Accompagnement à la Protection des Données Personnelles

Commune d'Aussac-Vadalle

© Site mairie

Compte Rendu d'audit

Année 1 – Avril 2020

Dossier suivi par Paul SABARY (EGH)
Délégué à la Protection des Données
Ligne directe : 05 45 20 08 28
Courriel : dpo@atd16.fr

SOMMAIRE

RAPPEL DU CONTEXTE

1 Rappel du contexte

Dans une volonté d'adaptation à l'ère numérique et un souci d'unification pour l'ensemble des États de l'Union Européenne, le Règlement Européen n°2016/679 dit Règlement Général sur la Protection des Données (ou RGPD) a été adopté le 27 avril 2016 et est entré en application le 25 mai 2018.

Le présent document a pour objectif de répondre aux exigences de ce Règlement en récapitulant notamment l'analyse d'évaluation des risques qui a été faite par l'ATD16 sur les traitements de données réalisées par la commune d'Aussac-Vallade et de porter à la connaissance de cette dernière une série de préconisations dont la mise en œuvre serait souhaitable dans les meilleurs délais mais également à moyen ou long terme.

Il convient toutefois de préciser que le rôle du Délégué à la Protection des Données est de conseiller et d'informer le responsable de traitement (Article 39 du RGPD). La pleine et entière réalisation de ces préconisations reste donc à la discrétion du responsable de traitement, à savoir la commune d'Aussac-Vallade.

- Audit du *11/02/2020* en présence de :
  - Commune d'Aussac-Vadalle : Gérard LIOT (Maire)
  - ATD16 : Paul SABARY (Délégué à la Protection des Données Personnelles)

- Rappel :
  - Responsable de traitement : Commune d'Aussac-Vadalle (représentant légal : Gérard LIOT)
  - Délégué à la Protection des Données (DPO) : ATD16 ;
  - Désignation du DPO à la Commission Nationale Informatique et Libertés (CNIL) : effectuée le 25/01/2019

Définitions :

- Responsable de traitement : La personne physique ou morale, l'autorité publique, le service qui détermine les finalités et les moyens du traitement
- Donnée personnelle : Toute information se rapportant à une personne physique identifiée ou qui peut être identifiée directement ou indirectement
- Traitement de données personnelles : Toute opération effectuée ou non à l'aide de procédés automatisés et appliqués à des données

DEMARCHE GLOBALE

2 Une démarche globale en 3 temps

(Cf. tableau en fin de paragraphe)

Dans le souci d'une démarche d'amélioration continue, l'ATD16 vous propose ces différentes étapes qui permettront à votre collectivité de se mettre en conformité avec les exigences du RGPD.

Année 1 :

Les objectifs de cette première année sont de plusieurs ordres. En premier lieu, il s'agira de réaliser un inventaire des traitements de données faits par le responsable de traitement. En deuxième lieu, il conviendra de réaliser le registre des activités de traitement (**Article 30 du RGPD**). En troisième lieu, cette année sera consacrée à l'établissement de préconisations « initiales » qui ont essentiellement pour objectif la mise en œuvre de mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel qui sont exposées aux risques les plus importants. Enfin, il appartiendra au Délégué à la Protection des Données d'écrire aux sous-traitants principaux de la commune concernée afin de les informer, notamment, de la nomination d'un Délégué et de préciser ses coordonnées.

Année 2 :

La seconde année permettra tout d'abord d'effectuer un point sur les éléments préconisés en première année et leurs mises en œuvre. Lors de cette deuxième année, il sera également important de faire un état des lieux des changements et nouveautés qui auront pu apparaître au sein de la commune d'Aussac-Vallade. Enfin, il sera nécessaire de se pencher plus en profondeur sur les éléments qui n'auront pas pu être développé en première année, à savoir l'évaluation et la mise en place des durées de conservation ou délais d'effacement des données, l'évaluation de la proportionnalité et de la nécessité des opérations de collectes au regard des finalités ou bien encore la recherche de mesures de sécurités techniques et organisationnelles plus poussées. Enfin, il appartiendra au Délégué à la Protection des Données d'écrire aux sous-traitants de la commune concernée qui n'auront pas été informés en année une de la nomination d'un Délégué à la Protection des données.

