


# DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO) : DÉFINITION ET OUTILS PRATIQUES

Désignation du DPO obligatoire au plus tard d'ici au 1<sup>er</sup> janvier 2026 [art. 30c LIPDA]

 Le prestataire IT de la commune et le Préposé cantonal à la protection des données et à la transparence du Canton du Valais restent les interlocuteurs de référence pour cette thématique. Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

 Pour des raisons de lisibilité, sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.

## OBJECTIFS



**Comprendre** le rôle et les responsabilités respectives du responsable du traitement, du DPO et de la personne ou du groupe de personnes en charge des questions relatives à la protection et à la sécurité des données.



**Opter** pour le scénario le plus adapté lors de la désignation du DPO selon les besoins et ressources spécifiques de la commune.



**Désigner** un DPO selon les critères induits par la LIPDA.

## CONTEXTE

Les communes sont responsables des données personnelles des administrés. Une attention particulière doit donc être portée à la **sécurité**, à la **protection** ainsi qu'à la **transparence**.

Dans son article 30c, la LIPDA prévoit que **tout responsable du traitement** doit avoir nommé un DPO d'ici au 1<sup>er</sup> janvier 2026 (cf : Annexe II).

Dans la pratique, la **création d'une commission** à la protection des données au sein de la commune permet de renforcer la conformité légale, d'améliorer la gestion des données et de sensibiliser les différents acteurs communaux sur l'importance de la protection des données personnelles.

L'**annexe I** présente une vue d'ensemble des différents rôles et interactions des acteurs.

## QUI ?

### Exécutif communal

L'Exécutif communal a la **responsabilité légale** de veiller à ce que son administration fonctionne en conformité avec la LIPDA. En ce qui concerne les questions relatives à la protection et à la sécurité des données au sein de la commune, il doit prévoir dans le budget, les ressources humaines et financières nécessaires pour nommer en interne une personne ou un groupe de personnes, par exemple une commission à la protection des données. Pour pouvoir proposer un DPO et établir tous les liens utiles entre celui-ci et la commune, les ressources et le temps nécessaire devront être mis à disposition.

### Commission à la protection des données

La commission dédiée permet de concentrer l'expertise en matière de protection des données, garantissant ainsi une gestion conforme et efficace :

- 1 Elle assure le lien entre l'Exécutif communal et l'échelon opérationnel de la commune.
- 2 Elle traite toutes les questions en lien avec la protection des données, propose un DPO à l'autorité communale pour désignation.
- 3 Elle centralise et transmet les nouvelles finalités de traitement des données provenant du ou des responsables de traitement opérationnels à l'autorité communale pour validation, assurant ainsi une coordination efficace et conforme aux réglementations en vigueur.

L'**annexe IV** propose un cas d'usage pour une commission chargée de répondre aux questions de protection des données.

### Opérationnel communal

Les employés devront être sensibilisés et formés à la protection des données, notamment par le biais de formations dispensées ou organisées par le DPO. Ils devront appliquer les directives du DPO et être prêts à lui signaler toute violation de la LIPDA qu'ils pourraient constater. Les employés devront également être prêts, dans la limite de leurs attributions, à répondre aux questions des citoyens concernant le traitement de leurs données personnelles par la commune.

### Le délégué à la protection des données (DPO)

Le **DPO** joue un rôle clé dans la mise en œuvre des pratiques de protection des données au sein des autorités communales :

- 1 Il **conseille** l'administration communale sur la conformité aux règlements de protection des données, plus particulièrement sur la LIPDA.
- 2 Il **contrôle** l'application des normes de protection des données au sein de la commune.
- 3 Il est le **point de contact** avec les autorités externes comme l'autorité de surveillance (Préposé cantonal) et selon l'organisation, il répond aux demandes des administrés.
- 4 Il **organise** des formations et **sensibilise** les employés aux enjeux de la protection des données.





# LA DÉSIGNATION D'UN DPO : POINTS DE CONTRÔLE ET ACTIONS MINIMALES

Désignation du DPO obligatoire au plus tard d'ici au 1<sup>er</sup> janvier 2026 [art. 30c LIPDA]

Le profil d'un DPO n'est pas figé. Bien que l'**annexe III** propose un cahier des charges complet, il est essentiel de souligner que la personne retenue devra faire preuve de rigueur, de précision et respecter une confidentialité sans faille.

