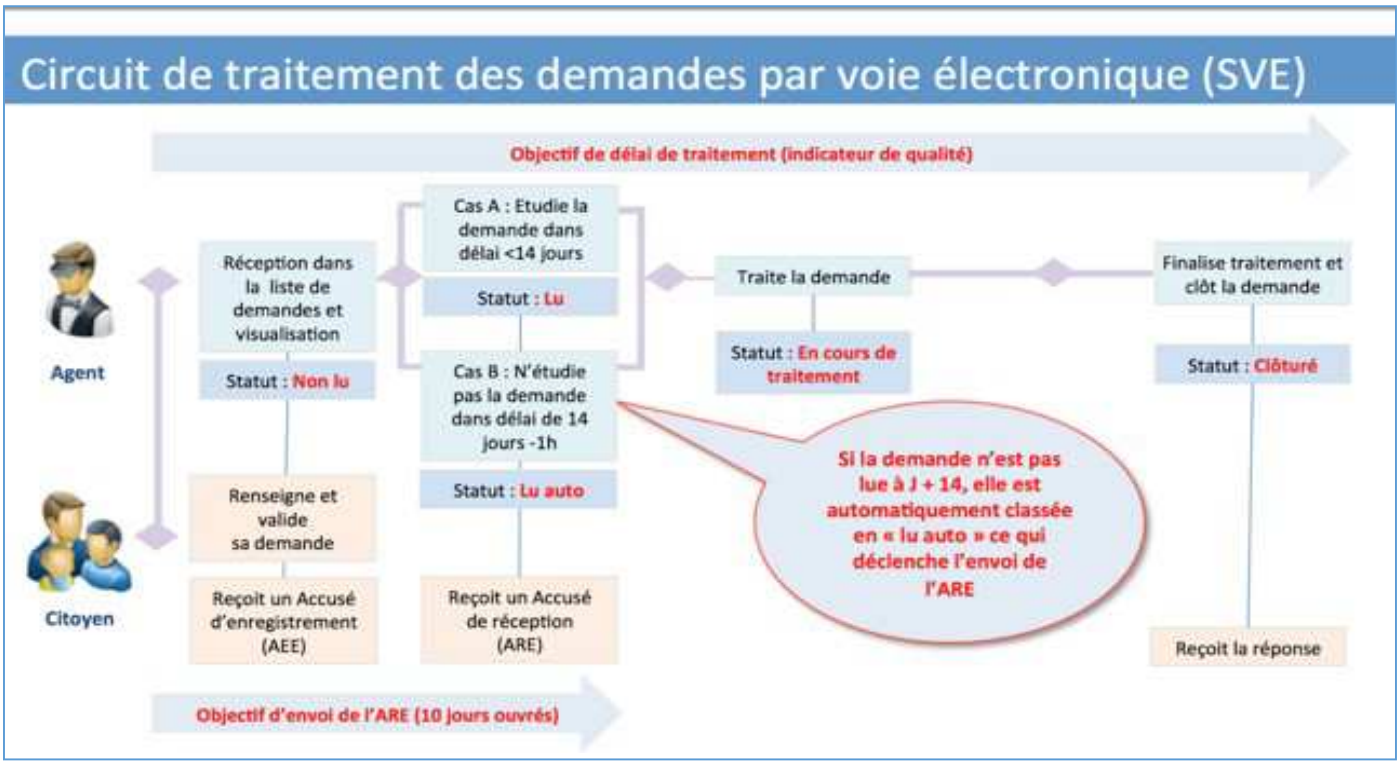
COMMENT LE LOGICIEL AIDE LA COLLECTIVITE A RESPRECTER CES CONTRAINTES ?