Année 3 et suivantes :

Ces années permettront de consolider la démarche et de la faire entrer dans une routine vertueuse.

Les trois temps sont synthétisés dans le tableau ci-après.

DEMARCHE GLOBALE

	Inventaires des données	Registre de traitement	AIPD	Formation en ligne	Privacy by Design	Préconisations
Année 1	✓	✓	Partielle	1er trimestre 2020	Pour tout nouveau traitement	*Initiales*
Année 2	Si compléments	Si compléments	Totale	Toute l'année	Pour tout nouveau traitement	*Avancées*
Année 3 et suivantes	Si compléments	Si compléments	Si compléments	Toute l'année	Pour tout nouveau traitement	*Avancées*

Définitions :

- Registre de Traitement : Document de recensement qui reflète la réalité des traitements de données personnelles réalisés par l'établissement.
- AIPD : Analyse d'impact relative à la protection des données.
- Formation en ligne : Capsule de formation en ligne permettant une meilleure sensibilisation des personnes qui traitent au quotidien des données personnelles.
- Portail des droits : plateforme informatisée permettant à toutes les personnes concernées d'exercer leurs droits sur leurs données (droit d'accès, droit à l'information…).
- Privacy by Design (ou protection des données dès la conception) : Aide à la mise en œuvre de mesures de sécurité dès lors qu'un nouveau traitement de données personnelles est envisagé par le responsable de traitement.
- Sous-traitant : La personne physique ou morale, l'autorité publique, le service qui traite des données à caractère personnel pour le compte du responsable de traitement

3 Environnement technique

3.1 Supports informatiques

INFORMATIQUE	Poste de travail	Imprimante	Serveur	Internet	Logiciel métier (de gestion)	Messagerie
Prestataire (Sous-Traitant RGPD)	ATD16	Ricoh (ancien)		OVH	ATD16	Nom de domaine propre
Système	Unités fixes / Windows 10 (secrétaire de mairie) et 7 / Antivirus à jour	Copieur / Photocopieur	Poste Maître	Réseau Filaire / Wifi	HOL / SIRAP	Thunderbird
Nombre	5		1			
Mesures de gestion des accès (Identification / Traçabilité)	Session d'identification Windows gérée		Dossiers partagés		Session d'identification Windows gérée	Session d'identification Windows gérée (Hébergement sur les serveurs de l'ATD16)
Mesures de sauvegardes	2 Disques Dur Externes stockés en mairie (2 sauvegardes locales)				Sauvegarde externalisée (Griffon Free + SIRAP)	2 disques durs externes stockés en mairie (2 sauvegardes locales)
Fréquences de sauvegarde	Journalier				Journalier	Journalier

3.2 Locaux & Accès

LOCAUX	Mairie	Commentaires	Archives
Fermeture accès principal	Oui	Même en cas d'absence momentanée du personnel	À l'étage de la mairie
Système de sécurité (clé, badge, alarme, vidéo-surveillance…)	Non		
Bureaux fermés	Non		Oui
Armoires fermées	Oui		Non
Gestions des clés	Oui		Oui

4 Bilan de l'inventaire et exposition aux risques

La nomenclature et les critères d'analyse sont détaillés en annexe 1.

Les résultats de l'analyse sur la *vraisemblance de perte, modification ou vol* et *d'exposition au risque* après Plan d'Action prennent en compte la réalisation par la commune des mesures prioritaires (Partie 5 *Le plan d'action*).

De plus, en cas de niveau de vraisemblance différent pour un même traitement, il sera retenu le niveau de vraisemblance le plus élevé dans les résultats d'analyse (exemple : en cas de niveau de vraisemblance minime concernant le contrôle des accès et de niveau fort concernant la pérennité, ce dernier sera pris en compte)

Enfin, les données mises à dispositions du public (site internet, bulletin municipal, affichage des délibérations, …) seront analysées selon une nomenclature et des critères distincts (le contrôle des accès n'étant pas pertinent pour une donnée mise à disposition du public). En revanche, pour ces données, sera appréhendé la base juridique de cette mise à disposition conformément à **l'article 6 du RGPD** (obligation légale ou règlementaire, consentement…)