Ce poste présente les caractéristiques suivantes :

**Formation** : Formation de niveau supérieur, de préférence en droit ou spécifiquement en protection des données.

**Taux d'activité** : Il est plus important au début du processus de mise en conformité. Puis, il est évolutif en fonction des volumes de données traitées et des demandes du moment. La pratique tend à démontrer qu'un taux annualisé pour une commune de taille moyenne se situerait entre 0,2 et 0,3 EPT.

**Type de poste** : Les **annexes V et VI** détaillent les différents scénarios possibles. L'engagement d'un DPO peut se faire en interne, être externalisé à une entreprise spécialisée ou mutualisé avec d'autres communes ou partenaires, selon les besoins exprimés par l'Exécutif communal.

## POINTS DE CONTRÔLE

- Nous avons désigné une personne ou un groupe de personnes chargé des questions relatives à la protection et à la sécurité des données au sein de la commune.
- Le ou les responsables du traitement ont été définis au sein de la commune et leurs rôles sont clairs.
- Nous avons analysé les différents scénarios en lien avec la désignation d'un DPO.
- Nous avons désigné un DPO, conformément à l'article 30c de la LIPDA et son cahier des charges est clair (au plus tard d'ici au 01.01.2026).

## ACTIONS MINIMALES PROPOSÉES

### 1. Nommer une personne, un groupe de personnes en charge des questions de protection et de sécurité des données

Une personne ou un groupe de personnes (par ex. : création d'une commission ad hoc) clairement désigné au sein de l'administration doit être nommé pour les questions relatives à la protection et à la sécurité des données (cf : Annexe IV). Pour les plus grandes communes, il peut s'agir d'une commission spécifique incluant par exemple des membres de l'Exécutif ainsi qu'un ou des membres ayant une expertise en informatique ou en gestion des données. Il pourrait s'agir du responsable de la sécurité des systèmes d'information (RSSI), du responsable informatique ou du directeur des systèmes d'information (DSI) – en fonction de l'organisation communale.

Pour les communes ne disposant pas de ces profils spécialisés, le secrétaire communal peut, par exemple, être chargé de ces tâches avec l'appui du responsable informatique et/ou du conseiller en charge du numérique. La seule exigence est que la personne ou le groupe de personnes soit en mesure de répondre aux demandes et de fournir les informations requises par la LIPDA.

La loi ne prévoit pas explicitement la nomination de personnes chargées des questions de protection et de sécurité des données. Cependant, cette pratique est courante afin que les administrés sachent à qui s'adresser pour toute question relative à ce sujet. Leur rôle ne se limite pas à traiter directement les demandes spécifiques et complexes des administrés. Ils sont également responsables de la mise en œuvre de la stratégie de protection des données approuvée par l'Exécutif communal.

La fiche [eGov O.3](#) propose un cahier des charges de responsable cybersécurité.

### 2. Définir un ou des responsables du traitement

Le ou les responsables du traitement sont définis en fonction de la taille et de la structure organisationnelle de la commune. Il peut s'agir de l'Exécutif, ou d'un ou plusieurs chefs de service. Il détermine **les finalités et les moyens du traitement** des données à caractère personnel.

L'**annexe II** expose le rôle et les responsabilités du responsable de traitement.





# LA DÉSIGNATION D'UN DPO : POINTS DE CONTRÔLE ET ACTIONS MINIMALES

Désignation du DPO obligatoire au plus tard d'ici au 1<sup>er</sup> janvier 2026 [art. 30c LIPDA]

## 3. Analyser et choisir un scénario pour la désignation d'un DPO

Le responsable de traitement a pris connaissance des différents scénarios applicables à son organisation en fonction des ressources et des besoins de la commune afin de désigner un DPO à l'interne, à l'externe ou pour opter pour une mutualisation avec une autre autorité.

En **annexe V**, les différents scénarios «DPO» sont exposés. L'**annexe VI**, quant à elle, propose un tableau comparatif de ces scénarios.

## 4. Désigner un DPO

D'ici au **1<sup>er</sup> janvier 2026**, l'Exécutif communal en tant que responsable du traitement doit désigner formellement un DPO et en informer le Préposé cantonal à la protection des données et à la transparence (autorité de surveillance).

