Caisse de prévoyance du Canton du Valais
(CPVAL)

Règlement de traitement des données personnelles

Table des matières

1. Introduction

1.1. Base légale, objet et portée ce de règlement de traitement

Ce règlement de traitement, basé sur les articles 5 et 6 de l'Ordonnance sur la Protection des Données du 31 août 2022 (**« OPDo »**) s'applique à tous les traitements automatisés de données personnelles par la Caisse de prévoyance du Canton du Valais (**« CPVAL »**), Rue du Chanoine-Berchtold 30, 1950 Sion, comme Responsable de Traitement au sens de la Loi fédérale sur la Protection des Données du 25 septembre 2020 (**« LPD »**). Le règlement de traitement contient des informations sur l'organisation interne, les procédures de traitement et de contrôle des données, ainsi qu'une description des mesures visant à garantir la sécurité des données.

1.2. Actualité du règlement de traitement

Ce règlement est régulièrement mis à jour par la Direction de CPVAL et mis à la disposition du conseiller à la protection des données de CPVAL (**« DPO »**) afin de documenter notamment les modifications du système. Dans tous les cas, la Direction vérifie annuellement le règlement pour s'assurer de sa mise à jour et informe le DPO de toute modification ou confirme sa mise à jour. La version actuelle et une liste des versions antérieures sont répertoriées dans la section 6

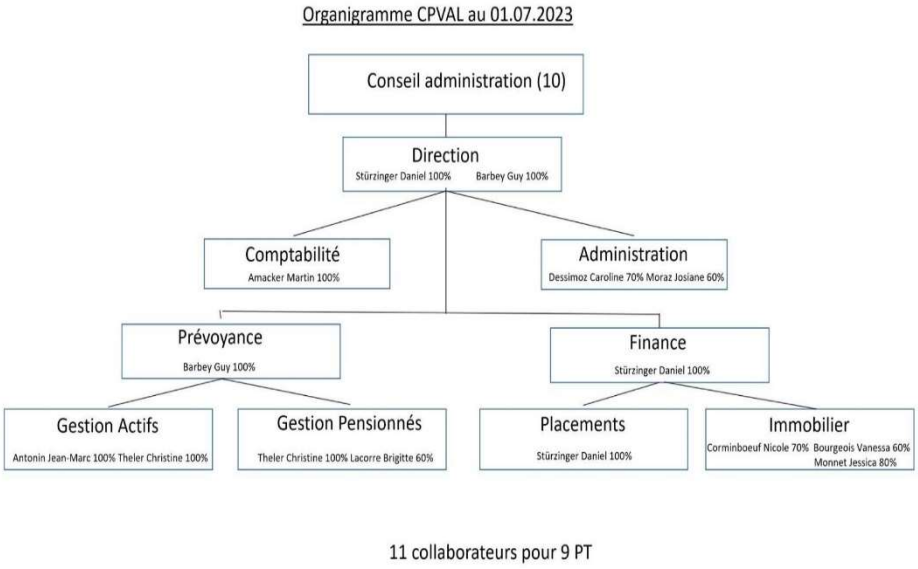
1.3. Définitions et abréviations

Les abréviations suivantes sont utilisées dans le document :

Abréviation	Description
DPO	Conseiller à la protection des données chez CPVAL
LPD	Loi fédérale du 25 septembre 2020 sur la protection des données
OPDo	Ordonnance relative à la loi fédérale sur la protection des données du 31 août 2022
PFPDT	Préposé fédéral à la protection des données et à la transparence
SCI	Service cantonal de l'informatique

2. Organisation interne

2.1. Organigramme



2.2. Responsabilités

Le **Conseil d'administration** de CPVAL assume la responsabilité globale du respect de la protection des données. Il délègue la mise en place d'une organisation adaptée à la Direction.

