



Guide d'utilisation

Un document pour vous guider lors de l'utilisation de la solution de conformité DP-Manager

www.dp-manager.com

Table des matières

| | |
|--|----|
| Introduction..... | 4 |
| Premiers pas dans DP-Manager | 4 |
| Gestion des tâches intégrée dans DP-Manager | 5 |
| Saisir les informations de votre organisme : | 5 |
| Création d'un traitement : | 6 |
| 1. Saisir la date de mise en œuvre du traitement..... | 8 |
| 2. Compléter l'onglet « Fondement légal » : | 9 |
| 3. Onglet Responsable du Traitement..... | 9 |
| 4. Complétez l'onglet « Catégories de données à caractère personnel »..... | 10 |
| 4.1. Modifier une catégorie de personnes concernées | 10 |
| 4.2. Modifier les catégories de données collectées..... | 14 |
| 5. Onglet « Finalité du traitement » | 18 |
| 6. Onglet « Sous-traitements » | 19 |
| 7. Onglet « conservation des données » | 22 |
| 8. Onglet «Destinataires des données » | 22 |
| 9. Onglet « Consentement » | 23 |
| 10. Onglet « Droit des personnes » | 24 |
| 10.1. Droit à l'information | 24 |
| 10.2. Droit d'accès (Article 34)..... | 25 |
| 10.3. Droit de rectification (Article 35) | 25 |
| 10.4. Droit d'opposition (Article 36) | 25 |
| 10.5. Bonnes pratiques DP-Manager | 26 |
| 11. Onglet « Sécurité du traitement » | 26 |
| Informers et collecter le consentement avec DP-Manager | 29 |
| Faire signer la charte de sécurité informatique : | 31 |
| Faites signer l'engagement de confidentialité : | 31 |
| Déclarer automatiquement sur le portail de l'ANPDP via DP-Manager | 32 |

| | |
|--|----|
| Finaliser votre traitement et réserver votre rendez-vous | 32 |
| Documents requis pour votre entretien à l'ANPDP | 32 |
| Lever les éventuelles réserves..... | 32 |

Introduction

Bienvenue dans le guide utilisateur de DP-Manager.

Ce document est conçu pour accompagner les entreprises dans leur démarche de mise en conformité à la loi 18-07 relative à la protection des données à caractère personnel.

DP-Manager est une plateforme numérique qui vous permet de gérer efficacement votre conformité grâce à une série de tâches automatiques générées dès la création de votre espace.

Premiers pas dans DP-Manager

Lors de la création de votre instance, DP-Manager initialise un ensemble de tâches essentielles. Ces tâches s'affichent automatiquement dans votre tableau de bord pour vous guider pas à pas.

 *Liste des tâches initiales générées automatiquement:*

- - Compléter les informations de votre organisme
- - Configurer les utilisateurs et leurs rôles
- - Lister les traitements existants
- - Créer le registre des traitements
- - Identifier les sous-traitants
- - Vérifier la base légale de chaque traitement
- - Préparer les documents types (politique de confidentialité, clauses contractuelles, etc.)
- - Configurer les procédures d'exercice des droits
- - Analyser les transferts internationaux éventuels
- - Valider la conformité avant déclaration à l'ANPDP

Gestion des tâches intégrée dans DP-Manager

DP-Manager intègre un module de gestion des tâches conçu pour vous faciliter le suivi de votre projet de conformité à la loi 18-07.

Dès l'activation de votre instance, un ensemble de tâches préconfigurées est automatiquement généré pour vous guider étape par étape. Ces tâches couvrent l'ensemble du cycle de mise en conformité : recensement des traitements, documentation, vérification des obligations légales, gestion des droits des personnes, etc.

✚ Les tâches sont directement visibles sur votre tableau de bord, dès votre connexion.

Vous pouvez également les consulter en détail dans le menu "Tâches". Chaque tâche indique :

- Ce qu'il faut faire
- Pourquoi cela est important
- Où effectuer l'action dans DP-Manager

Saisir les informations de votre organisme :

Dans le menu vertical à gauche, cliquez sur [Paramètres].

Vous accéderez à la fiche suivante :

Vous devez compléter les 3 volets suivants :

- Responsable de traitement
- Délégué à la protection des données (DPO)
- Logo

✚ Le logo que vous importez sera automatiquement utilisé dans les documents générés par DP-Manager, notamment dans les notices d'information et les politiques de confidentialité.

Création d'un traitement :

Dans le menu vertical à gauche, cliquez sur [Registre des traitements].

Vous accédez à l'interface dédiée à la gestion de vos traitements de données.



À ce stade, vous avez deux options pour créer un traitement :

- 1- Créer un traitement vierge : vous saisissez manuellement toutes les informations nécessaires.
- 2- Importer un modèle prédéfini : DP-Manager propose une bibliothèque de traitements standards, prêts à l'emploi.

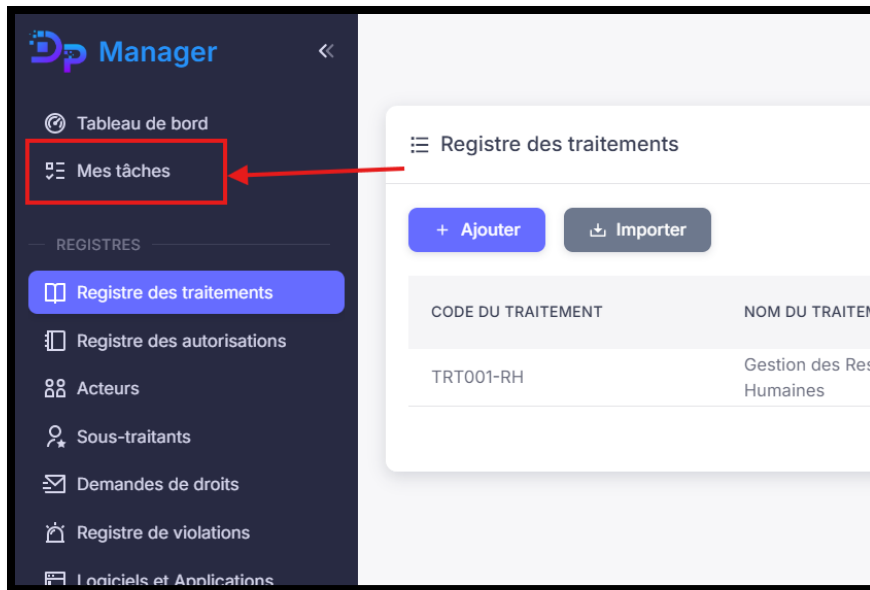
👉 Pour les traitements les plus courants (comme le traitement des données Ressources humaines), nous vous recommandons vivement d'utiliser l'option d'importation. Cela vous fera gagner un temps précieux.

Cliquez sur le bouton Importer, tapez par exemple « ressources humaines » dans la barre de recherche, puis sélectionnez le modèle correspondant. Vous pourrez ensuite l'ajuster selon les spécificités de votre organisme.

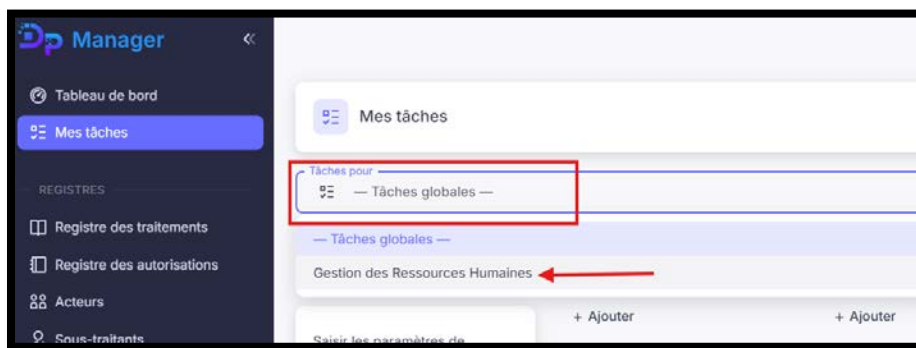


Nous allons à présent nous concentrer sur le traitement des Ressources Humaines, qui est l'un des plus courants dans tout organisme.

Une fois le traitement importé, rendez-vous dans le gestionnaire des tâches.



