



Guide d'utilisation du logiciel MADIS

Version du 16/12/2021 . Madis V1.7.12



SIN - Service Intercommunal du Numérique

Agence Publique de Gestion Locale

Cité administrative

Rue Auguste Renoir

CS 40609

64006 PAU CEDEX

Courriel : dpo@apg164.fr

Tel : 05 59 90 18 11

Sommaire

A.	Présentation générale de MADIS	1
B.	Se connecter à MADIS	1
C.	Présentation de la page d'accueil	2
C.1	Tableau de bord :	2
C.2	Présentation du menu	3
C.2.1	Paramétrage : ma collectivité	4
C.2.2	Mon compte utilisateur	6
D.	Les registres	6
D.1	Le registre des traitements	6
D.2	Le registre des sous-traitants	13
D.3	Les demandes de personnes concernées	14
D.3.1	Créer une nouvelle demande	14
D.4	Les registres de violations de données	16
E.	Les actions de protection	18
E.1	Modifier une action de protection	18
E.2	Créer une action de protection	19
F.	Indice de maturité	20
G.	Plan d'actions	23
H.	Générer un bilan	23
I.	Gestion de la preuve	24

A. Présentation générale de MADIS

Madis est un logiciel conçu pour accompagner les collectivités à la mise en œuvre de leur conformité au règlement européen de protection des données (RGPD).

Cette notice, basée sur celle communiquée avec le logiciel, sera amenée à évoluer selon les évolutions juridiques en matière de protection des données et les besoins des collectivités.

B. Connexion au Logiciel de Protection des données

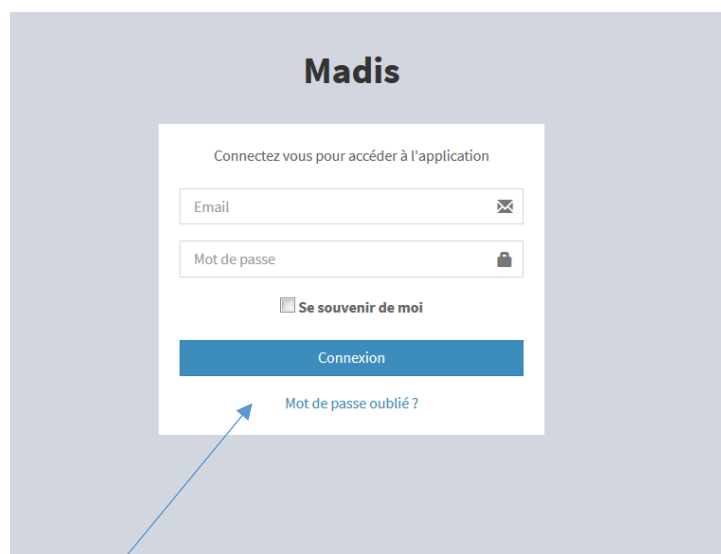
Pour vous connecter, vous devez avoir un compte.

Lors de votre première connexion sure : <https://dpo.apgl64.fr/>, je clique sur « Mot de passe oublié » et je renseigne mon adresse courriel.



L'adresse courriel rattachée à votre compte est celle communiquée au service Protection des Données.

Si aucune adresse n'a été communiquée, l'adresse courriel à renseigner est, par défaut, celle de la collectivité.



En cas d'oubli de mot de passe, cliquez ici. Vous devez changer votre nouveau mot de passe en respectant les règles de sécurité suivantes : 14 caractères, une lettre majuscule/minuscule minimum, au moins un chiffre et un caractère spécial.

C. Présentation de la page d'accueil

Une fois connecté, différents modules vous permettent d'effectuer la saisie des registres, de documenter votre mise en conformité et de piloter sa mise en œuvre.

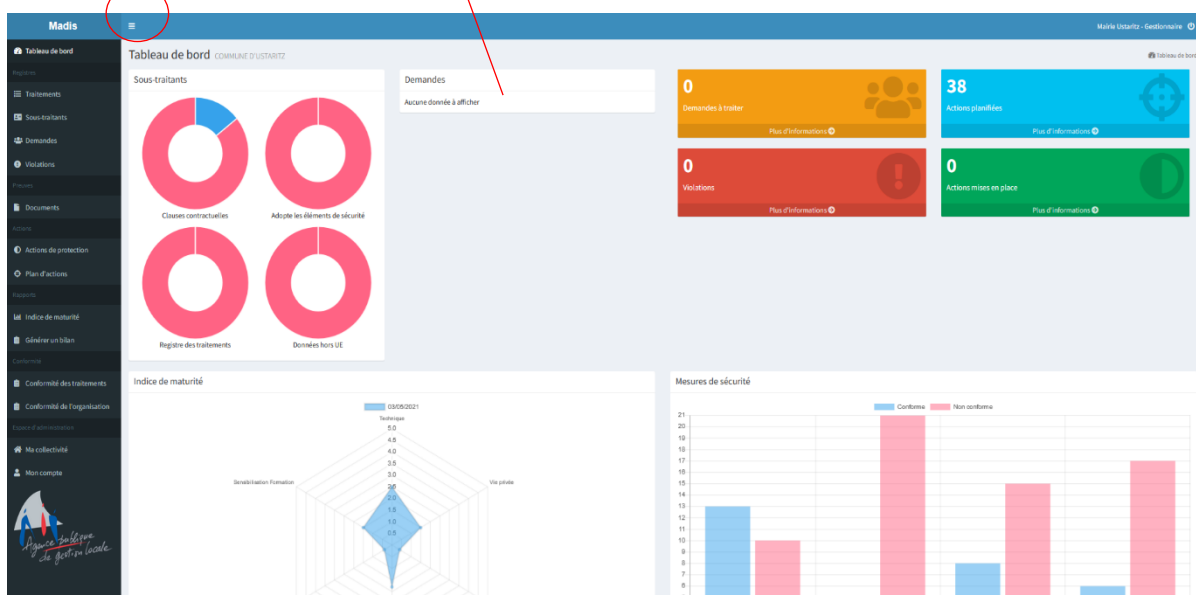
C.1 Tableau de bord :

La fenêtre principale vous permet de visualiser en un coup d'œil l'état d'avancement de votre mise en conformité.

Réduire le bandeau de gauche

Le détail des contenus est affecté lors du survol de la souris

Statistiques + accès rapide pour 4 modules figurants également dans le menu à gauche.