La **Direction** est responsable de la promulgation, de la mise en œuvre, de la communication, du contrôle et de la surveillance du règlement de traitement de CPVAL. Elle s'assure que CPVAL dispose d'une organisation efficace qui garantisse la conformité en matière de protection des données. À cette fin, elle désigne un conseiller à la protection des données (DPO), qui veille à la mise en œuvre des exigences en matière de protection des données

Le **DPO** indique les principaux comportements à adopter en matière de protection des données et veille au respect des dispositions légales en matière de protection des données applicable à CPVAL. Au nom de la Direction et en coopération avec les services internes concernés, le DPO élabore des instructions et des directives appropriées pour le respect des lois et normes.

Tous **les employés** de CPVAL sont responsables du respect des exigences en matière de protection des données dans leur domaine de compétence. Chaque employé de CPVAL doit signer une politique de confidentialité lors de son embauche. La Direction veille à ce que les collaborateurs soient informés en permanence des dispositions légales et internes en vigueur.

3. Activités de traitement et de contrôle des données

3.1. Infrastructure informatique de CPVAL

3.1.1. Aperçu des principales applications

La mise en œuvre de la prévoyance professionnelle s'effectue via l'infrastructure informatique ci-dessous :

Domaine	Description	Données personnelles
Prévoyance	Logiciel de mise en œuvre du système de prévoyance professionnelle / d'administration des fonds de pension.	OUI
	Logiciel de gestion et d'archivage des documents pour les personnes assurées et bénéficiaires de rentes	OUI
Gestion de fortune	Logiciels de gestion de la fortune immobilière directe	OUI
	Logiciels de gestion de la fortune mobilière	NON
Gestion comptable	Logiciels de gestion comptable	NON

Les services informatiques de base comprenant notamment la gestion des PC, de la messagerie, le partage de fichiers, la téléphonie et les accès Internet sont hébergés et opérés par le Service cantonal de l'informatique (SCI).

Il en est de même pour les applications métiers en matière de prévoyance, gestion comptable et gestion de fortune.

3.2. Traitement de l'information

3.2.1. Finalité du traitement des données

La CPVAL traite les données personnelles principalement dans le but de mettre en œuvre la prévoyance professionnelle obligatoire et surobligatoire. Cela inclut par exemple :

- La conclusion et le traitement des **contrats d'affiliation** avec l'employeur, l'exécution des droits légaux découlant des contrats, la comptabilité et la résiliation des contrats ;
- L'admission **des assurés** : à cette fin, CPVAL traite notamment les données de base. CPVAL tient ensuite un ou plusieurs comptes pour chaque assuré, pour lesquels CPVAL traite les informations sur les cotisations, les rachats, les avoirs de vieillesse et les versements ;
- L'examen et le traitement des **demandes de pension** y compris la coordination avec d'autres assureurs tels que l'assurance invalidité et l'exécution des recours. À cette fin, CPVAL traite principalement les données contractuelles, de cas et de prestations de la personne assurée et des proches et bénéficiaires, ainsi que les données de santé et les données de tiers telles que des experts externes et des prestataires de services.

En outre, la CPVAL traite également les données personnelles à des fins liées à la mise en œuvre de la prévoyance professionnelle, par exemple pour la communication, le traitement des contrats, la sécurité et la prévention, le respect des exigences légales, la protection juridique et dans le cadre des processus internes et de l'administration.

Dans le domaine obligatoire, le traitement des données personnelles concerne les finalités définies à l'article 85a de la loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité (LPP).

3.2.2. Origine des données personnelles

En tant que responsable, CPVAL traite principalement les données personnelles nécessaires à la mise en œuvre de la prévoyance professionnelle, principalement celles provenant d'employeurs actuels ou anciens qui sont légalement tenus de transmettre à CPVAL toutes les données nécessaires à la mise en œuvre de la prévoyance professionnelle. En outre, les données personnelles peuvent également provenir d'autres tiers, par exemple des membres de la famille des assurés, des autorités ou des institutions de prévoyance et de libre passage.