- Le logiciel GRC envoie automatiquement un **Accusé d'Enregistrement Electronique** (AEE) ;

- Lorsque l'agent en charge du traitement de la demande lit la demande (passage du statut « non lu » à « lu », le logiciel GRC envoie automatiquement un **Accusé de Réception Electronique (ARE)** avec les informations obligatoires ;

- Si la demande n'a pas été lue par un agent avant 14 jours calendaires (soit moins de 10 jours ouvrés), le logiciel classe automatiquement la demande du statut « non lu » à « lu auto» et envoie automatiquement un **Accusé de Réception Electronique (ARE)** avec les informations obligatoires ;

- Enregistre la **date d'emission de l'AEE et de l'ARE**.



REGLEMENT GENERAL EUROPEEN SUR LA PROTECTION DES DONNEES (RGPD)

MISE EN CONFORMITE RGPD DU LOGICIEL MUTILCANAL

Le logiciel permet à la collectivité de respecter les obligations CNIL/RGPD, notamment en matière de gestion des consentements et de durée de conservation des données. Le logiciel est paramétré avec des durées de conservation par défaut, permettant de fonctionner sans intervention particulière de la collectivité.

Il n'en reste pas moins que la collectivité est le responsable légal du traitement et qu'il lui appartient de vérifier le bon usage du logiciel fait par ses services. Nous mettons met à la disposition du délégué à la protection des données, dont la désignation par la collectivité est obligatoire, toute la documentation nécessaire à l'exercice de ses missions.

La dernière version du logiciel GRC Multicanal (version 2.8.7 conforme RGPD) comporte plusieurs évolutions :

- Gestion explicite des consentements du citoyen concernant la durée de conservation et l'usage de ses données à caractère personnel ;
- Possibilité pour le citoyen d'exercer ses droits de suppression, rectification ou portabilité de ses données à caractère personnel ;
- Gestion des durées de conservation des données à caractère personnel pour chaque téléservice déterminée par la finalité du traitement ;
- Mise à jour des conditions générales d'utilisation (C.G.U).

GESTION DES CONSENTEMENTS

Un message d'avertissement s'affichera lors de la première connexion d'un citoyen à son compte, l'invitant à accéder à la page de gestion de ses consentements. Il ne pourra pas utiliser son compte sans consentir explicitement à la conservation des données d'identification pour une durée de 24 mois après sa dernière connexion.

Le consentement du citoyen à ce que la collectivité utilise son profil pour lui envoyer des informations ciblées ne bloque pas l'accès à son compte mais est mémorisé dans la base de données.

Par ailleurs, lors de la transmission de chaque demande, le citoyen doit explicitement donner son accord pour que les données à caractère personnel de la demande (identification du demandeur et éventuellement données dans le formulaire) soient conservées pour une durée clairement indiquée, ainsi que la justification de cette durée.

RUBRIQUE « DONNEES PERSONNELLES »

Le compte citoyen s'enrichit d'une nouvelle rubrique « Données personnelles » regroupant :

- Les conditions générales d'utilisation du logiciel (CGU) ;
- Les consentements recueillis;
- L'accès au téléservice d'exercice des droits d'accès, de suppression, de rectification ou de portabilité des données à caractère personnel.

EXERCICE DU DROIT DE SUPPRESSION, RECTIFICATION OU PORTABILITE

Le citoyen accède à un téléservice lui permettant d'exercer ses droits de suppression, de rectification ou de portabilité (restitution de ses informations sous un format standard).

Ce téléservice est accessible dans la nouvelle rubrique « Données personnelles » du compte citoyen et sur le site www.localeo.fr/rgpd.

Les demandes issues de ce téléservice sont traitées par le support Localeo. En effet, un citoyen peut disposer d'un compte multi-collectivité. Dans tous les cas, le support Localeo se rapprochera de la (des) collectivité(s) concernée(s) pour valider avec elle(s) la réponse à apporter à la demande du citoyen.