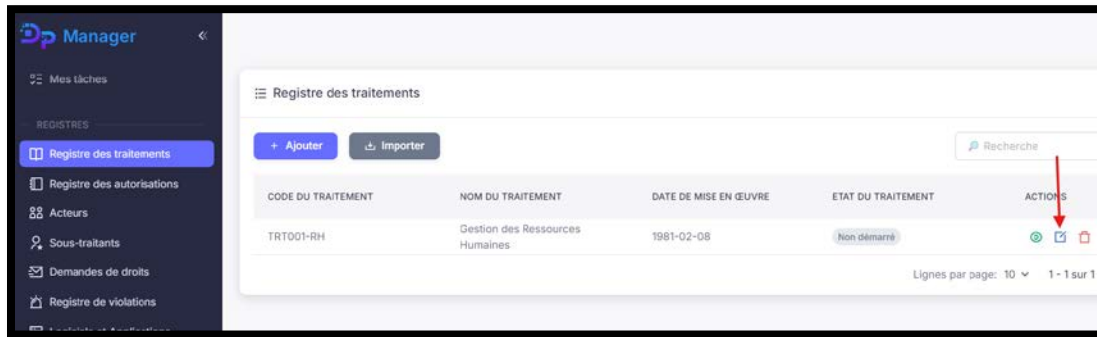
Accédez au filtre situé en haut de la liste des tâches (comme illustré sur l'image ci-dessous), puis sélectionnez "Ressources humaines" afin d'afficher uniquement les tâches liées à ce traitement spécifique.



Vous y trouverez la liste des actions à accomplir pour compléter et valider ce traitement. Chaque tâche est liée à une section spécifique du traitement et vous guide pas à pas dans sa mise en conformité.

Pour commencer à compléter le traitement, cliquez sur le bouton Modifier (identifié par l'icône signalée par la flèche rouge dans l'image ci-dessous). Cela vous permettra de personnaliser les informations du traitement en fonction des spécificités

propres à votre organisme.



1. Saisir la date de mise en œuvre du traitement

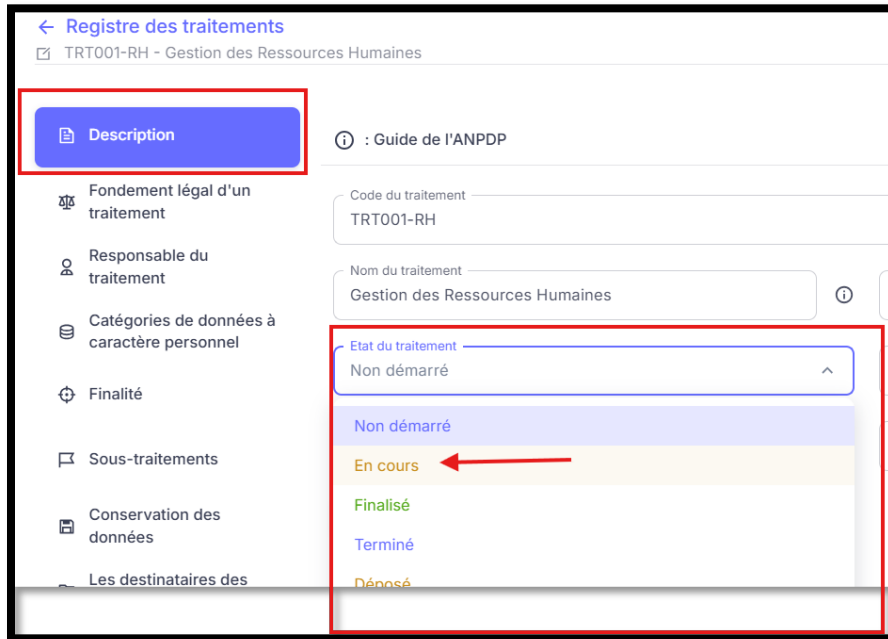
Cette date correspond généralement à la date de votre premier recrutement ou, plus largement, à la date à laquelle vous avez obtenu votre numéro d'employeur. Il s'agit de la date à partir de laquelle le traitement des données Ressources Humaines a effectivement débuté dans votre organisme.

The screenshot shows the 'Registre des traitements' form, specifically the 'Description' tab (highlighted with a red box). The form is for 'RH - Gestion des Ressources Humaines'. It includes the following fields:

- Code du traitement:** RH
- Nom du traitement:** Gestion des Ressources Humaines
- Etat du traitement:** Finalisé (dropdown menu)
- Date de mise en œuvre:** 23-11-2002 (highlighted with a red box)
- Type de traitement:** Manuel / Automatique (dropdown menu)
- Date de modification:** (empty field)

Buttons 'Enregistrer' and 'Annuler' are at the bottom. A sidebar on the left lists other tabs: 'Fondement légal d'un traitement', 'Responsable du traitement', 'Catégories de données à caractère personnel', 'Finalité', 'Sous-traitements', 'Conservation des données', and 'Les destinataires des données'.

Dans le même onglet, pensez à définir l'état du traitement sur *EN COURS*, afin d'indiquer que ce traitement est actif et que sa mise en conformité est en cours.



The screenshot shows the 'Registre des traitements' interface. The 'Description' tab is selected. The 'Etat du traitement' dropdown menu is open, showing the following options: 'Non démarré', 'En cours' (highlighted with a red arrow), 'Finalisé', 'Terminé', and 'Déposé'. The 'En cours' option is selected.

2. Compléter l'onglet « Fondement légal » :

Dans l'onglet Fondement légal, si vous avez importé le traitement à partir de nos modèles, le cadre légal et les bases légales sont déjà préremplis.

En revanche, si vous avez créé un traitement vierge, vous devrez les renseigner manuellement.

Dans ce cas, il est recommandé de consulter votre juriste pour identifier le cadre et les bases légales adaptés à votre traitement.

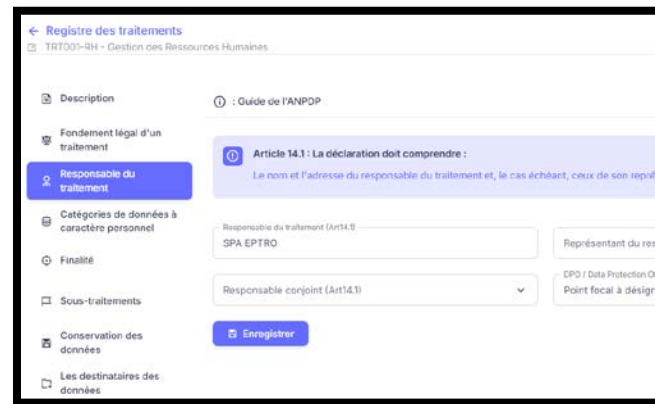
Vous pouvez également nous solliciter par email à : info@tadjeddine-partners.com.

3. Onglet Responsable du Traitement

Si cet onglet est vide, vous devez compléter ces informations dans la section « Paramètres » du menu principal.

Cela permettra de lier automatiquement le responsable de traitement à tous vos traitements déclarés.

👉 Pour rappel, cette étape correspond à la première tâche à réaliser lors de la configuration de votre espace DP-Manager.

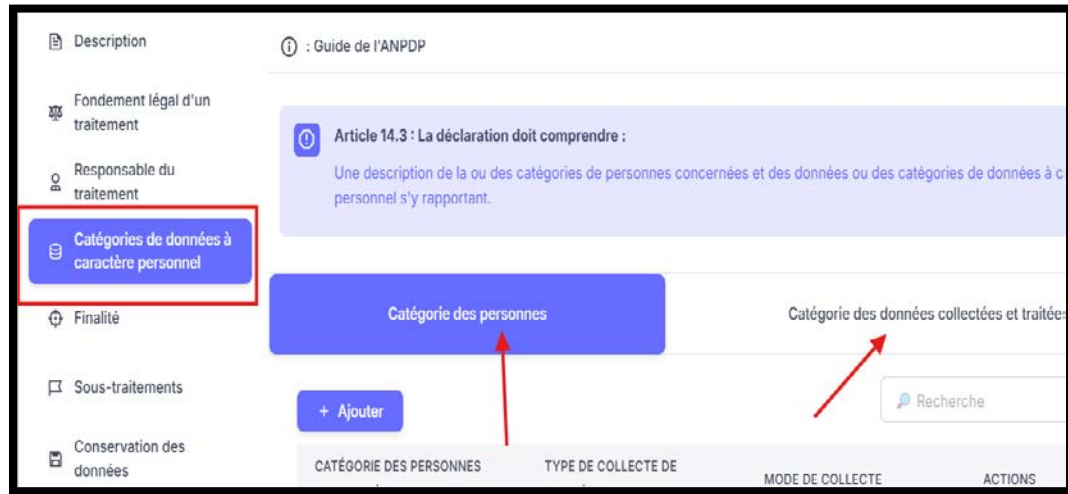


The screenshot shows the 'Registre des traitements' interface. The 'Responsable du traitement' tab is selected. The 'Article 14.1 : La déclaration doit comprendre :' section is visible, showing fields for 'Responsable du traitement (Art14.1)' and 'Responsable conjoint (Art14.1)'. The 'Enregistrer' button is visible.

4. Complétez l'onglet « Catégories de données à caractère personnel »

Dans le troisième onglet, intitulé « Catégories de données à caractère personnel », vous devez compléter deux éléments essentiels :

- ✓ Les catégories de personnes concernées par le traitement (par exemple : salariés, candidats, clients, etc.)
- ✓ Les catégories de données collectées et traitées (par exemple : données d'identification, données contractuelles, données de santé, etc.)