3.2.3. Catégories de données

Les catégories de données suivantes sont traitées dans les applications (systèmes) respectives et sont protégées contre tout accès non autorisé par des mesures techniques et organisationnelles appropriées (voir section 4

- Données de base
- Données du contrat
- Données de performance
- Données financières
- Données de communication
- Données de santé
- Données provenant de tiers (par exemple proches, employeurs, experts externes, prestataires de services)

3.2.4. Rectification des données

Une fois identifiées, les personnes enregistrées peuvent demander que les données enregistrées les concernant soient rectifiées ou détruites. Le DPO statue sur les demandes correspondantes.

3.2.5. Divulgation de données

Les données peuvent être transmises aux catégories de destinataires suivantes :

- Employeur
- Institutions de libre passage, autres institutions de prévoyance
- Autorités et bureaux
- Autres personnes (par exemple personnes impliquées dans une procédure devant les tribunaux ou les autorités, bénéficiaires, institutions financières et autres organismes impliqués dans une transaction juridique)
- Sous-traitants (prestataire de services)

Dans le domaine obligatoire, le transfert de données personnelles est limité au cadre légal (art. 86a LPP).

3.2.6. Stockage, conservation et archivage des données personnelles

Les données personnelles sont stockées et conservées aux fins et pour les périodes suivantes :

- Aussi longtemps que cela est nécessaire à la finalité du traitement (par exemple, affiliation pension en cours) ;
- Selon l'obligation de conservation des données (notamment art. 27i et suivants de l'ordonnance sur la prévoyance professionnelle vieillesse, survivants et invalidité, OPP 2) ;
- Selon les intérêts légitimes de CPVAL. Cela peut être le cas en particulier si les données personnelles sont nécessaires pour faire valoir ou se défendre contre des réclamations, ainsi qu'à des fins d'archivage et pour assurer la sécurité informatique.

La procédure de stockage/suppression des données est documentée dans le référentiel d'archivage mis en place par CPVAL. Ce qui suit s'applique spécifiquement à CPVAL en ce qui concerne le stockage des données :

- Lorsqu'aucune prestation de prévoyance n'est versée parce que la personne assurée n'a pas fait usage de son droit, les données seront conservées jusqu'à ce que la personne concernée ait 100 ans, après quoi l'intégralité du compte sera supprimée ;
- En cas de sortie de CPVAL, les données seront supprimés 10 ans après la date de sortie, respectivement la date de paiement de la prestation ;
- Dans le cas des pensionnés de vieillesse, les données seront supprimées 10 ans après le décès du pensionné de vieillesse ; dans le cas des prestations de survivants qui en résultent, les deux comptes (pensionné de vieillesse et pensionné de survivant) seront supprimés 10 ans après la fin de la prestation (décès du pensionné de survie) ;
- Dans le cas des rentes d'enfants et d'orphelins, les données sont supprimées 10 ans après la date réglementaire de la fin du droit à la prestation ;
- En cas de rentes de divorce, les données seront supprimées 10 ans après le décès du bénéficiaire ;

En règle générale, les documents Excel et Word contenant des données personnelles sont supprimés au bout de 10 ans.

3.2.7. Pseudonymisation et anonymisation des données personnelles

Les évaluations et les tests sont basés sur des données génériques et non personnelles. Les données statistiques sont anonymisées conformément aux exigences légales. Il n'est pas possible de tirer des conclusions sur des personnes spécifiques.

3.2.8. Suppression et destruction des données personnelles

La procédure de suppression des données est documentée dans une directive de stockage/suppression détaillée.

3.3. Procédures de contrôle

3.3.1. Autorisations et accès

Chaque employé de CPVAL a uniquement accès aux données dont il a besoin pour accomplir ses tâches.