Une proposition de cahier des charges pour le DPO se trouve en **annexe III**.

## ANNEXES / RÉFÉRENCES

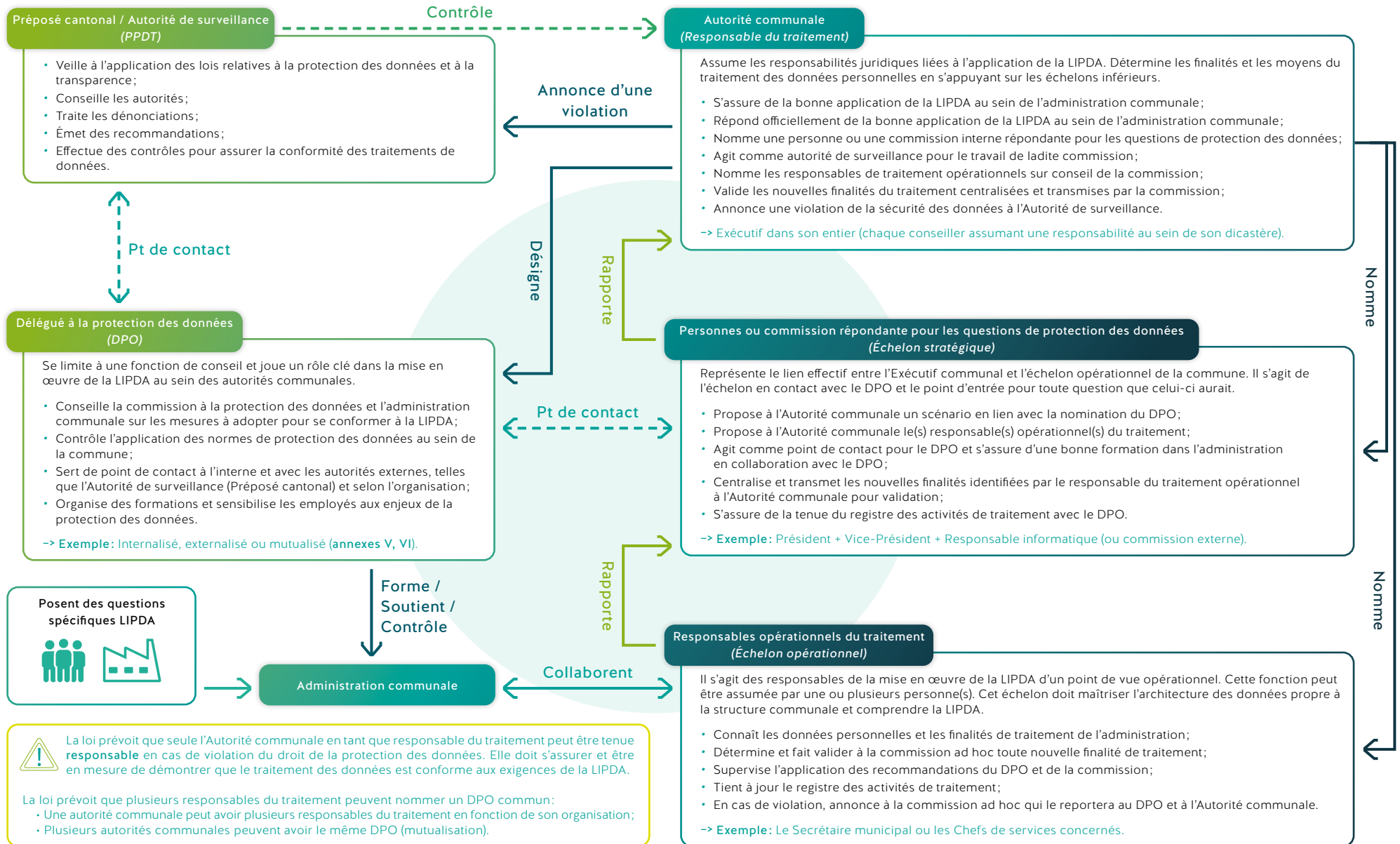
- I: La désignation d'un DPO: Acteurs et interactions
- II: Fiche sur le responsable du traitement
- III: Le délégué à la protection des données (DPO): Rôle et cahier des charges
- IV: Cas d'usage: Création d'une commission dédiée à la protection des données
- V: Scénarios envisageables pour la désignation d'un DPO
- VI: Tableau récapitulatif - analyse des différents scénarios