Sous-traitants

Dernier indice de maturité (en bleu) et avant dernier (en rouge).

Vous pouvez visualiser un seul indice : en cliquant sur une date, vous supprimez l'affichage du radar correspondant

Mesures de sécurité

Graphique synthétisant les mesures de sécurité de base sur les traitements informatisés.

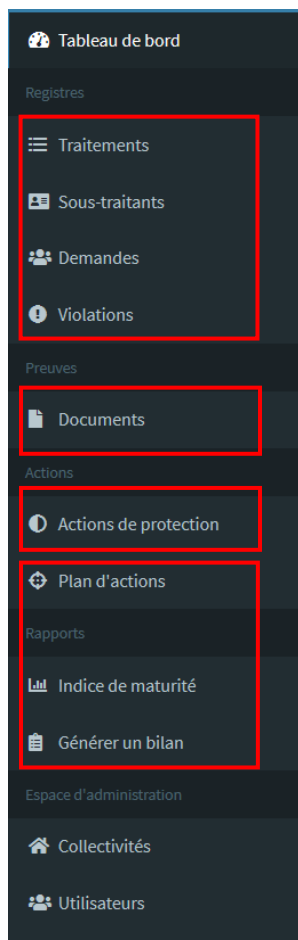


Indice de maturité

Dernier indice de maturité (en bleu) et avant dernier (en rouge).

Vous pouvez visualiser un seul indice : en cliquant sur une date, vous supprimez l'affichage du radar correspondant

C.2 Présentation du menu



Ici les 4 registres à renseigner puis tenir à jour.

Insérez ici les justificatifs permettant de documenter la conformité (Contrat d'accompagnement à la délégation à la protection des données, attestations de présences, politique de gestion des données ...)

Recensez ici l'ensemble des actions de protection mises en place dans votre collectivité. Une liste d'actions triées par thématique vous est proposée. Vous pouvez vous en inspirer mais vous pouvez également ajouter des actions de protection que vous avez déjà mises en place et qui ne sont pas dans cette liste.

Ici les points abordés en Gouvernance

Ci-après les explications (p.4)

C.2.1 Paramétrage : ma collectivité

Vous pouvez visualiser les données de votre collectivité. Vous n'avez pas la possibilité de modifier les informations générales et l'adresse. En cas de rectification souhaitée, merci de faire votre demande à l'adresse dpo@apgl64.fr.

Vous avez la possibilité de modifier les différents acteurs de votre mise en conformité (réfèrent opérationnel, responsable informatique, éventuellement responsable de traitement).

Informations générales		Adresse	
Nom	SOCLE COMMUNE MAIRIE	Adresse	A RENSEIGNER
Nom court	MAIRIE	Complément d'adresse	
Type	Autre	Code postal	64999
SIREN	111 111 111	Ville	A RENSEIGNER
Statut	Actif	Code INSEE	64999
Site internet			
Module conformité des traitements	Non		
Module conformité de l'organisation	Non		

Responsable de traitement		Responsable informatique		Réfèrent Opérationnel		DPD	
Civilité	Madame	Différent du Réfèrent Opérationnel Non		Civilité	Madame	Différent du DPD moral Non	
Prénom	A RENSEIGNER			Prénom	A RENSEIGNER	Civilité	m
Nom	A RENSEIGNER			Nom	A RENSEIGNER	Prénom	Service
Fonction	A RENSEIGNER			Fonction	A RENSEIGNER	Nom	DPD
Email	nomail@nomail.apgl64.fr			Email	nomail@nomail.apgl64.fr	Fonction	Délégué à la protection des données
N° tél.	0501010101			N° tél.	0501010101	Email	dpo@apgl64.fr
						N° tél.	0559901811

Responsable de traitement : personne qui détermine les moyens et finalités d'un traitement (responsabilité de la collectivité)

Réfèrent opérationnel : personne qui tient à jour les registres

DPD	
Différent du DPD moral	Oui
Civilité	Monsieur
Prénom	Attighou
Nom	DIALLO
Fonction	Délégué à la protection des données - DPO
Email	attighou.diallo@apgl64.fr
N° tél.	0559901811

N'oubliez pas de cocher ici « oui » si votre DPO est différent du DPO APGL 64

Bilan paragraphe "Engagement de la direction"

B I | ← → | ☰ ☷ | ☰ ☷ | ☰ ☷ | ☰ ☷

Bilan paragraphe "Principe d'amélioration continue"

B I | ← → | ☰ ☷ | ☰ ☷ | ☰ ☷ | ☰ ☷

body p

C.2.2 Mon compte utilisateur

Votre compte utilisateur vous permet de vous identifier (nom, prénom, adresse mail). Vous pouvez y accéder en cliquant sur « **mon compte** » et le modifier au besoin.

Éditer un utilisateur Georges Lemaire

Tableau de bord - Éditer mon profil

Vos informations

Prénom* Georges

Nom* Lemaire

E-mail* g.lemaire@demoville.solaris.fr

Soumettre

Pour votre information

- Vous disposez d'un compte associé à la collectivité **Commune de Demoville**.
- Vous disposez des droits de **lecture** sur votre collectivité.
- Vous disposez des droits d'**écriture** sur votre collectivité.

Affichage des droits

Madis

Connectez vous pour accéder à l'application

Email

Mot de passe

Se souvenir de moi

Connexion

Mot de passe oublié ?

Rappel : En cas d'oubli de votre mot de passe vous avez la possibilité de le réinitialiser en cliquant ici

D. Les registres

D.1 Le registre des traitements

Le registre des traitements permet de recenser l'ensemble des traitements de données à caractère personnel de votre collectivité.

Lorsque vous cliquez sur « **traitements** », la fenêtre ci-dessous s'ouvre. Il est possible ici de consulter ou de créer.

Lors de la première connexion sur votre profil, l'APGL 64 vous aura créé une liste de traitements. Vous devrez vérifier et compléter chaque traitement avant de les valider en traitement.