À retenir :

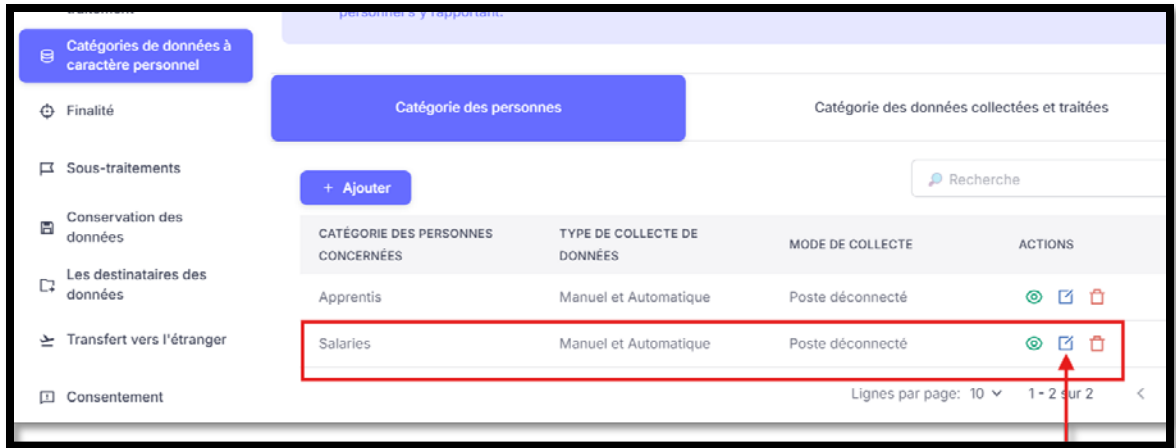
Si vous avez importé le traitement depuis nos modèles, certaines informations sont déjà préremplies.

Toutefois, vous devez **vérifier et adapter** ces informations pour qu'elles correspondent exactement aux pratiques de votre organisme.

Si vous avez créé un traitement vierge, vous devrez tout renseigner manuellement.

4.1. Modifier une catégorie de personnes concernées

Prenons l'exemple de la catégorie « Salarié ». Cliquez sur le bouton Modifier, comme indiqué par la flèche sur l'image ci-dessous, pour accéder aux paramètres détaillés.



Vous obtenez la fiche suivante :

The screenshot shows the 'Modifier' form for the 'Salaries' category. The form includes the following fields and options:

- Catégorie des personnes concernées:** A dropdown menu with 'Salaries' selected.
- Type de collecte de données:** A dropdown menu with 'Manuel et Automatique' selected, highlighted with a blue circle 1.
- Mode de collecte:** A dropdown menu with 'Poste déconnecté' selected, highlighted with a blue circle 2.
- La sécurité de la collecte des données:** A section with three numbered circles (1, 2, 3) and several checkboxes:
 - ☒ Traçabilité
 - ☐ Signature électronique
 - ☐ Chiffrement
 - ☒ Charte de sécurité

At the bottom of the form is a blue button labeled 'Enregistrer'.

Conseil : rapprochez-vous de votre informaticien ou de votre responsable IT pour renseigner ces éléments de manière précise.

Vous trouverez ci-après une explication détaillée de chaque rubrique pour bien les renseigner :

1- Type de collecte des données :

- Manuel : collecte de données réalisée sur support papier, par exemple remise d'une photocopie de pièce d'identité, fourniture de documents administratifs ou remplissage d'un formulaire papier. Les informations peuvent ensuite être saisies manuellement dans un logiciel, mais la collecte initiale reste physique.
- Automatique : collecte directement sur un logiciel ou un système.
- Manuel et Automatique : combinaison des deux modes, utilisée simultanément selon les types de données collectées.

Si vous utilisez les deux types, conservez l'option « Manuel et Automatique ».

Si vous ne collectez que sur support papier, Choisissez « Papier ».

2- Mode de collecte automatisée (si activée) :

Si vous sélectionnez le type de collecte « Automatique » ou « Manuel et Automatique », vous devez préciser le mode de collecte utilisé dans votre organisme :

- Poste déconnecté : la collecte s'effectue sur un ordinateur isolé, sans connexion réseau. Dans ce cas, le logiciel et les données sont stockés localement sur le poste où se fait la saisie.
- Réseau local : le logiciel RH est installé sur un serveur interne. Les postes de travail y accèdent via le réseau local. Les données sont saisies depuis un poste de travail, puis transmises au serveur à travers le réseau interne.
- Internet : le logiciel est accessible en ligne, via un serveur distant ou une solution cloud. La saisie et la transmission des données se font alors via une connexion Internet.

3- Sécurité de la collecte :

Si la collecte implique un outil informatique, complétez également la partie « Sécurité de la collecte ».

Quatre mesures peuvent être cochées, selon les pratiques mises en place :

- Traçabilité : Cela signifie que les actions effectuées sur les données personnelles (création, consultation, modification, suppression) sont enregistrées et historisées dans un journal d'audit (log).
Objectif : pouvoir retracer qui a fait quoi, quand et comment, en cas de contrôle ou d'incident de sécurité.
Exemple concret : un logiciel RH conserve une trace chaque fois qu'un dossier salarié est ouvert, modifié ou exporté.

- **Chiffrement** : Le chiffrement est une mesure de sécurité qui rend les données illisibles sans une clé de déchiffrement.
Cela protège les données pendant leur transfert (par exemple, lors d'un envoi par Internet).
- **Signature électronique** : Il s'agit d'une méthode qui garantit l'authenticité et l'intégrité d'un document numérique ou d'une donnée.
Elle permet de prouver qu'un document n'a pas été modifié depuis sa signature et d'identifier clairement le signataire.

Attention : dans 99,99 % des cas, ne cochez pas cette option.

En effet, l'utilisation d'une signature électronique légale et opposable en Algérie nécessite de disposer d'un certificat de signature électronique qualifié, délivré par un prestataire agréé tel que l'Autorité Gouvernementale de Certification Electronique AGCE ou l'Autorité Economique de Certification Electronique AECE.

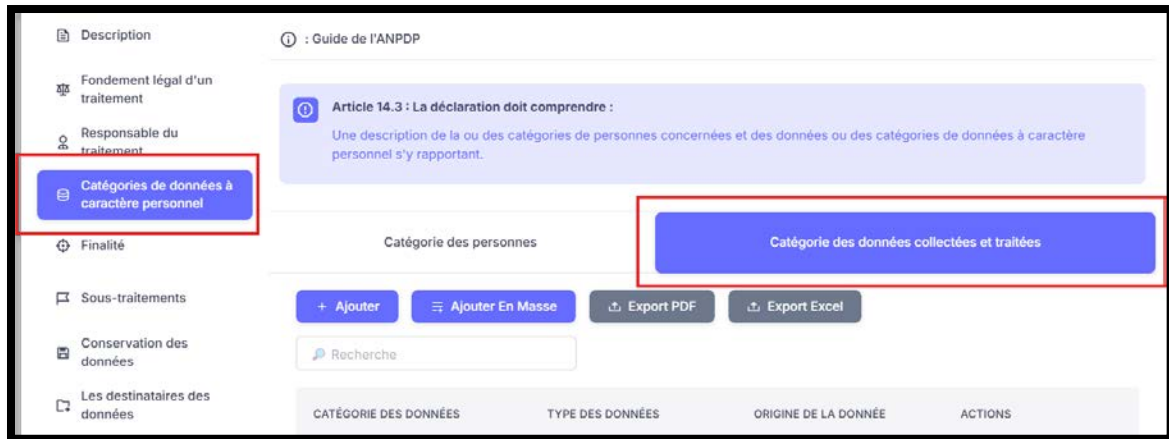
- **Charte de sécurité** : Il s'agit d'un document interne qui définit les règles de sécurité informatique applicables au sein de l'organisme.
Cette charte précise les bonnes pratiques que doivent respecter les employés pour protéger les données personnelles : gestion des mots de passe, accès aux serveurs, usage des clés USB, navigation sécurisée, etc.
À noter : la charte de sécurité informatique fait partie des actions de conformité exigées par l'ANPDP.
Elle doit être signée par tous les employés ayant accès aux systèmes et outils informatiques de l'organisme.

👉 Répétez cette démarche pour chaque catégorie de personnes affichée. Vous pouvez également en ajouter de nouvelles si besoin, selon la réalité de votre organisme.

Si la catégorie de personne que vous souhaitez ajouter n'apparaît pas dans la liste, allez dans le menu vertical à gauche, cliquez sur « Données de base », puis sur « Catégorie de personne » pour la créer. Revenez ensuite dans votre traitement pour finaliser l'ajout.

4.2. Modifier les catégories de données collectées

Passons maintenant au 2^{ème} volet de l'onglet CATEGORIES DE DONNEES A CARACTERE PERSONNEL



Il s'agit de renseigner exhaustivement toutes les catégories de données à caractère personnel collectées et traitées dans le cadre du traitement en cours.