# LA DÉSIGNATION D'UN DPO : ACTEURS ET INTERACTIONS

Désignation du DPO obligatoire au plus tard d'ici au 1<sup>er</sup> janvier 2026 [art. 30c LIPDA]

## EN BREF : ACTEURS IMPLIQUÉS ET LEURS INTERACTIONS



## FICHE SUR LE RESPONSABLE DU TRAITEMENT



Le prestataire IT de la commune et le Préposé cantonal à la protection des données et à la transparence du Canton du Valais restent les interlocuteurs de référence pour cette thématique. Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.



Pour des raisons de lisibilité, sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.

D'un point de vue légal, le responsable du traitement est l'entité en charge de la stratégie de gestion des données personnelles, incluant leur collecte, stockage, traitement et protection. En cas de violation, il doit en informer l'autorité de surveillance, conformément aux conseils du DPO et de la personne ou commission chargée des questions relatives à la protection et à la sécurité des données. Selon l'organisation communale et les décisions prises par l'exécutif, cette responsabilité peut incomber à l'ensemble de l'Exécutif communal ou à un ou plusieurs services spécifiques.

Par exemple, le conseiller municipal en charge d'un dicastère sera tenu pour responsable si le chef de service concerné est désigné comme responsable du traitement. En revanche, l'exécutif dans son ensemble sera responsable uniquement dans les situations où il est collectivement désigné comme responsable du traitement, faute de désignation d'un ou plusieurs chefs de service spécifique pour cette responsabilité.

Le responsable du traitement des données détermine les **finalités** et les **moyens** du traitement des données à caractère personnel. Ainsi, si l'autorité communale décide «**pourquoi**» et «**comment**» les données à caractère personnel devraient être traitées, elle est la responsable du traitement.

### Exemple de finalité de traitement de données personnelles :

- Gestion du fichier des habitants : enregistrement et mise à jour des informations sur les résidents de la commune pour la gestion administrative, les services de vote, et d'autres obligations légales ;
- Gestion des impôts communaux : collecte des données pour l'établissement des bases d'imposition et le recouvrement des taxes locales ;
- Etc.

### Exemple de moyen de traitement de données personnelles :

- Formulaire papier ;
- Portail en ligne pour les services aux citoyens ;
- Système de vidéosurveillance ;
- Base de données des résidents ;
- Logiciel de gestion des ressources humaines ;
- Plateforme de gestion électronique des documents (GED) ;
- Etc.

Les employés communaux qui traitent les données à caractère personnel au sein de l'administration communale agissent sous la direction du responsable du traitement, dans le cadre des missions qui leur sont confiées. Le responsable du traitement est chargé de garantir la conformité des traitements de données avec la législation en vigueur et de superviser l'application des recommandations émises par le DPO et la commission. En somme, il incombe au responsable du traitement de valider les **finalités** et les **moyens** de traitement des données personnelles proposés par la commission.

Le responsable du traitement doit également s'assurer que le DPO dispose de l'**indépendance, du temps et des moyens** requis pour accomplir ses tâches.

Concrètement, l'Exécutif communal peut décider que le responsable du traitement est le secrétaire municipal. Ce dernier ne peut de facto pas être nommé DPO, mais il a une excellente connaissance des processus internes et un lien privilégié avec l'Exécutif, ce qui en fait un bon candidat. Si les ressources humaines et la structure de l'administration le permettent, le responsable informatique (interne) de la commune pourrait également assumer ce rôle. Il est à relever que quelque soit le choix final, **la responsabilité juridique incombe toujours à l'exécutif communal.**





## FICHE SUR LE RESPONSABLE DU TRAITEMENT

### EN BREF : QUE DOIT FAIRE UN RESPONSABLE DU TRAITEMENT ?

Le responsable du traitement doit:

- Nommer un DPO d'ici au 1<sup>er</sup> janvier 2026 ;
- Mettre à disposition du DPO les moyens nécessaires pour l'accomplissement de ses tâches: l'indépendance, les ressources, un accès aux informations ;
- Définir et valider les finalités et les moyens du traitement des données personnelles en collaboration avec la commission ;
- S'assurer de la conformité des traitements avec la législation en vigueur ;
- Superviser l'application des recommandations du DPO par l'opérationnel communal ;
- Adopter une stratégie de protection des données grâce à des mesures techniques et organisationnelles, telles que:
  - Désigner une personne ou un groupe de personnes (par ex.: création d'une commission) chargé des questions relatives à la protection et à la sécurité des données,
  - Limiter l'accès aux données,
  - Sécuriser les postes de travail,
  - Mettre en œuvre des procédures de gestion des incidents et de journalisation des accès, etc. ;
- Annoncer les violations de sécurité des données personnelles au Préposé cantonal et s'assurer qu'elles soient correctement enregistrées et traitées, en coordination avec le DPO et la personne ou le groupe de personnes en charge des questions relatives à la sécurité et protection des données.

# LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO) : RÔLE ET CAHIER DES CHARGES



Le prestataire IT de la commune et le Préposé cantonal à la protection des données et à la transparence du Canton du Valais restent les interlocuteurs de référence pour cette thématique. Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.



Pour des raisons de lisibilité, sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.

## PROFIL

Le DPO devrait être désigné **en interne**. Toutefois, en fonction des ressources disponibles, il se peut que l'intégralité ou une partie des activités soient **mutualisées** avec d'autres administrations communales ou **sous-traitées**.

Une **formation de niveau supérieur**, idéalement dans le domaine de la cybersécurité et/ou juridique, convient pour le rôle qui exige rigueur, précision et discrétion. Le DPO doit être capable de décider, d'agir, de planifier et d'organiser. Il doit posséder d'excellentes compétences en matière de communication, car il devra **sensibiliser, superviser et informer** les employés communaux.

Le taux d'activité annualisé sera de l'ordre de **20 à 30% en EPT**, en fonction du nombre de collaborateurs, du volume des données traitées et de la part de l'activité externalisée.

## RESPONSABILITÉ ET CADRE LÉGAL

Le DPO se voit mettre à disposition les **moyens nécessaires** pour l'accomplissement de ses tâches par le responsable de traitement:

- 1 **L'indépendance** : Le DPO doit pouvoir agir sans être influencé;
- 2 **Les ressources** : Le DPO doit avoir un **budget** suffisant et du **temps** alloué pour ses tâches;
- 3 **Un accès aux informations** : Le DPO doit avoir **accès aux données** requises pour l'exercice de sa fonction.

S'il peut exercer d'autres tâches que celles liées à sa fonction de DPO, celles-ci ne doivent pas entraver l'exercice de ses missions de DPO. Par exemple, **un secrétaire communal** ou **un élu** ne peut pas exercer la fonction de DPO pour la commune dans laquelle il travaille **en raison d'un conflit d'intérêts**, car il participe aux décisions concernant le traitement des données effectué par cette commune. **Les fonctions dirigeantes** telles que la direction, les responsables RH ou les responsables informatiques sont **incompatibles** avec les tâches du DPO, contrairement aux rôles de juriste ou de délégué à la sécurité de l'information.

**Le DPO ne doit pas craindre de subir un licenciement ou une rupture de contrat en raison de l'exécution de ses missions.**

## TÂCHES ET MISSIONS PRINCIPALES

La fonction d'un DPO est double:

### A Dans sa fonction interne

1. **Aider l'exécutif** à mettre en place les processus de conformité aux règles légales applicables;
2. **Proposer des mesures** en cas de constatation de violations des règles de protection des données personnelles;
3. **S'assurer que les collaborateurs soient sensibilisés** à l'importance de la protection des données et aient reçu les formations nécessaires;
4. **Venir en soutien au responsable du traitement** à la tenue du **registre des activités de traitement** et à la **réalisation d'analyses d'impact** lorsque cela est nécessaire, en collaboration avec la personne ou le groupe de personnes en charge des questions relatives à la sécurité et à la protection des données.







# LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO) : RÔLE ET CAHIER DES CHARGES

## B En tant que représentant externe

1. Il définit **les modalités de réponse** et est le **point de contact** dans le cadre d'une demande d'accès, de rectification ou d'effacement de données personnelles **des administrés**. Selon l'organisation de la commune, il transmet à la personne requérante les coordonnées du responsable du traitement ou de la personne ou du groupe de personnes en charge des questions relatives à la sécurité et à la protection des données;
2. Il est la personne **de contact des autorités et de l'autorité de surveillance** en matière de protection des données (Préposé cantonal). Il se charge de **communiquer** avec les autorités compétentes les informations qui doivent leur être transmises, notamment dans la **tenue du registre des activités de traitement cantonal** et de **l'annonce des violations** de la sécurité des données personnelles **en coordination avec le responsable de traitement**.