Nom	Collectivité	Actions
AFFAIRES SCOLAIRES, PÉRI-SCOLAIRES, EXTRASCOLAIRES ET PETITE ENFANCE	SOCLE COMMUNE MAIRIE	Modifier Supprimer
CCAS - Aides financières facultatives	SOCLE COMMUNE MAIRIE	Modifier Supprimer
CCAS - Aidant démarches administratives	SOCLE COMMUNE MAIRIE	Modifier Supprimer
CCAS - Assistance sociale	SOCLE COMMUNE MAIRIE	Modifier Supprimer
CCAS - Domiciliation	SOCLE COMMUNE MAIRIE	Modifier Supprimer
CCAS - Gestion des aides sociales légales	SOCLE COMMUNE MAIRIE	Modifier Supprimer
CCAS - Gestion du conseil d'administration	SOCLE COMMUNE MAIRIE	Modifier Supprimer
CCAS - Jardins familiaux	SOCLE COMMUNE MAIRIE	Modifier Supprimer
CCAS - Présence verte	SOCLE COMMUNE MAIRIE	Modifier Supprimer
MAIRIE - Accès Public à Internet - Hot Spot Wi-Fi	SOCLE COMMUNE MAIRIE	Modifier Supprimer
MAIRIE - Accueil des nouveaux arrivants sur la commune	SOCLE COMMUNE MAIRIE	Modifier Supprimer
MAIRIE - Adressage	SOCLE COMMUNE MAIRIE	Modifier Supprimer
MAIRIE - AFA - Acte à la forme administrative	SOCLE COMMUNE MAIRIE	Modifier Supprimer
MAIRIE - Affaires scolaires - Portail famille (espace web)	SOCLE COMMUNE MAIRIE	Modifier Supprimer
MAIRIE - Annuaire des contacts	SOCLE COMMUNE MAIRIE	Modifier Supprimer

Il vous sera possible, par la suite, de rajouter d'autres traitements en créant de nouvelles fiches de traitement.

Zoom sur la création d'un nouveau traitement :

Lorsque vous cliquez sur « nouveau traitement », la fenêtre ci-dessous s'affiche.

Informations générales

Nom : Indiquez ici l'intitulé précis du traitement.

Finalités : Objectifs du traitement et ses fonctions – ex. pour une activité de formation des personnels : suivi des demandes et des périodes de formations effectuées, et organisation des sessions et évaluation des connaissances.

Plusieurs finalités peuvent être renseignées. Peuvent être précisées également les sous-finalités.

Gestionnaire : Personne(s) ou service qui gère le traitement. Peut être différent du responsable de traitement ou du référent opérationnel.

Statut : Dans le logiciel, le statut actif est coché par défaut lors de la création d'une nouvelle fiche. Toutefois pour les traitements déjà pré-identifiés par l'APGL 64, ils seront « inactifs » et vous devrez les activer après vérification pour les intégrer à votre registre de traitements

Base légale : La base légale est ce qui autorise légalement la mise en œuvre du traitement et doit être définie pour chaque finalité.

Il faut indiquer une seule base légale par finalité. Si plusieurs finalités sont poursuivies par un traitement, une base légale doit être définie pour chacune d'entre elles.

Toute base légale doit être justifiée.

Justification de la base légale : Indiquez ici les références du texte réglementaire (ex. CGCT) qui permet de justifier le choix de la base légale. Vous pouvez également indiquer le texte réglementaire qui vous permet de justifier votre choix du délai de conservation

Les champs précédés d'un * sont obligatoires

Observations : Certaines précisions y sont mentionnées (détails quant aux personnes concernées, DUA à respecter etc..)

Ci-dessous un exemple d' « informations générales » pré-rempli :

Informations générales	
Nom	Gestion de la cantine
Finalités	Sous-finalités: Facturation des repas Gestion des repas spécifiques (allergies, régime)- Suivi sanitaire (Fiche sanitaire de liaison Cerfa 1008*02/Rapport incident)
Gestionnaire	
Statut	Actif
Base légale	L'exécution d'un contrat
Justification de la base légale	
Observations	Personnes concernées: enfants d'administrés, personnes à contacter en cas d'incident, personnes habilitées à récupérer l'enfant Facturation: 10 ans Données d'état civil de l'enfant et des parents: année scolaire Suivi des impayés: durée de remboursement de la somme due Données de santé: conservation le temps de fréquentation du service NS-058

En tant que : Ce champ permet d'identifier si le traitement est réalisé en tant que "Responsable de traitement", "Responsabilité conjointe" ou "Sous-traitant". Par défaut, le statut « responsable de traitement » sera appliqué.

En tant que*	Responsable de traitement
Gestionnaire	<ul style="list-style-type: none"> Responsable de traitement Sous-traitant Responsabilité conjointe

Les catégories de données

Vous devez préciser ici toutes les catégories de données concernées par le traitement :

Catégorie des données	
Catégorie de données	Date, lieu de naissance, Situation familiale, Coordonnées postales, Situation fiscale
Autres catégories	<ul style="list-style-type: none"> Nom, Prénom Date, lieu de naissance ✓ Situation familiale ✓ Filiation Coordonnées postales ✓ Coordonnées téléphoniques
Destination	<ul style="list-style-type: none"> Information bancaire Situation bancaire Patrimoine Situation fiscale ✓ Situation professionnelle
Catégorie de destinataires	<ul style="list-style-type: none"> Revenus Emails Adresse IP Connexion Géolocalisation Numéro de CAF Santé Numéro de Sécurité Sociale Pièces d'identité Photos-vidéos Appartenance Syndicale Opinion politique ou religieuse
Sous-traitants	
Traitement spéci	

Rappel du détail des catégories :

- *Données d'identification, état civil : nom, prénom, adresse, téléphone, courriel, date et lieu de naissance, photographies, n°CAF, autres n°...*
- *Vie personnelle : habitude de vie, situation familiale,*
- *Vie professionnelle : scolarité, formation, adresse professionnelle, CV*
- *Informations d'ordre économique et financier : patrimoine, coordonnées bancaires, situation fiscale, éléments de salaire...*
- *Données de connexion : adresse IP, logs, identifiants de connexion*
- *Données de localisation : déplacement, données GPS, GSM*
- *Données de navigation sur le site web : cookies, données de navigation, mesures d'audience*

Détails

<input type="checkbox"/>	Personnes concernées*	<input type="checkbox"/>	Particuliers	<input type="text" value="Précisez"/>
<input type="checkbox"/>		<input type="checkbox"/>	Internautes	<input type="text" value="Précisez"/>
<input type="checkbox"/>		<input type="checkbox"/>	Agents	<input type="text" value="Précisez"/>
<input type="checkbox"/>		<input type="checkbox"/>	Élus	<input type="text" value="Précisez"/>
<input type="checkbox"/>		<input type="checkbox"/>	Entreprises	<input type="text" value="Précisez"/>
<input type="checkbox"/>		<input type="checkbox"/>	Partenaires	<input type="text" value="Précisez"/>
<input type="checkbox"/>		<input type="checkbox"/>	Autres	<input type="text" value="Précisez"/>

Nombre de personnes concernées : ce champ permet de préciser l'estimation du nombre de personnes concernées par le traitement (nécessaire pour l'analyse d'impact plus tard et éventuellement en cas de violation de données à caractère personnel).