																AVANT PLAN D'ACTION		APRÈS PLAN D'ACTION	
Traitements		Données personnelles								Impact en cas de perte, modification ou vol (Gravité)	Support informatique	Contrôle d'accès informatique	Sauvegarde informatique	Support physique	Contrôle d'accès physique	Vraisemblance de perte, modification ou vol	Exposition au risque	Vraisemblance après plan d'action	Exposition au risque après plan d'action
		Nom	Prénom	Adresse	Mail	Naissance		N° tel	Autres										
						Date	Lieu												
1	**Vie du conseil**	X	X	X	X	X	X	X	Délégation	Conséquences minimes	REDA / Messagerie / STELA	2 accès ou plus gérés	1 sauvegarde distante			Minime	Négligeable	Minime	Négligeable
2	**Listes électorales**	X	X	X	X	X	X	X	Nationalité, numéro d'électeur	Conséquences importantes	Plateforme ÉLIRE / HOL	2 accès ou plus gérés	1 sauvegarde distante	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
3	**État-Civil**	X	X	X		X	X	X	Date et cause du décès, extrait de jugement de divorce, filiation, acte de reconnaissance d'un enfant, mesures judiciaires (tutelle, curatelle)	Conséquences graves	Logiciel HOL / COMEDEC	2 accès ou plus gérés	1 sauvegarde distante	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Significatif	Minime	Significatif
	PACS	X	X	X		X	X	X	Dissolution précédent PACS	Conséquences importantes	Logiciel HOL	2 accès ou plus gérés	1 sauvegarde distante	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
	Recensement militaire	X	X	X	X	X	X	X	Filiation, diplôme, lieu de scolarité	Conséquences importantes	Plateforme MaJDC	2 accès ou plus gérés	1 sauvegarde distante	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable

BILAN DE L' INVENTAIRE ET EXPOSITION AUX RISQUES

Traitements		Données personnelles								Impact en cas de perte, modification ou vol (Gravité)	Support informatique	Contrôle d'accès informatique	Sauvegarde informatique	Support physique	Contrôle d'accès physique	AVANT PLAN D'ACTION		APRÈS PLAN D'ACTION	
		Nom	Prénom	Adresse	Mail	Naissance		N° tel	Autres							Vraisemblance de perte, modification ou vol	Exposition au risque	Vraisemblance après plan d'action	Exposition au risque après plan d'action
						Date	Lieu												
ST1	**Recensement population**	X	X	X		X			Composition du foyer, profession, description de l'habitation (surface, nombre de pièces)	Conséquences minimes	Logiciel OMER	2 accès ou plus gérés	1 sauvegarde distante	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
4	**Licence et débit temporaire de boissons**	X	X	X		X		X	Permis d'exploitation	Conséquences minimes	Logiciel HOL	2 accès ou plus gérés	1 sauvegarde distante	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
	Police administrative (Arrêtés)	X	X	X						Conséquences minimes	Logiciel HOL	2 accès ou plus gérés	1 sauvegarde distante	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
5	**Cadastre**	X	X	X	X	X	X	X	Taxes foncière et d'habitation (DGFIP), nombre de pièces, type de propriété, parcelle, surface, date de mouvement, données sur l'habitat, montant des transactions	Conséquences importantes	X'MAP / VISDGI	2 accès ou plus gérés	1 sauvegarde distante		NC	Minime	Négligeable	Minime	Négligeable
	Délivrance des autorisations d'urbanisme	X	X	X			X	X	données sur le projet (plan, constructeur…)	Conséquences minimes	R'ADS	2 accès ou plus gérés	1 sauvegarde distante	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
	Cimetière	X	X	X	X	X	X	X	Numéro de concession, emplacement, durée de la concession, date de décès	Conséquences minimes	Logiciel Carta Cim	2 accès ou plus gérés	1 sauvegarde distante	Dossier papier (mis sous clé)	2 accès géré	Minime	Négligeable	Minime	Négligeable
7	**Marchés publics**	X	X	X	X			X	Numéro de SIRET	Conséquences minimes	AWS / Chorus / Excel / Word	1 accès géré	2 sauvegardes gérées localement		NC	Probable	Négligeable	Probable	Négligeable
	Comptabilité	X	X	X					Dettes (Factures), coordonnées bancaires	Conséquences minimes	Logiciel HOL	2 accès ou plus gérés	1 sauvegarde distante	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
8	**Assurance (Responsabilité civile / Flotte automobile)**	X	X	X					Nom, prénom, adresse, déclaration d'incident	Conséquences minimes	Plateforme Assureur	2 accès ou plus gérés	1 sauvegarde distante	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable

BILAN DE L' INVENTAIRE ET EXPOSITION AUX RISQUES

	Traitements	Données personnelles								Impact en cas de perte, modification ou vol (Gravité)	Support informatique	Contrôle d'accès informatique	Sauvegarde informatique	Support physique	Contrôle d'accès physique	AVANT PLAN D'ACTION		APRÈS PLAN D'ACTION	
		Nom	Prénom	Adresse	Mail	Naissance		N° tel	Autres							Vraisemblance de perte, modification ou vol	Exposition au risque	Vraisemblance après plan d'action	Exposition au risque après plan d'action
						Date	Lieu												
8	**Locations (dont salles et matériels)**	X	X	X	X			X	Attestation d'assurance, justificatifs de revenus, avis d'imposition, coordonnées bancaires (chèque, chèque de caution)	Conséquences minimes		NC	NC	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
	Domaine immobilier	X	X	X	X	X	X	X	Coordonnée bancaires	Conséquences importantes		NC	NC	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
9	**Gestion du personnel**	X	X	X	X	X	X	X	Numéro de sécurité sociale, adresse, coordonnées bancaires, identité des enfants, arrêts de travail, évènements familiaux, décharges syndicales et locales, carrière, taux prélevé, garantie de maintien de salaire, retraite complémentaire, extrait de casier judiciaire	Conséquences graves	Logiciel HOL	2 accès ou plus gérés	1 sauvegarde distante	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Significatif	Minime	Significatif
	Recrutement	X	X	X	X	X	X	X	Éléments de carrière	Conséquences minimes		NC	NC	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
10	**Signalements, planification et suivi**	X	X	X	X			X	Objet de la demande	Conséquences minimes	Messagerie / SVE	2 accès ou plus gérés	1 sauvegarde distante		NC	Minime	Négligeable	Minime	Négligeable
11	**Repas anciens**	X	X	X		X		X		Conséquences minimes		NC	NC	Dossier papier (mis sous clé) **extraction de la liste électorale**	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
	Accueil nouveaux arrivants	X	X	X				X		Conséquences minimes		NC	NC	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
	Vœux du maire	X	X	X				X		Conséquences minimes		NC	NC	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable

BILAN DE L' INVENTAIRE ET EXPOSITION AUX RISQUES

Traitements		Données personnelles								Impact en cas de perte, modification ou vol (Gravité)	Support informatique	Contrôle d'accès informatique	Sauvegarde informatique	Support physique	Contrôle d'accès physique	AVANT PLAN D'ACTION		APRÈS PLAN D'ACTION	
		Nom	Prénom	Adresse	Mail	Naissance		N° tel	Autres							Vraisemblance de perte, modification ou vol	Exposition au risque	Vraisemblance après plan d'action	Exposition au risque après plan d'action
						Date	Lieu												
13	**École (inscription)**	X	X	X				X	Élève : nom, prénom Responsables légaux : nom, prénom, adresse, téléphone professionnel et personnel Motif de la dérogation	Conséquences importantes		NC	NC	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable
15	**Associations**	X	X	X	X			X		Conséquences minimes		NC	NC	Dossier papier (mis sous clé)	2 accès ou plus gérés	Minime	Négligeable	Minime	Négligeable

Données mises à disposition du public

Traitements	Données personnelles	Support de diffusion	Base Juridique de la diffusion
Diffusion Délibération et comptes rendus	Nom, prénom	Délibérations et comptes rendus	Obligation légale ou règlementaire
Communication	Données d'état civil : nom, prénom, date (pour des avis de décès, mariages, naissances).	Bulletin	**Absence de consentement**

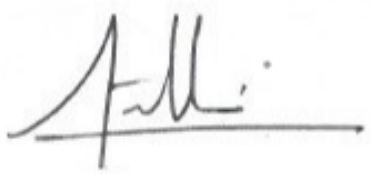
5 Le plan d'action

« Récapitulation des préconisations »

Il est à noter que les mesures à moyen ou long terme pourront être prises dans un second temps (sur les conseils et avec l'aide du DPO) afin de faire entrer la commune dans une routine vertueuse.