Le rôle du DPO se limite à une fonction de conseil et celui-ci ne devrait pas prendre de décision quant au traitement.

## CAHIER DES CHARGES

Lors de la désignation d'un DPO, il est essentiel de vérifier que la personne sélectionnée en interne ou le prestataire spécialisé choisi en cas d'externalisation, assure les activités suivantes :

### Mise en œuvre du programme de conformité LIPDA :

- Proposer les mesures nécessaires à la mise en œuvre du programme de conformité, en collaboration avec la personne ou le groupe de personnes en charge des questions relatives à la sécurité et à la protection des données, qui devront être **approuvés par l'exécutif**.

### Conseil et formation :

- Fournir les **conseils** nécessaires à l'exécutif et aux collaborateurs. Il s'assure que les informations et formations nécessaires sont données aux collaborateurs, afin que ces derniers mettent correctement en application le programme de conformité.
- Vérifier et mettre à jour **les contrats de sous-traitance** et autres documents légaux.

### Surveillance de la conformité :

- S'assurer du respect des bases légales applicables par le **responsable de traitement** ;
- Informer l'Exécutif communal et proposer les mesures à prendre lorsqu'**une violation** des bases légales est constatée.

### Analyses d'impact :

- Participer à la réalisation d'analyses d'impact lorsqu'un traitement est envisagé et susceptible de présenter un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (administrés).

### Gestion des demandes des personnes concernées :

- Soutenir le responsable du traitement et la personne ou le groupe de personnes en charge des questions relatives à la sécurité et à la protection des données pour traiter les requêtes des personnes concernées, notamment lorsque celles-ci exercent le **droit à l'effacement** ou à la **rectification** des données, le **droit d'opposition**, ou encore **une demande d'accès**.

### Point de contact pour les autorités de surveillance :

- Transmettre au Préposé cantonal les informations requises pour le Registre cantonal des activités de traitement en collaboration avec le responsable du traitement ;
- Informer le Préposé cantonal de toute violation de la sécurité des données personnelles en coordination avec le responsable du traitement ;
- Rester à disposition du Préposé pour toute requête et lui fournir les informations requises.

### Mise en place et gestion du registre des activités de traitement interne :

- Mettre en place le registre des activités de traitement en collaboration avec le responsable du traitement interne ;
- S'assurer que les informations qu'il contient sont exactes et régulièrement mises à jour.



## CAS D'USAGE : CRÉATION D'UNE COMMISSION DÉDIÉE À LA PROTECTION DES DONNÉES



Le prestataire IT de la commune et le Préposé cantonal à la protection des données et à la transparence du Canton du Valais restent les interlocuteurs de référence pour cette thématique. Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.



Pour des raisons de lisibilité, sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.

Dans la pratique, la création d'une commission dédiée à la protection des données offre de nombreux avantages. Elle permet de concentrer l'expertise nécessaire pour assurer une gestion conforme et efficace des données, grâce à des membres formés et constamment mis à jour sur les législations et les meilleures pratiques.

### STRUCTURE ET FONCTIONS DE LA COMMISSION

#### Composition:

- La commission devrait inclure des membres ayant une expertise en droit, en informatique, et en gestion des données (le responsable de la sécurité des systèmes d'information (RSSI), le responsable informatique ou le directeur des systèmes d'information (DSI)).
- Un Président, un Vice-Président et/ou par exemple un Conseiller en charge du numérique pourraient être nommés pour diriger les activités de la commission.