Nombre de personnes concernées

Délai de conservation Jour(s)

Autre délai

Données d'état civil de l'enfant et des parents: année scolaire
 Suivi des impayés: durée de remboursement de la somme due
 Données de santé: conservation le temps de fréquentation du service

Rappel: Le délai de conservation doit correspondre à la durée de la base active des données du traitement, elle doit pouvoir s'appuyer sur une justification (base légale par exemple ou se référer à la méthodologie mise en place pour le traitement). Si vous ne pouvez pas indiquer une durée chiffrée, préciser les critères utilisés pour déterminer le délai de conservation (ex : 3 ans à compter de la fin de la relation contractuelle)

Sort final : ce champ permet d'identifier le sort réservé aux données à l'issue du traitement.

Sort final

Origine des données

Moyens de la collecte

- Précisez
- Destruction
- Conservation
- Versement
- Tri

Origine des données : ce champ permet d'identifier l'origine des données

Origine des données

Moyens de la collecte

Précisez	▼
Précisez	
Formulaire web	
Formulaire papier	
Contrat	
Liste reçu	
Document interne	

Destination	
Catégorie de destinataires	Service interne: cantine, agents techniques Partenaires institutionnels: DGFiP, Services de secours (SDIS et SMUR)
Sous-traitants	CDG46 Cosoluce - éditeur de logiciel Créateur Site web Hébergeur site web imprimeur

Indiquez ici les destinataires des données à caractère personnel (service, organisation extérieure, partenaires, tiers autorisés etc.)

Apparaissent ici tous les sous-traitants identifiés dans le registre des sous-traitants. Pour sélectionner le(s) sous-traitant(s) rattaché(s) à ce traitement, veuillez le(s) sélectionner à l'aide la touche Ctrl (sur ordinateur) ou les cocher si vous travaillez sur tablette.

Les **mesures de sécurité** renseignées ici sont propres à chaque traitement concerné.

Mesures de sécurité

- Contrôle d'accès** ← Ex : accès via login/mot de passe ou certification, gestion des habilitations, badges
- Traçabilité** ← Ex : journalisation des accès utilisateurs, données enregistrées (identifiant, date et heure de connexion, actions)
- Sauvegarde** ← Préciser ici le type de sauvegarde (support, interne/externe, fréquence...)
- Mise à jour** ← Mises à jour des logiciels, de l'environnement, contrat de mise à jour etc.
- Autres** ← Préciser toute autre mesure que l'on souhaite documenter

Un ou plusieurs traitement(s) spécifique(s) peuvent conditionner une analyse d'impact notamment s'ils sont croisés avec des données sensibles.









Autres éléments relatifs à la sécurité du traitement :

Je suis en capacité de ressortir les personnes habilitées : Le gestionnaire est en capacité de ressortir les personnes habilitées en cas de nécessité ou de contrôle. Le gestionnaire a documenté ou a connaissance de la marche à suivre pour obtenir cette information.

La personne ou la procédure qui permet d'ouvrir des comptes est clairement identifiée : Le gestionnaire sait où se trouve la personne ou la procédure permettant de gérer les comptes ayant un accès aux données.

Les spécificités de sensibilisation liées à ce traitement sont délivrées : Les personnes ayant accès à ce traitement ont fait l'objet d'une sensibilisation y compris aux spécificités de ce traitement.

Traitement spécifique

- Surveillance systématique  *Surveillance systématique de personnes (ex: télésurveillance)*
- Collecte à large échelle  *Ex : qui visent à traiter un volume considérable de données à caractère personnel au niveau régional*
- Personnes vulnérables  *Personnes âgées, enfant de moins de 15 ans, personne en situation de handicap, patients, employés...*
- Croisement de données  *Croisement ou combinaison d'ensemble de données*
- Évaluation ou notation 
- Décisions automatisées avec effet 
- Exclusion automatique d'un service 
- Usage innovant 

D.2 Le registre des sous-traitants

Un sous-traitant est un prestataire de services qui traite des données à caractère personnel pour le compte, sur instruction et sous l'autorité du responsable de traitement.

Le registre des sous-traitants vise à recenser les sous-traitants de votre collectivité et à effectuer le suivi de leur conformité au RGPD (clauses contractuelles vérifiées, conforme au RGPD)

Lorsque vous cliquez sur « **sous-traitants** », la fenêtre ci-dessous s'ouvre. Vous visualisez ainsi l'ensemble des sous-traitants recensés dans votre collectivité.

Nom	Clauses contractuelles vérifiées	Conforme RGPD	Actions
Berger Levrault	Oui	Oui	Modifier
CDG46	Non	Non	Modifier Supprimer
Créateur Site web	Non	Non	Modifier Supprimer
Hébergeur site web	Non	Non	Modifier Supprimer
Imprimeur	Non	Non	Modifier
Opérateur messagerie	Non	Oui	Modifier Supprimer
Relieur	Non	Non	Modifier Supprimer

Vous pouvez modifier ou créer un nouveau sous-traitant comme ci-dessous :

+ Nouveau sous-traitant

Créer un sous-traitant

Informations générales

Nom*

Agent référent

Clauses contractuelles vérifiées
 A adopté les éléments de sécurité nécessaires
 Tient à jour un registre des traitements
 Envoi des données hors UE

Autres informations

Coordonnées

Prénom

Nom

Adresse

Compl. adresse

Code postal

Ville

Email

N° de tel

Les clauses contractuelles (obligatoires) sont-elles vérifiées ? Si oui, cochez la case.

Sont-elles conformes au RGPD ? Si oui, cochez la case.

Vous retrouvez sur votre tableau de bord l'état d'avancement du suivi de conformité de vos sous-traitants.