OBLIGATIONS DE LA COLLECTIVITE, RESPONSABLE DU TRAITEMENT DES DONNEES

La désignation d'un délégué à la protection des données (*Data protection Officer*), successeur du correspondant informatique et libertés (CIL) dont la désignation était facultative, sera obligatoire pour les organismes et autorités publics, et donc pour les collectivités, quelle que soit leur taille. Le DPO peut être mutualisé entre plusieurs collectivités (ex : EPCI ou syndicats informatiques).

Missions du Délégué à la Protection des Données

Le délégué aura **pour principales missions** :

- D'informer et de conseiller le responsable de traitement de la collectivité ou le sous- traitant, ainsi que les agents ;
- De diffuser une culture Informatique & Libertés au sein de la collectivité ;
- De contrôler le respect du règlement et du droit national en matière de protection des données, via la réalisation d'audits en particulier ;
- De conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution;
- De coopérer avec la CNIL et d'être le point de contact de celle-ci.

Dans l'exercice de ces missions, le délégué devra être à l'abri des conflits d'intérêts, rendre compte directement au niveau le plus élevé de la hiérarchie et bénéficier d'une liberté certaine dans les actions qu'il décidera d'entreprendre.
De plus, la collectivité devra s'assurer qu'il dispose **d'un niveau d'expertise et de moyens suffisants pour exercer son rôle de façon efficace**. Ainsi, le délégué devra :

- Etre désigné sur la base de ses connaissances spécialisées du droit et des pratiques en matière de protection des données;
- Etre associé en temps utile et de manière appropriée à l'ensemble des questions Informatique & Libertés ;
- Bénéficier des ressources et formations nécessaires pour mener à bien ses missions.

Dans ce contexte, la mutualisation de la fonction de DPO apparaît un enjeu essentiel pour les collectivités territoriales, notamment pour celles de petite taille.

(Source CNIL)

IMPACTS SUR LE PARAMETRAGE DU LOGICIEL GRC MULTICANAL

La collectivité est responsable du traitement, ce qui lui confère plusieurs responsabilités :

- Lors du paramétrage et de l'administration du logiciel, en :
  - Donnant les accès d'administrateurs de services aux seuls agents dont la mission nécessite l'accès à ces informations ;
  - Intégrant dans les notifications envoyées au citoyen le rappel des consentements recueillis ;
  - Désactivant les comptes des agents quittant la collectivité.

- Lors de la conception d'un téléservice, que ce formulaire soit réalisé par votre collectivité avec le générateur de formulaires intégré au logiciel ou réalisé, à votre demande, par le fournisseur, en :
  - Limitant les informations demandées au citoyen à celles strictement nécessaires pour le traitement de sa demande et interdire le recueil de données sensibles[1] ;
  - Dans les formulaires en ligne, évitant autant que possible les champs « textes » et leur préférer des menus déroulants ou des cases à cocher, ce qui permet de limiter les informations non structurées ;
  - Déterminant pour chaque téléservice la durée de conservation nécessaire et la justifier (voir encadré). Pour simplifier le travail de vos services, nous avons mis une valeur par défaut de 24 mois et un motif générique, que nous vous invitons à compléter ou modifier le cas échéant.

- Lors de l'enregistrement dans le logiciel d'une demande d'un citoyen en mode présentiel ou par téléphone par l'un de vos agents, il appartient à vos services de recueillir le consentement du citoyen (par un imprimé remis au guichet ou par un consentement oral[2]).

- Lors du traitement de la demande par un agent de votre collectivité, en sensibilisant les services à ne stocker aucune donnée à caractère personnel dans les notes ou commentaires et naturellement aucune donnée sensible.

1 - Parmi les données à caractère personnel, les données couramment appelées « données sensibles » font l'objet d'un régime de protection renforcée. A titre d'exemple, il s'agit des données relatives aux origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale, ou données concernant la santé, la vie sexuelle, les données génétiques ou les données biométriques.

2 - Si l'adresse électronique du citoyen est enregistrée, il recevra une notification lui rappelant le consentement recueilli