Si vous avez importé le traitement à partir des modèles préremplis de DP-Manager, vous trouverez déjà les catégories de données les plus courantes renseignées pour ce traitement.

👉 Ce qu'il vous reste à faire :

- Vérifiez chaque catégorie de données : supprimez celles que vous ne collectez pas réellement.
- Ajouter les catégories de données manquantes : complétez celles que vous collectez réellement mais qui ne figurent pas dans le modèle prérempli.

Cette étape demande souvent une vérification minutieuse et une collaboration avec le service concerné.

Nous vous recommandons donc d'exporter la liste au format Excel ou PDF (les boutons export sont visible sur la fiche), de la partager avec le responsable métier pour validation, puis de mettre à jour DP-Manager en conséquence.

Découvrez ci-dessous l'explication de chacune des rubriques à renseigner dans la fiche « Donnée à caractère personnel ».

The screenshot shows a 'Modifier' (Edit) form for a 'Donnée à caractère personnel' (Personal Data). The form contains several dropdown menus and text fields, each with a numbered annotation (1-7) and an information icon (i). The annotations point to the following fields:

- 1: 'Catégorie des données' (Data Category) dropdown menu, currently showing 'Données professionnelles..... بيانات مهنية'.
- 2: 'Type des données' (Data Type) dropdown menu, currently showing 'Sanction disciplinaire'.
- 3: 'Origine de la donnée' (Data Origin) dropdown menu, currently showing 'Personne concernées'.
- 3: 'Utilisé(s) pour la finalité du traitement' (Used for the purpose of processing) dropdown menu, currently showing 'Oui'.
- 4: 'Source de données' (Data Source) dropdown menu, currently showing 'Support papier et électronique'.
- 5: 'Durée de conservation' (Retention Period) dropdown menu, currently showing 'Limitée'.
- 6: 'Préciser la durée (mois)' (Specify duration in months) text field, currently showing '384'.
- 7: 'Élément déclencheur' (Triggering Element) text field, currently showing 'A partir de la date de cessation de la relation de travail'.

At the bottom of the form is a blue button labeled 'Enregistrer' (Save).

1 Catégorie des données

Indiquez la nature générale des données collectées. L'ANPDP distingue notamment quatre grandes catégories : données personnelles, données professionnelles, données financières et données sensibles. Cette rubrique permet de classer les informations traitées par grands types.

Cette rubrique se présente sous forme d'une liste déroulante proposant quatre choix. Lorsque vous sélectionnez l'une de ces grandes catégories, la rubrique suivante vous affichera automatiquement les types de données détaillés qui y sont associés.

2 Type des données

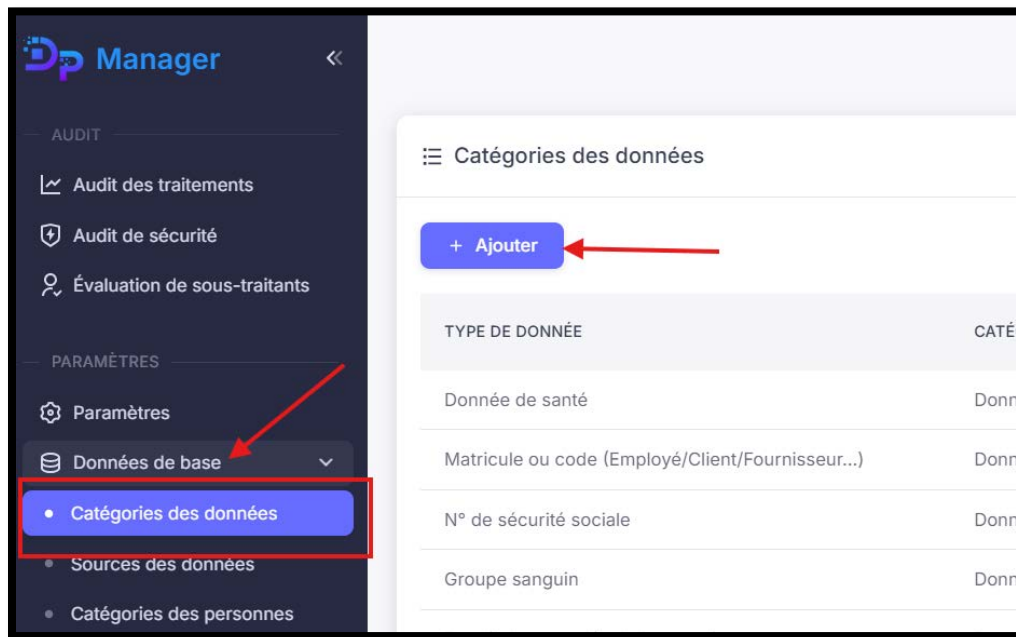
Précisez le détail de la catégorie en indiquant le type exact de données concerné (ex. : Nom, Prénom, copie de la pièce d'identité, numéro de téléphone...).

Cela permet de savoir précisément quelles informations sont incluses dans la catégorie générale.

Cette rubrique se présente sous forme d'une liste déroulante où nous avons recensé les types de données les plus couramment utilisés.

Si une catégorie de données apparaît grisée et non sélectionnable, cela signifie qu'elle est déjà présente dans la liste des données collectées par ce traitement.

👉 Si vous ne trouvez pas dans la liste un type de données que vous collectez réellement, vous devez vous rendre dans « Données de base » pour l'ajouter, comme illustré dans l'image ci-dessous. Revenez ensuite dans votre traitement pour finaliser l'ajout.



3 Origine de la donnée

Spécifiez d'où proviennent ces données.

Pour un traitement RH, l'origine est généralement « Personnes concernées » (ex. : le salarié fournit lui-même ses justificatifs).

Si vous choisissez « Autre », un champ s'affichera pour vous permettre de préciser l'origine réelle.

4 Utilisée pour la finalité du traitement

Indiquez « Oui » si ces données sont effectivement utilisées pour atteindre la finalité du traitement déclaré.

Si une donnée est collectée mais non exploitée, elle ne doit pas être conservée.

Ce champ rappelle le principe de minimisation des données.

👉 L'article 9, point c) de la loi précise :

« Les données collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ou traitées. »

Assurez-vous donc que chaque catégorie de données contribue réellement à l'objectif du traitement concerné.

5 Source de données

Précisez le support de collecte :

- Papier : si les données sont fournies sous format papier uniquement.
- Électronique : si elles proviennent directement d'un système informatique.
- Papier et électronique : si vous utilisez les deux supports (ex. : formulaire papier scanné et archivé).

👉 Si vous ne trouvez pas dans la liste la source de données que vous utilisez réellement, vous devez vous rendre dans « Données de base » pour l'ajouter. Revenez ensuite dans votre traitement pour finaliser l'ajout

6 Durée de conservation

Indiquez ici combien de temps vous conservez ces données avant de les supprimer.

👉 Objectif : Respecter le principe de limitation de conservation (article 9 point d de la loi 18-07) et éviter toute conservation excessive ou non justifiée.

Vous devez choisir entre deux options :

- Limitée : la durée est fixée à un nombre précis de mois (ex. : 384 mois).
- Illimitée : à éviter sauf justification légale ou réglementaire claire. Dans ce cas, gardez une preuve écrite de cette justification.

💡 Comment déterminer la durée ?


Référez-vous :

- Aux obligations légales (ex. : code du travail, réglementation fiscale, CNAS, CASNOS, archives, etc.)
- À vos politiques internes ou aux recommandations de votre juriste.
En cas de doute, consultez le DPO ou un conseiller spécialisé.

Et après ?

Une fois la durée de conservation atteinte pour une donnée ou un dossier :

- Supprimez définitivement les données devenues inutiles ou périmées.
- Ou basculez-les en archivage sécurisé, si une obligation d'archivage s'applique.

 Bonnes pratiques :


Mettez en place des mécanismes techniques et organisationnels pour suivre ces échéances :

- Paramétrez des alertes automatiques (via DP-Manager ou votre système d'information).
- Préparez une procédure interne pour gérer la purge ou l'archivage au bon moment.
- Formez les services concernés à surveiller ces dates et à appliquer la suppression ou l'archivage.

7 Élément déclencheur

Précisez à partir de quand démarre le calcul de la durée de conservation.

Exemple : « À partir de la date de cessation de la relation de travail », « À partir de la date de fin de contrat », etc.

 Pour fixer la durée et l'élément déclencheur, consultez vos obligations légales ou rapprochez-vous de votre juriste. Ces deux champs sont essentiels pour démontrer la maîtrise du cycle de vie des données.

5. Onglet « Finalité du traitement »

Cet onglet décrit l'objectif principal pour lequel les données sont collectées et traitées.

Si vous avez importé le traitement à partir de nos modèles, la finalité est déjà renseignée.

Dans le cas contraire, vous devez saisir vous-même la finalité, de manière claire et conforme à la réalité du traitement.

Assurez-vous que cette finalité soit précise, légitime et proportionnée au regard des données collectées.