#### Attributions:

- Sur demande de l'Autorité communale, examiner et proposer les politiques de protection des données de la commune en suivant les recommandations du DPO.
- Superviser les traitements des données personnelles et assurer leur conformité avec les lois et règlements applicables en collaboration avec le DPO.
- Gérer les demandes d'accès aux documents officiels et les plaintes liées à la protection des données.
- Collaborer avec les autorités telles que le Préposé à la protection des données et à la transparence avec le soutien du DPO.
- Proposer à l'Autorité communale un scénario en lien avec la nomination du DPO.
- Proposer à l'Autorité communale le(s) responsable(s) opérationnel(s) du traitement.
- Agir comme point de contact pour le DPO et s'assurer d'une bonne formation dans l'administration communale en collaboration avec le DPO.
- Centraliser et transmettre les nouvelles finalités identifiées par le responsable du traitement opérationnel à l'Autorité communale pour validation.
- S'assurer de la tenue du registre des activités de traitement en collaboration avec le DPO.

#### Fonctionnement:

- La commission devrait se réunir régulièrement (par exemple 2 à 3 fois par année) pour discuter des questions en cours et évaluer les pratiques de protection des données.
- Des rapports périodiques devraient être produits pour informer le conseil communal et les citoyens des activités et des résultats de la commission.

Cette commission garantit que la commune respecte les lois en vigueur, comme la LIPDA, et applique correctement les règlements associés. Elle joue également un rôle crucial dans la gestion des incidents de violation de données, en assurant une communication rapide avec le responsable de traitement et l'Autorité de surveillance ainsi qu'en mettant en place des mesures correctives.

En centralisant les efforts de protection des données, la commission évite les doublons et garantit une approche cohérente, tout en coordonnant avec d'autres entités et autorités, pour harmoniser les pratiques et politiques. De plus, elle organise – en collaboration avec le DPO – des sessions de sensibilisation et de formation pour le personnel communal, et informe les citoyens sur leurs droits et les mesures de protection en place.

La commission évalue régulièrement les politiques et pratiques de protection des données de la commune, proposant des améliorations et des mises à jour en fonction des évolutions législatives et technologiques.

# SCÉNARIOS ENVISAGEABLES POUR LA DÉSIGNATION D'UN DPO



Le prestataire IT de la commune et le Préposé cantonal à la protection des données et à la transparence du Canton du Valais restent les interlocuteurs de référence pour cette thématique. Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.



Pour des raisons de lisibilité, sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.

Chaque commune doit évaluer ses propres **besoins, ressources et priorités** pour choisir le scénario le plus adapté. La décision pourrait être influencée par **la taille** de la commune, **le volume et la complexité des données traitées**, ainsi que **les ressources financières et humaines disponibles**.

## A Internalisation

La fonction de DPO est pleinement assumée par un employé de la commune, agissant soit à temps plein, soit partiel.

### AVANTAGES

- **Connaissance** accrue de l'organisation interne;
- **Proximité** avec les collaborateurs;
- **Plus grande réactivité** aux sollicitations internes;
- **Disponibilité** en cas de contrôle de l'autorité.

### INCONVÉNIENTS

- **Risque de conflits d'intérêts** avec d'autres fonctions internes (en cas de temps partiel dédié au rôle de DPO);
- **Difficulté à trouver un profil pertinent**, particulièrement pour des pourcentages de travail < 50%;
- Coûts en cas de sous-occupation.

## B Externalisation

Le responsable du traitement **externalise** les services de DPO via un contrat de mandat, **tout en conservant un référent interne à la sécurité et protection des données** pour se coordonner avec le DPO externe:

### AVANTAGES

- **Expertise** et utilisation d'outils spécifiques;
- **Haut degré de spécialisation** et connaissance des bonnes pratiques;
- **Facilitation** en cas d'absence de ressources humaines internes;
- **Flexibilité** de l'organisation de travail;
- **Ratio coût/bénéfice positif** pour les petites communes.

### INCONVÉNIENTS

- **Moins grande intégration** du DPO dans l'organisation interne;
- **Disponibilité** moins grande;
- **Nécessite quand même la nomination d'un référent interne à la sécurité et protection des données** avec qui le DPO externe doit pouvoir interagir;
- **Coûts** peuvent être élevés en cas de besoins réguliers (notamment pour les grandes communes).

## C Mutualisation

**Plusieurs responsables du traitement** peuvent se regrouper pour nommer un DPO **conjointement**. Cette mutualisation peut se réaliser entre différentes communes et/ou autorités.