Il est important de recenser vos sous-traitants en premier lieu car ils s'affichent dans les fiches de traitements. Il vous suffira alors de sélectionner les sous-traitants rattachés au traitement en question.



Pensez à document la conformité des sous-traitants en ajoutant les preuves dans « Documents ».

D.3 Le Registre des demandes d'exercice de droit des personnes concernées

Lorsque vous cliquez sur « **demandes** », la fenêtre ci-dessous s'ouvre.

Liste des demandes Non archivés Tableau de bord > Liste des demandes

[+ Nouvelle demande](#) [Générer une impression](#) [Voir les demandes archivées](#)

Rechercher :

Personne concernée	Date de la demande	Objet de la demande	Demande complète	Demandeur légitime	Demande légitime	Date de traitement	Actions
Georges GERARD	2018/08/13	Rectifier des données	Oui	Oui	Oui	2018/08/19	Modifier Archiver
Georges Skuunic	2018/09/17	Supprimer des données	Oui	Oui	Oui		Modifier Archiver

D.3.1 Créer une nouvelle demande

A chaque nouvelle demande (droit d'accès, d'opposition, etc.), vous devez l'enregistrer dans « **nouvelle demande** ».

Créer une demande Tableau de bord > Liste des demandes > Créer

Demande

Objet de la demande*
 Rectifier des données
 Supprimer des données
 Retirer le consentement
 Accéder à des données
 Portabilité des données
 Limiter le traitement

Autre demande:

Date de la demande*
22 oct. 2018

Motif*

Demande complète
 Demandeur légitime
 Demande légitime

Demandeur

Civilité* Madame
Prénom*
Nom*
Adresse
Email
N° de téléphone
 Est la personne concernée

Personne concernée

— Si différente du demandeur

Civilité
Prénom
Nom
Adresse
Email
N° de téléphone
Lien avec le demandeur

[Retour à la liste](#) [Soumettre](#)

Lorsque la réponse est délivrée, vous devez retourner dans la demande, « **modifier** » et enregistrer la réponse apportée, les moyens de réponse et la date de réponse.



Rappel : La réponse doit être délivrée dans un délai maximum de 1 mois.

Demande

Objet de la demande*

- Rectifier des données
- Supprimer des données
- Retirer le consentement
- Accéder à des données
- Portabilité des données
- Limiter le traitement

← Préciser le type de demande formulée

Autre demande

Date de la demande*

← Complétez ici l'objet de la demande

Motif*

Demande complète

← Le formulaire est correctement rempli et accompagné des justificatifs

Demandeur légitime

← La personne concernée est la personne qui fait la demande ou est le tuteur dument habilité à faire la demande

Demande légitime

← La demande repose sur une base légale. Elle est pertinente et proportionnée (?)

Le **tableau de bord** affiche les demandes saisies dans ce registre qui ne sont pas traitées.

Vous pouvez ainsi suivre les demandes recensées et restant à traiter sur la page d'accueil en un coup d'œil.

D.3.2 Editer le registre des demandes de droit

Pour l'éditer, dans demandes, cliquez dans le menu sur « **Générer une impression** ».

Le fichier du registre est généré sous Word afin que vous puissiez ajouter vos logos et le personnaliser (notamment retirer ou non la colonne identifiant les personnes ayant exercé leurs droits).

D.4 Les registres de violations de données

Un incident de sécurité, d'origine malveillante ou non, intentionnel ou non, et qui risque de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles est une violation de données.

Pour vous aider à remplir le registre des violations de données, n'oubliez pas de nous informer pour vous accompagner.

La première fenêtre affiche la liste des violations recensées dans votre collectivité.

Liste des violations Non archivés Tableau de bord Liste des violations

Rechercher :

Date de violation	Nature	Cause	Niveau de gravité	Actions
2018/01/01	Perte de la confidentialité	Acte externe accidentel	Limité	Modifier Archiver

Pour enregistrer une nouvelle violation, veuillez suivre les étapes ci-dessous

Informations sur la violation

Date de la violation* : 22 oct. 2018

La violation est toujours en cours

Nature de la violation* :

- Perte de la confidentialité
- Perte de l'intégrité
- Perte de la disponibilité

Origine de la perte de données* :

- Mise au rebut de documents papier contenant des données personnelles sans destruction physique
- Mise au rebut d'appareils numériques contenant des données personnelles sans effacement sécurisé
- Publication non volontaire d'informations**
- Données de la mauvaise personne affichées sur le portail du client
- Données personnelles envoyées à un mauvais destinataire

Cause de la violation* :

- Acte interne malveillant
- Acte interne accidentel
- Acte externe malveillant
- Acte externe accidentel
- Inconnu

Nature des données concernées* :

- État civil (nom, sexe, date de naissance, âge...)
- NIR (Numéro de sécurité sociale)
- Coordonnées (adresse postale ou électronique, numéros de téléphone fixe ou portable...)**
- Données d'identification ou d'accès (identifiant, mot de passe, numéro client...)

Catégorie des personnes concernées* :

- Employés
- Utilisateurs**
- Adhérents
- Étudiants / élèves

Nombre approximatif d'enregistrements concernés par la violation* :

Nombre approximatif de personnes concernées par la violation* :

La date renseignée est celle de la constatation de la violation

Conséquences de la violation

Nature des impacts potentiels pour les personnes*

Perte de contrôle sur leurs données personnelles
Limitation de leurs droits
Discrimination
Vol d'identité

Niveau de gravité*

- Négligeable
- Limité
- Important
- Maximal

Communications aux personnes concernées*

- Oui, les personnes ont été informées
- Non, mais elles le seront
- Non ils ne le seront pas

Précisions sur les communications

Mesures techniques et organisationnelles appliquées suite à la violation*

Notification

- Aucune notification à envoyer
- Cette notification concerne un traitement transfrontalier ciblant des personnes de différents états membres
- La violation a ou va être notifiée à la CNIL
- La violation a ou va être notifiée à une autre autorité en charge de la protection des données

Précisions sur les notifications

Commentaire

E. Les actions de protection

Les actions de protection sont les mesures (techniques, organisationnelles, juridiques etc...) que vous avez déjà mises en place dans votre collectivité.

Vous devez modifier les actions en fonction de votre propre organisation, ajouter les mesures déjà mises en place dans votre collectivité et qui n'auraient pas été identifiées ici...