6. Onglet « Sous-traitements »

Un traitement peut être composé de plusieurs sous-traitements qui précisent ses différentes composantes pratiques.

Dans certains cas, le traitement déclaré peut être unique et ne comporter aucun sous-traitement, car il est considéré comme indivisible.

L'ANPDP laisse la liberté à l'organisme soit de déclarer un traitement découpé en plusieurs sous-traitements, soit de le déclarer comme un bloc unique et complet, selon sa réalité de fonctionnement.

👉 Exemple concret :

Pour le traitement « Gestion des ressources humaines », il est indispensable de détailler les sous-traitements, car il regroupe généralement plusieurs volets : gestion des contrats, paie, évaluation, formation, médecine du travail, etc.

L'objectif est de découper le traitement global en blocs opérationnels plus clairs, afin de mieux décrire les données concernées, les sous-traitants impliqués et les finalités spécifiques.

Si vous avez importé le traitement à partir de nos modèles, une liste de sous-traitements est déjà préremplie.

Vous devez vérifier pour chaque sous-traitement s'il implique un sous-traitant externe et, le cas échéant, l'ajouter à la fiche.

Sous-traitements

Conservation des données

Les destinataires des données

Transfert vers l'étranger

Consentement

Droit des personnes

Sécurité du traitement

+ Ajouter

Export PDF

Export Excel

Recherche

| FINALITÉ ↓ | BASE LÉGALE | SOUS TRAITANT | ACTIONS |
|---|--|---------------|---|
| Virement paies et primes | L'exécution d'un contrat ou précontrat à la demande de la personne. | BDL | <div><div></div><div><div></div></div><div></div></div> |
| Traitement des litiges juridiques | La réalisation d'un intérêt légitime poursuivi par le responsable du traitement. | AVOCAT | <div><div></div><div><div></div></div><div></div></div> |
| Traitement des demandes de droits | Le respect d'une obligation légale. | | <div><div></div><div><div></div></div><div></div></div> |
| Suivi et prévention des risques professionnels | La réalisation d'un intérêt légitime poursuivi par le responsable du traitement. | | <div><div></div><div><div></div></div><div></div></div> |
| Suivi et maintenance du parc informatique et gestion des comptes utilisateurs | La réalisation d'un intérêt légitime poursuivi par le responsable du traitement. | | <div><div></div><div><div></div></div><div></div></div> |
| Réservation d'hôtels et réservation billets d'avion | La réalisation d'un intérêt légitime poursuivi par le responsable du traitement. | | <div><div></div><div><div></div></div><div></div></div> |
| Réalisation de statistiques et rapports sur les RH | La réalisation d'un intérêt légitime poursuivi par le responsable du traitement. | | <div><div></div><div><div></div></div><div></div></div> |
| Organisation des réunions des instances représentatives du personnel. | Le respect d'une obligation légale. | | <div><div></div><div><div></div></div><div></div></div> |
| Médecine de travail | Le respect d'une obligation | | <div><div></div><div><div></div></div><div></div></div> |

Le sous-traitant doit d'abord être enregistré dans la liste des sous-traitants (accessible depuis le menu vertical à gauche), puis ajouté au sous-traitement concerné.

La fiche sous-traitement se présente comme suit :

Modifier

Dénomination du sous-traitement
Virement paies et primes

Type de traitement
Automatique

Base légale
L'exécution d'un contrat ou précontrat à la demande de la personne.

Sous-traitant
BDL

Logiciel utilisé
Plateforme eBanking de la banque

Catégories de données utilisées
Nom et Prénom RIB/ RIP / IBAN / Numéro de compte Revenu

Note

Enregistrer

Chaque sous-traitement décrit une opération précise liée au traitement principal. Voici comment remplir chaque champ correctement :

1. **Dénomination du sous-traitement**

Indiquez le nom clair et explicite du sous-traitement pour qu'il soit facilement compréhensible.

Exemple : *Virement paies et primes*

اسم المعالجة الفرعية (en arabe)

Saisissez la traduction du nom du sous-traitement en arabe, comme exigé par l'ANPDP.

Exemple : *صرف الرواتب والمنح*

2. **Type de traitement**

Précisez si l'opération est automatique, manuelle ou mixte, selon son mode de réalisation.

Exemple : *Automatique* (virement réalisé via un logiciel bancaire)

3. **Base légale**

Indiquez la justification juridique du sous-traitement (ex. : exécution d'un contrat, respect d'une obligation légale, intérêt légitime). (Article 7)

Exemple : *Exécution d'un contrat ou précontrat à la demande de la personne.*

4. **Sous-traitant**

Si ce sous-traitement est réalisé par un prestataire externe, indiquez le **nom du sous-traitant** qui l'exécute pour votre compte. Veillez à l'avoir préalablement ajouté dans votre liste des sous-traitants.

Si le sous-traitement est effectué **en interne**, laissez ce champ vide.

Exemple : *BDL (Banque de Développement Local)*

5. **Logiciel utilisé**

Indiquez l'**outil ou la plateforme** mobilisé pour réaliser le sous-traitement.

Exemple : *Plateforme eBanking de la banque*

Cette rubrique n'est **pas exigée par l'ANPDP**, mais elle reste très utile pour savoir **où se trouvent vos données** et par **quels outils** elles sont traitées.

6. **Catégories de données utilisées**

Détaillez les données à caractère personnel traitées dans le cadre de ce sous-traitement.

Exemples :

- Nom et Prénom / اللقب والاسم
- RIB / RIP / IBAN / Numéro de compte
- Revenu / المداخيل

Cette rubrique n'est pas exigée par l'ANPDP mais reste utile pour bien cartographier les données traitées.

⚠ Attention

Si vous faites appel à un sous-traitant, vous devez obligatoirement établir un **contrat conforme à l'article 39** de la loi 18-07.

DP-Manager met à votre disposition des **modèles de contrats** adaptés selon le type d'activité du sous-traitant.

7. Onglet « conservation des données »

Dans cet onglet, vous devez préciser **où sont stockées les données** :

- Indiquez l'emplacement de conservation des données **au format numérique** (serveur interne, cloud, hébergeur, etc.)
- Indiquez l'emplacement de conservation des données **au format papier** (salle d'archives, bureau administratif, etc.)
L'ANPDP exige également de préciser si ces données sont conservées **en Algérie ou à l'étranger**.

The screenshot shows the 'Conservation des données' form in DP-Manager. The form is divided into two main sections: 'Conservation informatique des données' and 'Conservation manuelle des données'. The 'Conservation informatique des données' section contains two fields: 'Nom de la base de données' (Base de données Personnel) and 'Lieu de stockage de la base de données' (PC en Algérie). The 'Conservation manuelle des données' section contains two fields: 'Nom du fichier manuel' (Doissiers employés) and 'Lieu de stockage du fichier' (siège de l'entreprise Algérie). A sidebar on the left lists various menu items, with 'Conservation des données' highlighted. At the bottom, there is an 'Enregistrer' button.

8. Onglet «Destinataires des données »

Selon la loi, un **destinataire** est « *toute personne physique ou morale, autorité publique, service ou autre entité qui reçoit communication des données à caractère personnel.* »

Dans cet onglet, indiquez les destinataires auxquels vous transmettez ou pourriez transmettre ces données.

Exemples : CNAS, impôts, services sécuritaires, autorités publiques ou tout autre organisme officiel.

La fiche Destinataire vous permet de décrire à qui vous transmettez les données du traitement. Certaines informations doivent être **créées au préalable** dans le menu **Données de base** (accessible dans le menu vertical à gauche).

Destinataire

Indiquez le nom de l'organisme, de l'administration ou du service destinataire.

Exemple : *CNAS*

Moyen de communication

Précisez comment les données sont transmises : par connexion, envoi papier, remise manuelle, portail en ligne, etc.

Exemple : *Connexion*

Objectifs

Décrivez la finalité de la transmission.

Exemple : *Paiement des cotisations sociales*

Cadre légal

Indiquez si la transmission est encadrée par une obligation légale ou réglementaire.

Exemple : *Oui*

Observation

Ajoutez toute précision utile, notamment le fondement réglementaire ou contractuel.

Exemple : *Obligation légale*

Modifier

Destinataire
CNAS

Moyen de communication
Connexion

Objectifs
Paiement des cotisations sociales

Cadre légal
Oui

Observation
Obligation légale

Enregistrer

9. Onglet « Consentement »

L'ANPDP exige que le **consentement explicite** de la personne soit recueilli **avant** toute collecte ou traitement de ses données personnelles.

Dans cette rubrique, vous devez :

- Indiquer si le consentement est effectivement demandé (*Oui* ou *Non*).

- Préciser le **mécanisme utilisé** pour obtenir ce consentement (ex. : signature d'une politique de confidentialité, case à cocher sur un formulaire, validation électronique).
- Remplir également le champ en arabe **حدد كيفية أخذ الموافقة الصريحة** donnant la traduction de la méthode.