Pour protéger les systèmes, l'accès n'est généralement possible qu'en vérifiant l'autorisation de la personne qui accède à l'aide d'un nom d'utilisateur/mot de passe (authentification). Les applications informatiques ayant accès à des données sensibles sont dotées d'une limite de temps, c'est-à-dire que si une application informatique n'est pas utilisée pendant un certain temps, le mot de passe doit être à nouveau saisi.

Le concept d'autorisation d'accès définit en outre de manière détaillée quels profils d'autorisation (rôles) peuvent exercer quelles fonctions et à quels champs de données il est possible d'accéder.

Les autorisations d'accès sont surveillées à l'aide de contrôles d'accès appropriés

Les employés de CPVAL ont accès aux locaux où les données sont traitées. Les tiers n'y ont accès que s'ils sont accompagnés par un employé de CPVAL. Cet accès des collaborateurs ou de tiers est limité au minimum nécessaire, tant du point de vue spatial que temporel.

Les autorisations d'accès sont surveillées à l'aide de contrôles d'accès appropriés.

4. Mesures pour assurer la sécurité des données

4.1. Mesures générales

Les mesures suivantes sont en place pour protéger les données personnelles contre la destruction non autorisée ou accidentelle, la perte accidentelle, les erreurs techniques, la falsification, le vol ou l'utilisation illégale et le traitement non autorisé :

- Sauvegardes des données
- Journalisation
- Gestion des identité, autorisations et accès
- Réseaux sécurisés
- Communication externe (e-mail, Internet) de données personnelles sensibles uniquement avec un chiffrement suffisant

L’ensemble des mesures techniques et organisationnelles sont celles mises en place par l’hébergeur, le service cantonal de l’informatique (SCI).

4.2. Confidentialité

Accès aux datacenter et locaux techniques : Protection contre l'accès non autorisé aux systèmes de traitement des données personnelles.

☒ Accès biométrique	☒ Locaux sous surveillance vidéo et sous alarme
☒ Règlement d'accès spécifique	☒ Inscription à l'accueil avec contrôle personnel
☒ Accès limité strictement selon le besoin	☒ Contrôle d'identité, journalisation de l'accès et accompagnement physique des tiers

Contrôle d'accès logique : Protection contre l'utilisation non autorisée des systèmes.

Postes de travail

☒ Accès par mot de passe ou biométrie	☒ Chiffrement des disques physiques
☒ Verrouillage automatique	☒ Système de protection des postes de travail

Accès distants

☒ VPN uniquement pour les postes de travail internes	☒ Autres accès distants au travers d'une authentification forte
☒ Accès des partenaires sur un système bastion après validation interne et authentification forte	

Contrôle d'accès applicatifs : interdiction de lecture, copie, modification ou suppression non autorisée au sein du système.

☒ Profils d'autorisation standard "need-to-know-basis"	☒ Processus d'autorisation standard
☒ Journalisation des accès	☒Stockage sécurisé des supports de stockage
☒ Examen périodique des autorisations accordées, notamment des comptes d'utilisateurs administratifs	☒ Réutilisation des supports de données dans le respect de la protection des données
☒ Élimination conforme à la protection des données des supports de données qui ne sont plus nécessaires	☒ Clear-Desk/Clear-Screen Policy

☒ Gestion des droits d'accès : L'Etat du Valais dispose d'un règlement et de possibilités techniques de surveillance des utilisateurs privilégiés, tels que B. *Administrateurs* qui ont accès aux données personnelles du client ou à l' *environnement informatique* dans lequel elles sont traitées.	☒ Sous-traitants : L'Etat du Valais veille à ce que tous ses sous-traitants soient soumis à une obligation légale de confidentialité.

Pseudonymisation : si cela est possible pour le traitement respectif des données personnelles, les principales caractéristiques d'identification des données personnelles sont supprimées lors du traitement respectif des données personnelles et stockées séparément.

☒Oui	☐Non

Schéma de classification des données : En raison d'obligations légales ou d'auto-évaluation (secrète/confidentielle/interne/publique).