Liste des actions de protection Tableau de bord > Liste des actions de protection

[+ Nouvelle action](#) [Générer une impression](#)

Rechercher :

Nom	Statut	Coût	Charge	Actions
1- Adopter une politique de mot de passe administrateur rigoureuse	Appliquée			Modifier Supprimer
1- Installer et vérifier périodiquement des alarmes anti intrusion	Non appliquée	2000€		Modifier Supprimer
1- Installer les éléments de sécurité sur le réseau (Antivirus, pare-feu)	Appliquée			Modifier Supprimer
1- Mettre en place un détecteur de fumée et un système anti-feu	Appliquée	100		Modifier Supprimer
1- Paramétrer les mises à jours automatiques des logiciels (Windows_Update, Antivirus, Navigateur, client email)	Appliquée			Modifier Supprimer
1- Prévoir des moyens de chiffrement pour les ordinateurs portables et les unités de stockage amovibles (clefs USB, CD, DVD,...)	Non appliquée			Modifier Supprimer
1- Sécuriser par VPN Les accès distants des appareils informatique nomades	Non appliquée			Modifier Supprimer

Une liste préétablie de mesures inscrites comme non appliquées est disponible dans votre profil.

E.1 Modifier une action de protection

Lorsqu'une action de protection est appliquée, vous devez changer le statut de l'application dans la fiche de l'action. Vous devez changer le statut de « non appliquée » à « appliquée ».

Lorsque vous planifiez une action, vous devez laisser l'action de protection en « non appliquée » et renseigner la date de planification.

Seules les actions « non appliquées » et pour lesquelles vous avez programmé une date apparaîtront dans le plan d'actions.

Une fois appliquée, vous changerez le statut de l'action.

Modifier une action de protection 1- Adopter une politique de mot de passe administrateur rigoureuse

Informations générales

Nom* 1- Adopter une politique de mot de passe administrateur rigoureuse

Description

Coût

Charge

Application

Statut* Appliquée Non appliquée Non applicable

Planification

Observations

[Retour à la liste](#) [Sauvegarder](#)

E.2 Créer une action de protection

Si une action de protection n'existe pas dans la liste préétablie, vous pouvez l'ajouter en cliquant sur « **créer une action de protection** ».

Créer une action de protection Tableau de bord - Liste des actions - Créer

Informations générales	Application
<p>Nom* <input type="text"/></p> <p>Description <input type="text"/></p> <p>Responsable d'action <input type="text"/></p> <p>Priorité <input type="text"/></p> <p>Coût <input type="text"/></p> <p>Charge <input type="text"/></p>	<p>Statut* <input type="radio"/> Appliquée <input type="radio"/> Non appliquée <input type="radio"/> Non applicable</p> <p>Planification <input type="text"/></p> <p>Observations <input type="text"/></p>

Vous avez la possibilité d'en ajouter mais également d'en supprimer.

Informer les agents de la collectivité	Non appliquée	Modifier Supprimer
Mener une homologation RGS	Non appliquée	Modifier Supprimer

Le plan d'action recense ensuite l'ensemble des mesures planifiées :

Plan d'actions Tableau de bord - Plan d'actions

Rechercher:

Nom	Date de planification	Coût	Charge	Actions
1- Installer et vérifier périodiquement des alarmes anti intrusion	2020/09/01	2000€		Voir l'action de protection
1- Prévoir des moyens de chiffrement pour les ordinateurs portables et les unités de stockage amovibles (clefs USB, CD, DVD,...)	2019/05/08			Voir l'action de protection
2- Mettre en place une politique de protection des données et la communiquer à tous (interne et externe)	2018/10/05			Voir l'action de protection

F. Indice de maturité

L'indice de maturité est établi par une liste de réponses à des questions, classées par thématiques. Il se traduit par un « radar » qui vous permet de suivre l'évolution de votre mise en conformité. A noter que cet indice est fait lors la mise en conformité par l'APGL 64.

Outil d'aide à la décision, il permet ainsi de mettre en exergue les thèmes prioritaires à développer. Il est votre repère pour vous aiguiller dans l'élaboration de votre plan d'actions.

Dans la liste des indices de maturité, vous retrouvez l'historique des indices effectués dans votre collectivité. Cela permet d'évaluer votre progression.

Liste des indices de maturité Tableau de bord > Liste des indices de maturité

[+ Nouvel indice de maturité](#)

Rechercher :

Date de création	Score	Actions
2018/08/01 17:20	1.1	Imprimer Modifier Supprimer
2018/07/31 15:09	2.2	Imprimer Modifier Supprimer
2018/07/31 15:13	2.5	Imprimer Modifier Supprimer

A chaque nouvel indice, vous devez répondre à l'ensemble des questions.

Attention si vous n'êtes pas certain de la réponse, veuillez cocher « non, ou je ne sais pas ».

Figure 1: Critères Indice de maturité – Technique – Vie privée

Technique	Vie privée
<p>Des alarmes anti intrusion ont été installées et sont vérifiées périodiquement*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Le mobilier contenant des données à caractère personnel est fermé à clé (ou avec un autre système de fermeture)*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les archives sont stockées dans un lieu sécurisé et accessible aux seuls agents habilités*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les documents contenant des données à caractère personnel et écrans d'ordinateur sont difficilement visibles ou accessibles au public*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Un broyeur est utilisé pour détruire les documents contenant des données à caractère personnel *</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Un coffre-fort ignifugé est utilisé pour sauvegarder des documents et autres supports contenant des données à caractère personnel *</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Un détecteur de fumée et un système anti-feu ont été mis en place*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Un système de vidéo-surveillance est installé et déclaré en préfecture*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p>	<p>Chaque agent travaillant sur un ordinateur possède une adresse courriel de service (non personnelle)*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Chaque utilisateur dispose d'un identifiant unique (pas de compte générique)*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les données à l'issu des traitements sont supprimées ou anonymisées*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les procédures à suivre en cas de demandes d'exercice de droit sont définies et connues*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les sessions Windows sont protégées par un mot de passe et se verrouillent automatiquement*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les éléments de sécurité de base ont été installés sur les postes informatiques de chaque agent (Antivirus, parefeu, antisipam)*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Une politique de mot de passe utilisateur rigoureuse a été adoptée (les mots de passe sont strictement confidentiels)*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Une politique de protection des données a été mise en place et est connue de tous (interne et externe)*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p>