Exemple :

Consentement existe : *Oui*

Méthode : *Signature sur la politique de confidentialité*

التوقيع على سياسة الخصوصية : الطريقة بالعربية

Fondement légal d'un traitement

Responsable du traitement

Catégories de données à caractère personnel

Finalité

Sous-traitements

Conservation des données

Les destinataires des données

Transfert vers l'étranger

Consentement des personnes concernées

Consentement des personnes concernées : Existe ?

Oui

Indiquer la méthode de consentement

signature sur la politique de confidentialité

حدد كيفية أخذ الموافقة الصريحة

التوقيع على سياسة الخصوصية

Enregistrer

Consentement

10. Onglet « Droit des personnes »

Dans cet onglet vous devez renseigner comment les personnes sont elles informées de leurs droits, comment elles peuvent l'exercer et auprès de quel service.

10.1. Droit à l'information

L'article 32 de la loi 18-07 impose au **responsable du traitement** d'informer clairement la personne concernée **avant** la collecte de ses données.

Cette information doit obligatoirement comprendre :

- L'identité et les coordonnées du responsable du traitement (RT).
- Les finalités précises du traitement.
- Les destinataires ou catégories de destinataires des données.
- Toute autre information utile permettant à la personne de comprendre comment ses données seront utilisées, ses droits et les modalités pour les exercer.

Cette obligation incombe **directement à l'organisme**, qui doit être en mesure de prouver à tout moment que l'information a bien été délivrée.

10.2. Droit d'accès (Article 34)

Toute personne concernée a le droit de savoir si ses données sont traitées et d'en obtenir une copie.

Elle peut demander :

- Quelles données sont détenues sur elle.
- Les finalités du traitement.
- L'origine des données.
- Les destinataires ou catégories de destinataires.

Obligation de l'organisme :

Mettre en place une procédure simple (ex. : formulaire en ligne, registre des demandes) et répondre dans les délais prévus.

10.3. Droit de rectification (Article 35)

Toute personne concernée peut exiger :

- La **rectification** de données inexactes ou incomplètes.
- La **suppression** de données lorsque leur traitement n'est plus justifié (ex. : retrait de consentement, finalité atteinte, traitement illicite).

Obligation de l'organisme :

Mettre à jour ou effacer les données demandées et informer les destinataires concernés.

10.4. Droit d'opposition (Article 36)

La personne peut s'opposer à tout moment, pour des raisons légitimes, à ce que ses données fassent l'objet d'un traitement, sauf dispositions contraires prévues par la loi (ex. : obligations légales, motifs de sécurité nationale, etc.).

Obligation de l'organisme :

Analyser la demande, justifier toute limitation et maintenir une trace écrite de la réponse.

10.5. Bonnes pratiques DP-Manager

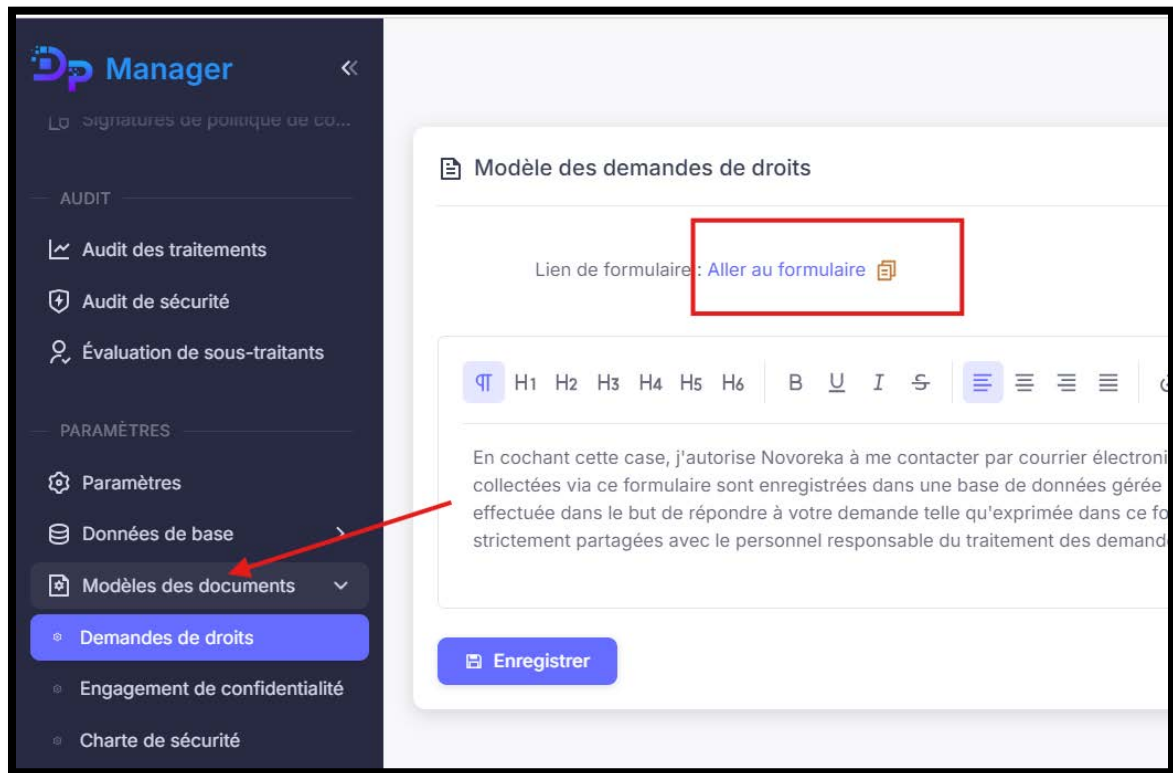
DP-Manager intègre un **registre de suivi des demandes d'exercice de droits** pour vous aider à gérer ces obligations.

Il est recommandé d'y consigner :

- Chaque demande reçue.
- La réponse apportée.
- Les délais de traitement.

Cela permet de prouver votre **conformité** lors d'un contrôle de l'ANPDP.

💡 Vous pouvez copier le lien du formulaire (comme illustré sur l'image ci-dessous) et l'intégrer directement sur votre site web, par exemple dans la rubrique « Politique de confidentialité » ou « Contact ».



11. Onglet « Sécurité du traitement »

L'article 38 de la loi 18-07 impose au responsable de traitement de mettre en place **toutes les mesures techniques et organisationnelles nécessaires** pour garantir la sécurité des données à caractère personnel.

Pour vous aider, l'ANPDP propose une liste de mesures prédéfinies sous forme de cases à cocher (ex. : sécurité des postes de travail, traçabilité, chiffrement...). DP-Manager reprend ces mêmes options pour faciliter votre déclaration.

👉 Si vous appliquez des mesures spécifiques qui ne figurent pas parmi ces cases, vous pouvez les détailler dans le champ texte prévu à cet effet.

The screenshot shows the 'caractère personnel' section in DP-Manager. On the left is a sidebar with icons for 'Finalité', 'Sous-traitements', 'Conservation des données', 'Les destinataires des données', 'Transfert vers l'étranger', 'Consentement', 'Droit des personnes', and 'Sécurité du traitement'. The main content area is titled 'Sécurité des données, disponibilité de : ⓘ'. It contains a table of security measures:

| Sécurité des données, disponibilité de : ⓘ | |
|--|---|
| <input type="checkbox"/> DATACENTER | <input type="checkbox"/> Chiffrement/Déchiffrement des Données |
| <input type="checkbox"/> Disaster Recovery (backup) | <input checked="" type="checkbox"/> Traçabilité d'accès aux Données |
| <input type="checkbox"/> Système de Télésurveillance | <input type="checkbox"/> Documentation des Procédures de Sécurité |
| <input checked="" type="checkbox"/> Sécurité de Postes de Travail | <input checked="" type="checkbox"/> Sécurité d'accès Physique aux Locaux |
| <input checked="" type="checkbox"/> Politique de Sauvergarde des Données | <input checked="" type="checkbox"/> Mesures de Sécurité du Fichier Manuel |

Below the table is a text area: 'Une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la confide...'. At the bottom, there are two dropdown menus: 'Existe-il une charte de sécurité (Engagement de confidentialité) ?' with 'Oui' selected, and 'La charte de sécurité est-elle lue et signé par le personnel habilité à accé...' with 'Oui' selected. Information icons ⓘ are present next to the table title and the dropdowns.

Voici une explication claire pour chacune des mesures présentées dans ce tableau :

1. DATACENTER

Indique que vos données sont hébergées dans un **centre de données sécurisé** disposant de protections physiques et techniques robustes (accès contrôlé, alimentation électrique de secours, protection incendie, etc.). Cela assure une haute disponibilité et une meilleure protection des données.

2. Disaster Recovery (Backup)

Signifie que vous appliquez une **politique de sauvegarde et de reprise après sinistre**. Des sauvegardes régulières et un plan de restauration sont prévus pour limiter la perte de données en cas de panne, incident ou cyberattaque.