☐Oui	☒Non, les données personnelles sont par défaut qualifiées de nature confidentielle

4.3. Intégrité des données[1]

Séparation des données

☒L'Etat du Valais assure une séparation stricte entre les données du client, les données de l'Etat du Valais et les données des autres clients de L'Etat du Valais, afin que les données personnelles du client ne soient pas mélangées avec d'autres données.

Contrôle de la divulgation : Aucune lecture, copie, modification ou suppression non autorisée lors du stockage, de la transmission électronique ou du transport.

☒Cryptage des supports de données	☒ Réseaux privés virtuels

Contrôle de saisie : Déterminer si et par qui des données personnelles ont été saisies, modifiées ou supprimées dans le cadre du traitement des systèmes de données personnelles.

☒journalisation des traitements

[1]Prévention de la destruction/destruction (involontaire), des dommages (involontaires), de la perte (involontaire), de l'altération (involontaire) des données personnelles.

4.4. Disponibilité et résilience

Contrôle de disponibilité : protection contre la destruction ou la perte accidentelle ou volontaire.

☒ Backup-Strategy (online/offline; on-site/off-site)	☒Alimentation électrique sans interruption (UPS, générateur diesel)
☒Protection contre le virus	☒Firewall
☒Canaux de signalement et plans d'urgence	☒Contrôles de sécurité au niveau de l'infrastructure et des applications
☒Concept de sauvegarde multi-niveaux avec externalisation cryptée des sauvegardes vers un centre de données de sauvegarde	☒Processus standard lors d'un changement/d'un départ d'employé
☒Surveillance de la sécurité : L'Etat du Valais garantit qu'il dispose d'un processus continu de surveillance de la sécurité pour détecter et corriger les menaces, les vulnérabilités et les alertes (SOC).	☒ L'Etat du Valais garantit que les *Backup* sont disponibles en temps opportun dans un format convertible et conventionnel à la demande du client.

4.5. Procédures d'examen, d'évaluation et d'évaluation périodiques

Gestion de la protection des données, y compris la formation régulière des employés.

☒Oui	☐Non

Gestion de la réponse aux incidents :

☒Oui	☐Non

Contrôle des sous-traitants : Aucun traitement de données personnelles sans instructions correspondantes du client.

☒Conception claire du contrat	☒Contrôles de suivi
☒Sélection rigoureuse des entrepreneurs	☒Obligation préalable à la condamnation

Development and Security Testing

☒ Différents systèmes sont testés sur une base continue à l'aide de tests d'intrusion.

5. Modalités d'exercice du droit d'accès et du droit d'obtenir ou de transférer des données

Les personnes concernées ont le droit d'exercer certains droits concernant leurs données personnelles. Ces droits comprennent :

- Obtenir des informations sur leurs propres données personnelles traitées par CPVAL ;
- Recevoir une copie de leurs données dans un format électronique couramment utilisé ;
- Demander la rectification de leurs données (si elles sont inexactes) ;
- De s'opposer au traitement de leurs données personnelles et
- De demander la limitation de leur traitement ou la suppression de leurs données personnelles (notamment s'il n'y a plus d'obligations légales de conservation).

5.1. Demande d'informations sur les données personnelles (« demande d'accès »)

Une demande d'informations sur des données personnelles (« demande d'accès ») est une demande émanant d'une personne concernée ou de son représentant légal pour accéder aux informations que CPVAL possède sur cette personne. La demande d'informations donne aux personnes concernées le droit de consulter leurs propres données personnelles et de demander des copies de ces données.

Une demande d'accès doit être faite par écrit. Les demandes verbales d'informations sur une personne ne constituent généralement pas une demande d'accès valable. Lorsqu'une demande formelle d'accès est faite oralement à un employé de CPVAL, il convient de demander conseil au DPO, qui examinera et approuvera toute demande d'accès aux données personnelles.

Une demande d'informations peut être effectuée de l'une des manières suivantes : par courrier ou par e-mail.