Figure 2: Critères indice de maturité – Violation de données - Organisation

Violation de données	Organisation
<p>Des études d'impact sur la vie privée sont conduites lorsque le traitement le nécessite*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>L'intégrité des documents est régulièrement vérifiée*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>La destruction des données à caractère personnel et sauvegardes est effectuée de manière sécurisée*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les clients mobiles sont régulièrement synchronisés*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les données sur les supports de sauvegarde sont cryptées ou chiffrées*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les jeux de sauvegarde sont régulièrement testés*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les procédures à suivre en cas de violation de données sont définies et connues*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les supports de sauvegarde sont externalisés*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p>	<p>L'identité du destinataire et sa légitimité est confirmée (en cas de transmission de données) *</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>La demande de droit d'accès est écrite ou repose sur un texte juridique*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les conditions de restitution et de destruction des données sont prévues*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les coordonnées du DPD et son rôle sont connus des personnes concernées, à l'interne et à l'externe*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les procédures d'exploitation du SI ont été documentées*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Un DPD a été désigné dans la collectivité*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Un registre des traitements est tenu dans la collectivité*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p>

Figure 3: Critères indice de maturité –Juridique – Sensibilisation/formation

Juridique	Sensibilisation Formation
<p>La conformité de chaque sous-traitant est vérifiée*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Le consentement des personnes concernées est organisé (classement, conservation, ...)*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les mentions font apparaître la finalité, les droits des personnes et la durée de conservation et sont présentes sur les formulaires (papier et électronique)*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Un référent informatique et l'identité a été nommé et se charge de diffuser la culture de protection des données au sein de sa structure*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Une charte informatique a été rédigée et annexée au règlement intérieur*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Une clause spécifique est prévue dans les contrats de sous-traitance et dans les cahiers des charges*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Une politique de gestion des données à caractère personnel a été mise en place*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p>	<p>Des actions de sensibilisation sont régulièrement menées*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Le personnel a été formé à la protection des données à caractère personnel*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Le personnel a été sensibilisé à la protection des données à caractère personnel*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Le principe d'interdiction de la collecte des données sensibles est connu par les agents et élus de la collectivité*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les agents connaissent et appliquent le principe de minimisation des données collectées*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les élus connaissent le principe d'interdiction d'utilisation des données à caractère personnel à des fins de communication politique*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p> <p>Les élus ont été sensibilisés à la protection des données à caractère personnel*</p> <p><input type="radio"/> Non / Je ne sais pas <input type="radio"/> En partie <input type="radio"/> Oui / Complètement</p>

Figure 4: Critères indice de maturité – Sécurité informatique

Sécurité informatique

Des moyens de chiffrement pour les ordinateurs portables et les unités de stockage amovibles (clefs USB, CD, DVD, etc.) ont été prévus*

Non / Je ne sais pas
 En partie
 Oui / Complètement

Les accès distants des appareils informatiques nomades sont sécurisés par VPN*

Non / Je ne sais pas
 En partie
 Oui / Complètement

Les comptes utilisateurs sont distincts selon les habilitations et droits d'accès des agents, et revus à chaque changement*

Non / Je ne sais pas
 En partie
 Oui / Complètement

Les mises à jours des logiciels sont faites régulièrement (WindowsUpdate, Antivirus, Navigateur, client email)*

Non / Je ne sais pas
 En partie
 Oui / Complètement

Les périphériques amovibles (clé USB, Disque dur externe...) sont automatiquement inspectés par l'antivirus de l'ordinateur et leur exécution automatique désactivée*

Non / Je ne sais pas
 En partie
 Oui / Complètement

Les éléments de sécurité ont été installés sur le réseau (Antivirus, parefeu, antispam)*

Non / Je ne sais pas
 En partie
 Oui / Complètement

Un antivirus analysant les courriels avant le dépôt dans la boîte de messagerie a été installé*

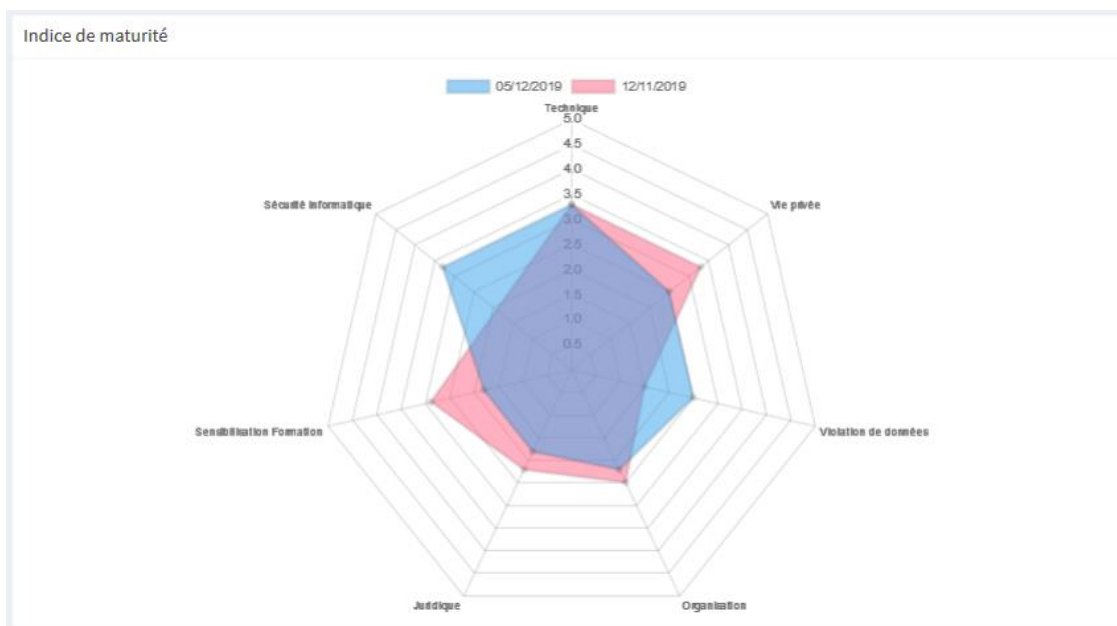
Non / Je ne sais pas
 En partie
 Oui / Complètement

Un système de journalisation protégé a été mis en place *

Non / Je ne sais pas
 En partie

Lorsque vous avez répondu à l'intégralité des questions et que vous avez validé, un nouvel indice de maturité est généré.