3. Système de Télésurveillance

Vous disposez d'un **système de vidéosurveillance** (caméras, alarmes) pour protéger physiquement les locaux où les données sont traitées ou conservées. Cela réduit les risques de vol ou d'intrusion.

4. Sécurité des Postes de Travail

Implique la mise en place de mesures pour sécuriser les ordinateurs : verrouillage des sessions, antivirus, pare-feu, contrôle des ports USB, mots de passe robustes, etc. C'est la mesure de base exigée si vous stockez les données en interne.

5. Politique de Sauvegarde des Données

Vous avez rédigé et appliquez une **politique interne** précisant les règles de sauvegarde : fréquence, durée de conservation, stockage hors site éventuel, et responsabilités associées.

6. Chiffrement/Déchiffrement des Données

Vous mettez en œuvre le **chiffrement** pour protéger les données sensibles, que ce soit pour leur stockage. Le chiffrement limite le risque en cas de perte ou vol.

7. Traçabilité d'accès aux Données

Vous tenez un **journal des accès** (logs) pour consigner qui accède à quelles données, quand et pourquoi. Cela facilite le contrôle, la détection d'incidents et les audits.

8. Documentation des Procédures de Sécurité

Vous avez formalisé vos **procédures de sécurité** dans des documents internes : contrôles d'accès, gestion des incidents, procédures d'urgence, règles pour les utilisateurs, etc.

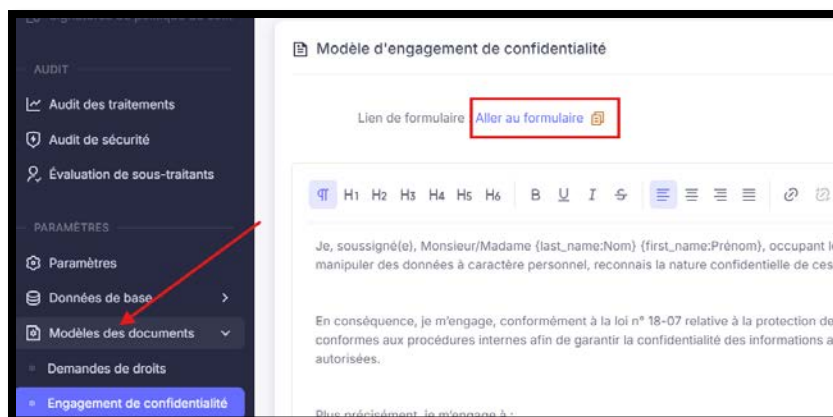
9. Sécurité d'accès Physique aux Locaux

Vous limitez l'accès physique aux zones où sont traitées ou stockées les données : serrures sécurisées, badges, surveillance physique ou gardiennage.

10. Mesures de Sécurité du Fichier Manuel

Si vous conservez des **données papier**, vous devez prévoir leur protection : armoires fermées à clé, salles d'archives sécurisées, accès restreint aux seules personnes habilitées.

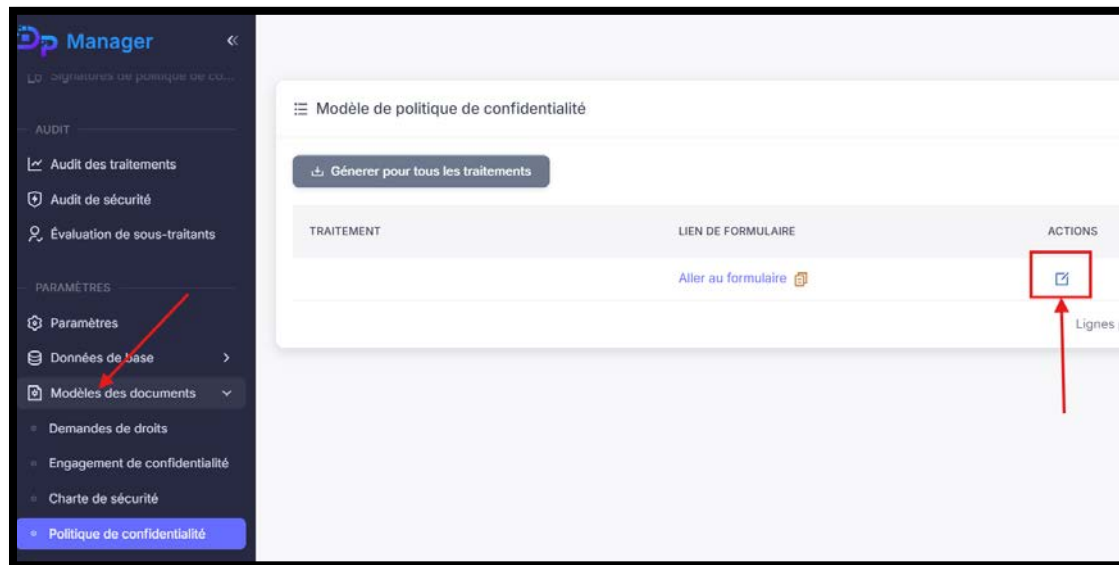
💡 Par ailleurs, l'ANPDP exige qu'un **engagement de confidentialité** soit lu et signé par tout employé ayant accès aux données personnelles. Pour vous accompagner, DP-Manager met à votre disposition un modèle d'engagement accessible dans le menu vertical à gauche, rubrique « **Documents** » comme indiqué sur l'image ci-dessous.



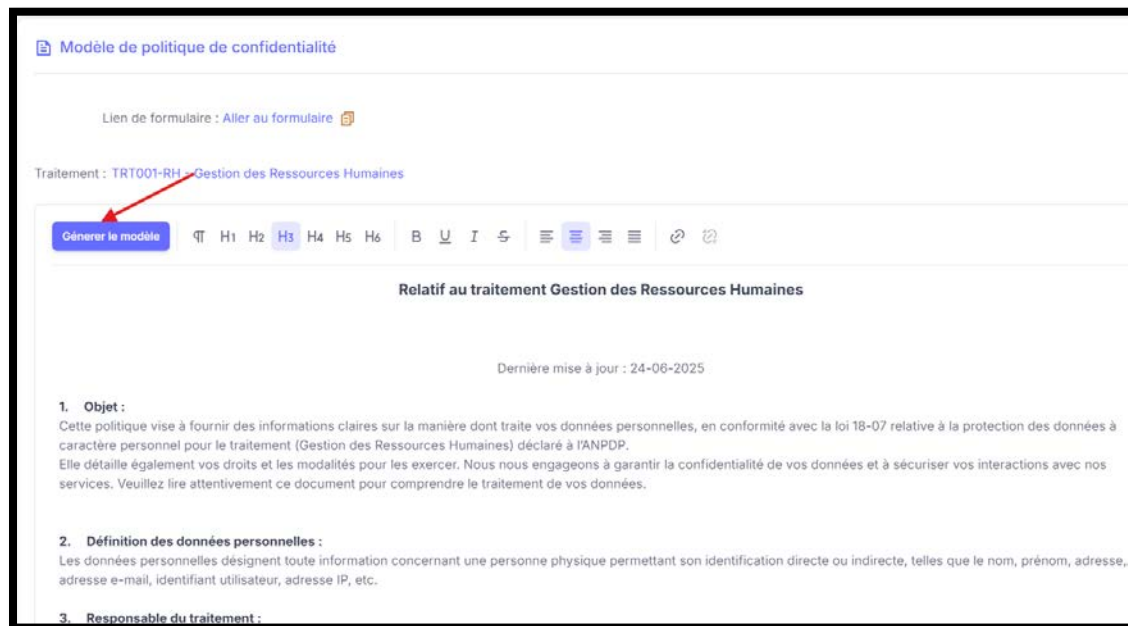
Informez et collectez le consentement avec DP-Manager

Maintenant que votre traitement est bien renseigné, Dp-Manager va générer pour vous une notice d'information ou une politique de confidentialité et vous permettra de la partager avec les personnes directement à travers un lien en ligne. Voyons maintenant comment générer cette notice :

Allez dans le menu vertical à gauche, rubrique « modèles de documents » puis choisissez l'option « politique de confidentialité »



Vous obtenez la fiche suivante :

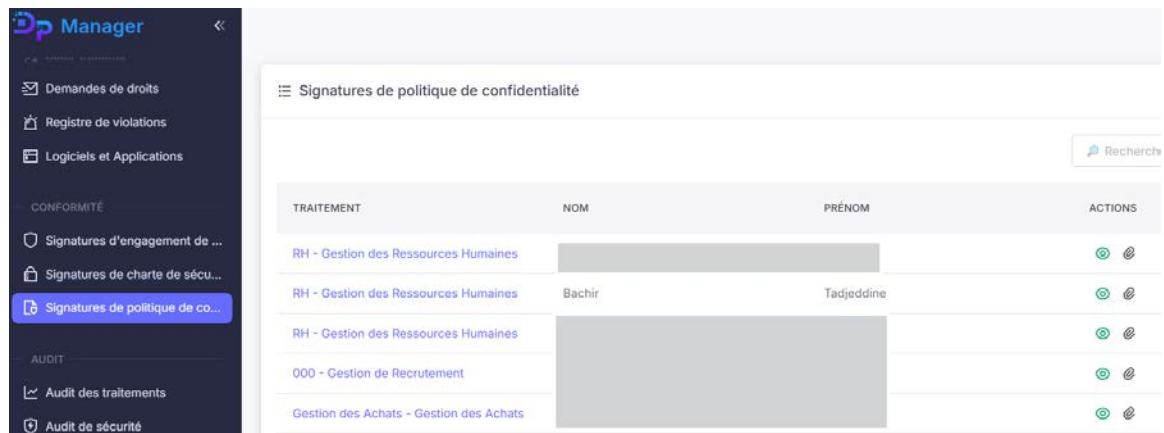


Cliquez sur le bouton « Générer le modèle » : cette action récupère automatiquement les informations que vous avez saisies pour le traitement et les intègre dans une structure standard de **politique de confidentialité** ou de **notice d'information**.