 **Mesures prioritaires**	 **Mesures à moyen ou long terme**
- (Le cas échéant), il serait opportun de **migrer le système d'exploitation sous Windows 10** car les mises à jour de sécurité ne sont plus faites par Microsoft sur Windows 7 depuis la fin du mois de janvier 2020. - Mettre en place une **procédure adéquate afin de demander l'autorisation au préalable des personnes concernées afin de pouvoir mettre leurs données sur tout support de communication communal** (Bulletin Municipal entre autres)	- (Le cas échéant), mettre en place une procédure adéquate afin **d'assurer l'organisation du repas des anciens sans effectuer de détournement de finalité** (par exemple par un système d'affichage ou de coupon-réponse inscrit sur le Bulletin municipal) - Dans la mesure du possible, mettre en place **une solution de sauvegarde externalisée pour les données serveur (et messagerie)**. Il peut s'agir d'un système de sauvegarde complètement externalisée de type cloud ou bien du stockage d'un des deux disques durs externes (en alternance avec le premier) dans un endroit sécurisé situé dans un bâtiment indépendant de la mairie afin de s'assurer, notamment, contre le risque d'incendie - **Assurer une gestion des traitements en conformité avec les durées de conservation** recommandées par les instructions publiées par la Direction des Archives de France - (Le cas échéant), **mettre en place des mesures de sécurité physique supplémentaires** pour les dossiers agents ainsi que pour les Registres d'État-Civil (exemple : armoire forte)

Le Directeur de l'ATD16,



Ronan MÉVELLEC

Annexe 1 : Nomenclature et critères d'analyse de l'évaluation des risques

EXPOSITION AUX RISQUES =

Impact x Vraisemblance

EXPOSITION AUX RISQUES

Impact *				
Conséquences graves	Significatif	Significatif	Critique	Critique
Conséquences importantes	Négligeable	Significatif	Significatif	Critique
Conséquences minimes	Négligeable	Négligeable	Significatif	Significatif
	Minime	**Probable**	**Forte**	**Maximale**
	Vraisemblance **			

ANNEXE 1

***** Impact pour la personne physique concernée

Conséquences graves	**2 critères ou plus de l'AIPD**
Conséquences importantes	**1 critère de l'AIPD**
Conséquences minimes	**Aucun critère de l'AIPD**

Une **Analyse d'Impact relative à la Protection des Données (AIPD)** doit obligatoirement être menée quand le traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées* ».

- Soit le traitement envisagé figure dans la liste des types d'opérations de traitements pour lesquelles la CNIL a estimé obligatoire de réaliser une AIPD.
- Soit le traitement remplit au moins **deux des neuf critères** issus des lignes directrices du G29 :
  - Évaluation/*scoring* (y compris le profilage) ;
  - Décision automatique avec effet légal ou similaire ;
  - Surveillance systématique ;
  - Collecte de données sensibles ou données à caractère hautement personnel ;
  - Collecte de données personnelles à large échelle ;
  - Croisement de données ;
  - Personnes vulnérables (patients, personnes âgées, enfants, *etc.*) ;
  - Usage innovant (utilisation d'une nouvelle technologie) ;
  - Exclusion du bénéfice d'un droit/contrat.

ANNEXE 1

** Niveau de vraisemblance (de perte, modification ou vol)

Niveau de vraisemblance		Contrôle des accès	Pérennité
Minime	cela ne devrait pas se (re-)produire	2 accès ou plus gérés	2 sauvegardes gérées localement ou 1 sauvegarde distante
Probable	cela pourrait se reproduire	1 accès géré	1 sauvegarde locale gérée
Forte	cela devrait se (re-)produire un jour ou l'autre	1 accès non ou partiellement géré	1 sauvegarde non ou partiellement gérée
Maximale	cela va certainement se (re-)produire d'un jour à l'autre	Aucun accès géré	Pas de sauvegarde

Exposition aux risques

Critique	Mesures urgentes
Significatif	Mesures à moyen terme
Négligeable	Mesures à long terme