La personne concernée reçoit les informations nécessaires pour lui permettre de faire valoir ses droits au titre de la présente loi et pour assurer un traitement transparent des données. Dans tous les cas, les informations suivantes lui sont communiquées :

- L'identité et les coordonnées du responsable de traitement ;
- Les données personnelles traitées en tant que telles, c'est-à-dire une description des données détenues à leur sujet et, lorsque cela est autorisé et réalisable, une copie de ces données ;
- La finalité du traitement ;
- La durée de conservation des données personnelles ou, si cela n'est pas possible, les critères de détermination de cette durée ;
- Les informations disponibles sur l'origine des données personnelles, dans la mesure où elles n'ont pas été obtenues auprès de la personne concernée ;
- Le cas échéant, l'existence d'une décision individuelle automatisée et la logique sur laquelle se fonde la décision ;
- Le cas échéant, les destinataires ou les catégories de destinataires dont les données personnelles sont divulguées.
- Si les données personnelles sont divulguées à l'étranger, l'État ou l'organisme international et, le cas échéant, les garanties (par exemple les clauses types de protection des données) ou l'application d'une exception (par exemple le consentement de la personne concernée) doivent également être notifiés.

CPVAL doit répondre aux personnes concernées demandant l'accès à leurs données dans les 30 jours calendaires suivant la réception de la demande d'accès, sauf disposition contraire de la loi cantonale dans la mesure où elle y est soumise.

5.2. Exemption

En principe, aucune information n'est donnée concernant les informations suivantes :

- Données personnelles concernant d'autres personnes - Une demande d'informations peut porter sur des informations relatives à une ou plusieurs personnes autres que la personne concernée. En principe, aucune information n'est fournie sur ces données à moins que les personnes concernées ne consentent à la divulgation de leurs données.
- Demandes répétées - Si une réponse à une demande similaire ou identique concernant la même personne concernée a déjà été donnée précédemment dans un délai raisonnable et qu'il n'y a pas de changement significatif dans les données personnelles traitées concernant cette personne concernée, toute nouvelle demande soumise dans une période de six mois à compter de la demande initiale sera considérée comme une demande répétée et CPVAL ne fournira en principe pas de nouvelle copie des mêmes données.
- Informations accessibles au public – CPVAL n'est pas tenue de fournir des copies de documents qui sont déjà accessibles au public.
- Avis confidentiels ou données protégées par des droits d'auteur - CPVAL n'est pas tenue de transmettre des données personnelles sur une personne concernée sous la forme d'un avis confidentiel ou d'un avis protégé par des droits d'auteur.
- Documents privilégiés - Les informations privilégiées détenues par CPVAL n'ont pas besoin d'être divulguées en copie en réponse à une demande d'informations. Les informations privilégiées comprennent généralement tout document confidentiel (tel qu'une communication directe entre un client et son avocat) et préparé dans le but d'obtenir ou de fournir une assistance juridique.

Les raisons du refus doivent être clairement indiquées par écrit. Toute personne insatisfaite de la réponse à sa demande d'information a le droit de demander au conseiller à la protection des données de revoir le résultat.

Le DPO est chargé d'accorder aux assurés le droit de consulter leurs propres données. Il doit veiller à ce que les informations soient examinées dans le délai prescrit, afin de ne pas dépasser le délai de 30 jours calendaires. Cette personne obtient les données, fournit les informations et, le cas échéant, veille à leur rectification. La procédure d'exercice du droit d'information et de communication ou de transfert de données est également documentée dans une directive interne (directive sur la politique de confidentialité).

6. Entrée en vigueur et modifications des règles

La version 1.0 de ce règlement a été adoptée par le Conseil d'Administration en date du 22 novembre 2023 et entre en vigueur au 01.09.2023.

La version actuelle et une liste des versions précédentes sont répertoriées ici :

Version 1.0 du 1er septembre 2023 adoptée le 22.11.2023