DP-Manager génère ensuite un **lien en ligne** vers ce document, consultable en ligne par les personnes concernées, qui pourront le remplir et le signer directement.



Chaque document signé par une personne est automatiquement enregistré et consultable dans le menu vertical à gauche, rubrique « Signatures de documents ».

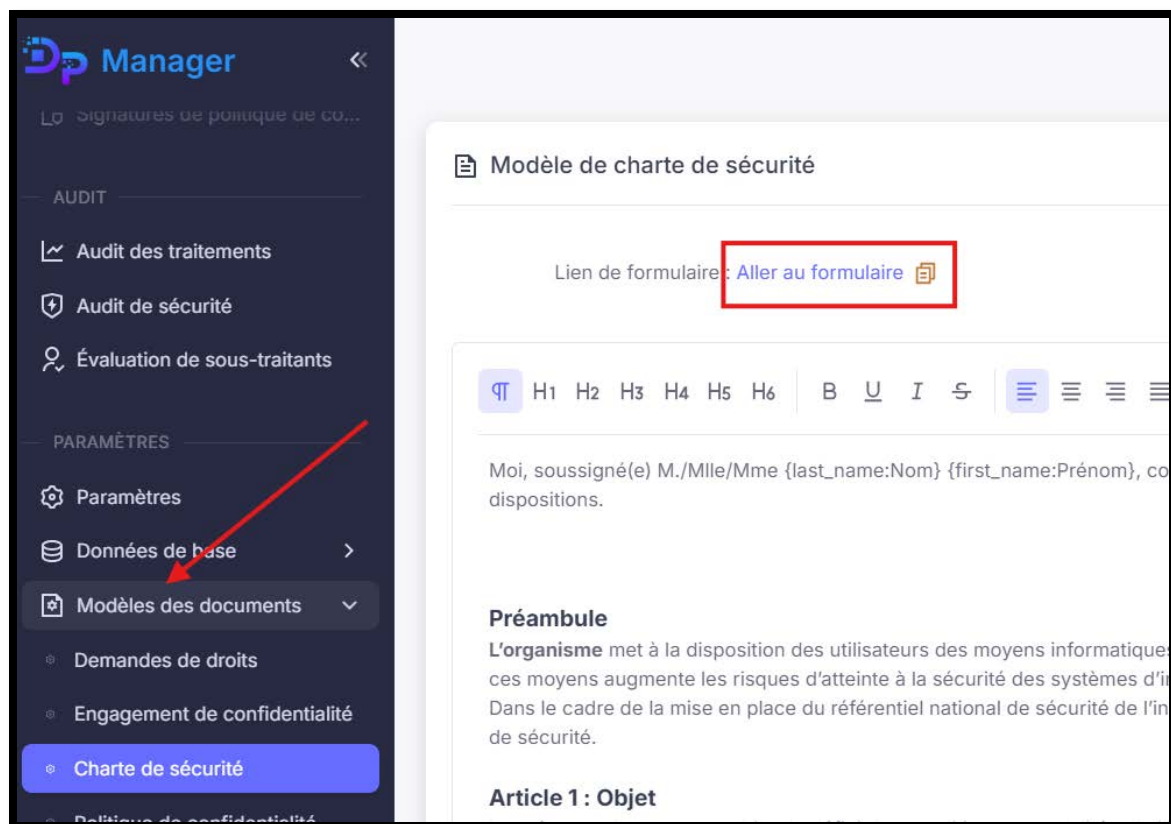


Faite signer la charte de sécurité informatique :

Dans le menu vertical à gauche, rubrique « Modèles de documents », vous trouverez la **charte de sécurité informatique** à faire signer par tous les employés ayant accès aux outils informatiques.

Cette charte est basée sur le Référentiel National de Sécurité de l'Information et peut être complétée ou adaptée selon les besoins spécifiques de votre organisme.

DP-Manager vous permet de partager un lien en ligne vers cette charte. Chaque personne qui la signe est automatiquement enregistrée dans la rubrique « Signatures » .

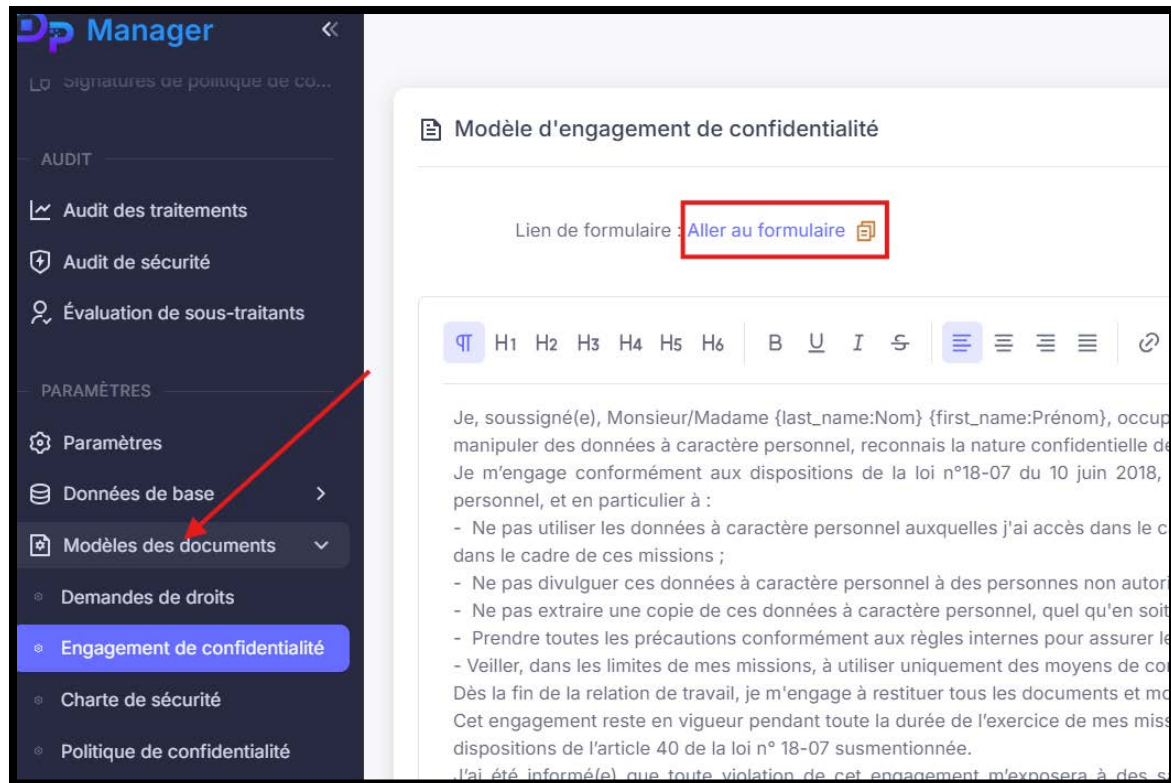


Faites signer l'engagement de confidentialité :

Dans le menu vertical à gauche, rubrique « **Modèles de documents** », vous trouverez un modèle d'engagement de confidentialité à faire signer par chaque employé ayant accès aux données à caractère personnel.

Cet engagement peut être complété ou personnalisé selon vos besoins internes.

DP-Manager vous permet de partager un lien en ligne vers ce document. Chaque signature est automatiquement enregistrée dans la rubrique « **Signatures** » du menu.



Déclarer automatiquement sur le portail de l'ANPDP via DP-Manager

Finaliser votre traitement et réserver votre rendez-vous

Documents requis pour votre entretien à l'ANPDP

Lever les éventuelles réserves

Sarl Leadersoft

Service commercial:

Yasmine 0560 57 26 96

Amina 0560 03 98 89

Imane 0560 95 21 28

Ilham O 0561 61 32 22

Ilham C 0560 01 25 11

Email : contact@leadersoft.dz

Service support :

Asma : 0560 03 98 97

Manal : 0560 32 28 50

Abdessamed : 0561 61 65 35

Support@leadersoft.dz