Vous retrouvez le schéma du « radar » avec le nouvel indice et l'indice N-1. Ce schéma est visible sur la page d'accueil du logiciel et également dans le bilan.



G. Plan d'actions

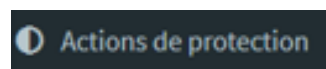
Le plan d'action reflète les décisions prises dans le but d'améliorer sa mise en conformité au RGPD. Il permet de planifier, budgétiser et évaluer les charges en jour/homme.

Plan d'actions Tableau de bord > Plan d'actions

Rechercher :

Nom	Date de planification	Coût	Charge	Actions
1- Installer et vérifier périodiquement des alarmes anti intrusion	2020/09/01	2000€		Voir l'action de protection
1- Prévoir des moyens de chiffrement pour les ordinateurs portables et les unités de stockage amovibles (clefs USB, CD, DVD,...)	2019/05/08			Voir l'action de protection
2- Mettre en place une politique de protection des données et la communiquer à tous (interne et externe)	2018/10/05			Voir l'action de protection
4- Communiquer les coordonnées du DPD et son rôle aux personnes concernées, à l'interne et à l'externe	2018/09/01	300		Voir l'action de protection
5- Organiser le consentement des personnes concernées (classement, conservation, ...)	2018/09/01			Voir l'action de protection
6- Sensibiliser les élus à la protection des données à caractère personnel	2018/08/29			Voir l'action de protection
Informers les agents de la collectivité	2018/08/10			Voir l'action de protection

Pour planifier les actions de protection, cliquez sur



Indiquer la date prévisionnelle des actions que vous choisissez de planifier, éventuellement le coût et la charge (temps passé pour effectuer l'action).

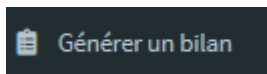
Lorsque vous cliquez sur « **plan d'actions** », vous visualisez la liste des actions que vous avez déjà planifiées.

Astuce : vous avez la possibilité de trier les actions par date / coût / charge, etc...

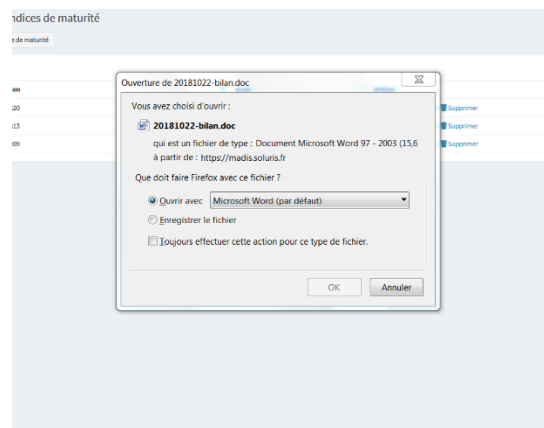
H. Générer un bilan

Au minimum une fois par an, vous devez générer le **bilan annuel**. Ce dernier synthétise l'ensemble des éléments renseignés dans le logiciel Madis, du recensement des traitements aux actions de protection en place et à planifier...

Pour le générer, cliquez dans le menu sur « **Bilan** ».



Le fichier du bilan est généré sous Word afin que vous puissiez ajouter vos logos et le personnaliser.

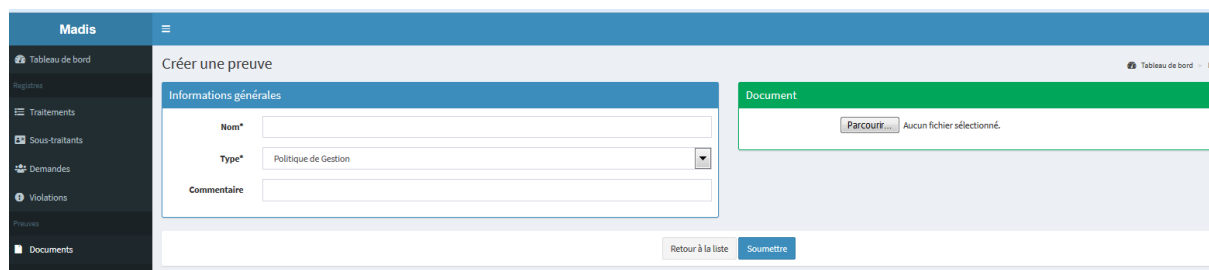
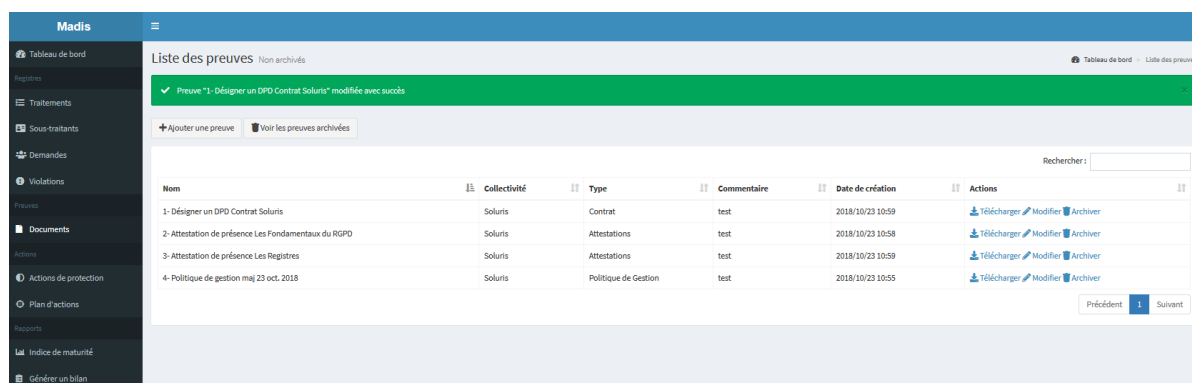


I. Gestion de la preuve

Afin de prouver votre conformité, vous devez constituer un dossier documentaire permettant de démontrer que le traitement de données personnelles est conforme au règlement.

Vous devez ajouter ici l'ensemble des preuves ...

La taille du fichier est volontairement limitée à 4 Mo.





Agence Publique de Gestion Locale (APGL)
Service Intercommunal du Numérique (SIN)

Cité administrative
Rue Auguste Renoir
64006 PAU CEDEX
Tel. 0559901811
dpo@apgl64.fr