### AVANTAGES

- **Partage des coûts** (économie d'échelle);
- Plus grande facilité à trouver un profil pertinent en raison du taux d'activité élevé (un 100%);
- **Uniformisation** des programmes de conformité entre communes;
- **Expérience transversale** parmi toutes les communes;
- **Renforcement de l'expertise** du DPO aux besoins spécifiques des communes.

### INCONVÉNIENTS

- La plupart des inconvénients liés à un DPO externe (moins grande intégration au sein de chaque organisation, disponibilité moins grande);
- **Risque de perte d'efficacité** en cas d'isolement du DPO mutualisé;
- **Complexité de l'organisation**.





# SCÉNARIOS ENVISAGEABLES POUR LA DÉSIGNATION D'UN DPO

## D Solution hybride

Le **responsable du traitement** peut opter pour une organisation comprenant un mélange d'internalisation, d'externalisation et/ou de mutualisation :

1. **Échelon 1** : Chaque petite commune nomme une personne responsable de la sécurité et de la protection des données (LIPDA), qui y consacre environ 10% de son temps.
2. **Échelon 2** : Un DPO mutualisé est nommé pour plusieurs communes ou une région, afin de coordonner les efforts de conformité.
3. **Échelon 3** : Un prestataire externe spécialisé est engagé pour les tâches complexes telles que l'élaboration de documentations modèles et le traitement de cas complexes.

Il est crucial que les rôles et responsabilités soient clairement définis à chaque niveau pour assurer une protection efficace des données personnelles.

### AVANTAGES

- **Maximisation des avantages** de chacune des solutions.

### INCONVÉNIENTS

- Coût variable selon les modalités ;
- **Plus complexe à mettre en place** ;
- Risque de défaillance si l'attribution des rôles n'est pas claire (dilution des responsabilités).

## TABLEAU R CAPITULATIF – ANALYSE DES DIFF RENTS SC NARIOS



Le prestataire IT de la commune et le Pr pos  cantonal   la protection des donn es et   la transparence du Canton du Valais restent les interlocuteurs de r f rence pour cette th matique. Cette fiche doit  tre consid r e comme indicative et n'est en aucun cas exhaustive.



Pour des raisons de lisibilit , sauf mention sp cifique, toute d nomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.

	INTERNALISATION (TAUX PARTIEL)	INTERNALISATION (TAUX PLEIN 80%)	EXTERNALISATION	MUTUALISATION	SELON HYBRIDE
<b>Taille de la commune</b>	Petites � moyennes communes	Grandes communes / villes	Petite et moyenne commune	Petites communes	Potentiel de solution optimale
<b>Comp�tences du DPO (m�tier et personnelles)</b>	Difficile � obtenir	Va d�pendre du profil trouv�	Prestataires externes avec comp�tences de pointe	Va d�pendre du profil trouv�	Capacit� d'aller chercher les ressources n�cessaires
<b>Int�gration et connaissance de l'organisation interne</b>	�lev�	�lev�	Difficile � assurer en pratique	Va d�pendre de l'organisation choisie	Va d�pendre de l'organisation choisie
<b>Ind�pendance / pr�vention des conflits d'int�r�ts</b>	Difficile	En principe, OK	�lev�	Moyen	Va d�pendre de l'organisation choisie
<b>Risques li�s � la protection des donn�es</b>	Restent � l'ex�cutif	Restent � l'ex�cutif	Externalisation d'une partie du risque au prestataire, selon le contrat en place	Va d�pendre de l'organisation choisie	Va d�pendre de l'organisation choisie
<b>Co�ts pour la commune</b>	Moyen	Important	De moyen � important (co�ts externes + co�ts internes du r�pondant)	Moyen	En principe, faibles
<b>Pertinence</b>	Pertinent pour les communes de petite taille ou de taille moyenne disposant � l'interne d'une personne apte � exercer cette fonction. Pr�voir en tout cas un 20 � 30% d�volu � cette activit�. � �viter dans les autres cas.	Solution � privil�gier pour les villes / grandes communes.	Une option pour les petites ou moyennes communes sans ressource sp�cialis�e disponible et pour lesquelles une mutualisation ne serait pas envisageable. Le choix du prestataire est important.	Une bonne solution en th�orie pour les petites communes dont l'organisation est semblable. Pourrait s'av�rer compliqu� en pratique.	Potentiel de solution optimale (tous les avantages), mais �galement de complexification. N�cessite une mise en place r�fl�ch�e.