Conditions contractuelles générales (CCG)

# Mise en œuvre de mesures de l’assurance-invalidité

1er septembre 2026

IV-Stelle Kanton Bern, Scheibenstrasse 70, 3001 Bern
T 058 219 71 11, www.ivbe.ch

Office AI Canton de Berne, Scheibenstrasse 70, 3001 Berne
T 058 219 71 11, www.aibe.ch

# Sommaire


Préambule ....4
1 Principes ....4
1.1 Bases légales ....4
1.2 Conditions contractuelles générales (CCG) ....4
1.3 Validité géographique du contrat ....4
1.4 Validité temporelle des conditions contractuelles générales ....4
1.5 Validité temporelle de la convention de prestations ....4
2 Définitions et abréviations ....4
2.1 Fournisseurs de prestations ....4
2.2 Office AI assignant ....4
2.3 Abréviations ....4
3 Droits et obligations ....5
3.1 Disponibilité temporelle des mesures ....5
3.2 Attribution des mandats ....5
3.3 Type de mise en œuvre des mesures ....5
3.4 Adaptation des mesures ....5
3.5 Obligation de renseigner en cas d'évolution défavorable de la mesure ....5
3.6 Arrêt anticipé de la mesure ....5
3.7 Contrôle de présence ....5
3.8 Stages externes ....5
3.9 Obligation d'enregistrement ....5
3.10 Rapports ....6
3.11 Prévention de la maltraitance et des violations de l'intégrité ....6
4 Modalités de décompte et de versement ....6
4.1 Nature et étendue de la rémunération ....6
4.2 Mois d'entrée et de sortie dans le cas des forfaits mensuels ....6
4.3 Forfaits horaires et journaliers ....6
4.4 Stage ....6
4.5 Courte interruption d'une mesure ....6
4.6 Interruption prolongée et cessation imprévue d'une mesure ....6
4.7 Mesure non débutée ....7
5 Facturation ....7
5.1 Factures individuelles ....7
5.2 Objet et teneur des factures ....7
6 Reporting ....7
7 Evaluation ....8

8 Confidentialité et protection des données ....8
8.1 Obligation de garder le secret ....8
8.2 Définition des informations confidentielles ....8
8.3 Traitement des données par le fournisseur de prestations ....8
8.4 Obligations des fournisseurs de prestations ....8
8.5 Publication légale ....8
8.6 Traitement des données des assurés à l'étranger ....9
8.7 Mesures de protection ....9
8.8 Obligation d'informer en cas d'incident ....9
8.9 Preuves et audits ....9
8.10 Restitution et suppression ....9
8.11 Sanctions ....10
9 Sous-traitance ....10
9.1 Recours à des sous-traitants ....10
9.2 Obligations en cas de recours à des sous-traitants ....10
10 Particularités ....10
10.1 Autorisations ....10
10.2 Protection des jeunes travailleurs ....10
10.3 Protection contre les accidents ....10
10.4 Responsabilité ....11
10.5 Taxe sur la valeur ajoutée ....11
10.6 Renseignements ....11
10.7 Communication relative à la cessation d’activité et aux changements personnels ....11
10.8 Procédure en cas de litiges ....11
11 Entrée en vigueur ....11
Annexe 1: Mesure technique et organisationelles (MTO) ....12
Annexe 2: Mémento Exigences relatives au concept de protection et de sécurité des données des fournisseurs de prestation ....14

# Préambule

L'Assurance-invalidité (AI) a pour but de réinsérer sur le marché primaire du travail les clientes et les clients (personnes assurées) présentant une atteinte à la santé, de manière individuelle et durable, en fonction des ressources. Lors des mesures qu'ils accomplissent sur mandat de l'Office AI assignant, les fournisseurs de prestations se basent sur cet objectif et donc sur les besoins du marché primaire du travail.

# 1 Principes

## 1.1 Bases légales

- Loi fédérale sur la partie générale du droit des assurances sociales (LPGA), RS 831.20
- Loi fédérale sur l'assurance-invalidité (LAI), RS 831.20
- Règlement sur l'assurance-invalidité (RAI), RS 831.201
- Circulaire sur les mesures de réadaptation d'ordre professionnel (CMRP)

## 1.2 Conditions contractuelles générales (CCG)

Conjointement avec la convention de prestations, les CCG forment le contrat. Elles règlent la collaboration entre les fournisseurs de prestations et les offices AI assignants, les modalités de décompte et de versement ainsi que l'évaluation du type et de la qualité des mesures, l'établissement des rapports et le reporting.

## 1.3 Validité géographique du contrat

La convention de prestations et les CCG sont valables pour tous les offices AI assignants (ch. 2.2).

## 1.4 Validité temporelle des conditions contractuelles générales

Lorsqu'une modification des CCG est nécessaire, l'AIBE informe les fournisseurs de prestations au plus tard trois mois à l'avance par écrit. En cas de résiliation du contrat par le fournisseur de prestations, les CCG précédentes restent valables jusqu'à la fin du contrat. En l'absence de résiliation, les nouvelles CCG s'appliquent à partir de la date de la modification communiquée.

## 1.5 Validité temporelle de la convention de prestations

La convention de prestations applicable à la date de l'exécution de la mesure s'applique.

# 2 Définitions et abréviations

## 2.1 Fournisseurs de prestations

Partenaires contractants qui exécutent des mesures sur mandat de l'office AI assignant.

## 2.2 Office AI assignant

Office AI qui confie l'exécution de mesures aux fournisseurs de prestations. Il peut s'agir de l'AIBE, mais aussi d'un autre office AI cantonal.

## 2.3 Abréviations

| | |
|---|---|
| CCG | Conditions contractuelles générales |
| CM | Case Manager, compétent en matière de collaboration avec les fournisseurs de prestations au niveau du cas |
| AI | Assurance-invalidité |

AIBE Office AI Canton de Berne, compétent pour la conclusion de la présente convention de prestations et l'assurance qualité

CdC Centrale de compensation, Genève

# 3 Droits et obligations

## 3.1 Disponibilité temporelle des mesures

Les fournisseurs de prestations proposent en principe les mesures toute l'année sans interruption. Demeurent réservées les exceptions expressément prévues dans la convention de prestations.

## 3.2 Attribution des mandats

L'office AI assignant confie aux fournisseurs de prestations la mise en œuvre des mesures convenues par contrat. Le CM octroie le mandat concret au moyen d'une prise en charge des coûts sur la base de la convention d'objectifs signée par toutes les parties impliquées. Il n'existe aucun droit à l'attribution de mandats.

## 3.3 Type de mise en œuvre des mesures

Conformément au mandat de l'office AI assignant, toutes les mesures sont réalisées de manière efficiente, adéquate et avec un bon niveau de qualité. Le type de mise en œuvre dépend de l'objectif inscrit dans le préambule.

## 3.4 Adaptation des mesures

Si les fournisseurs de prestations considèrent qu'une adaptation de la mesure ordonnée est nécessaire, p. ex. un changement de l'orientation de la formation, ils en discutent avec le CM. Sans l'assentiment exprès du CM, les fournisseurs de prestations ne procèdent à aucune adaptation.

## 3.5 Obligation de renseigner en cas d'évolution défavorable de la mesure

Si la mise en œuvre d'une mesure s'avère non judicieuse ou que l'atteinte des objectifs fixés semble menacée, les fournisseurs de prestations en avisent immédiatement le CM.

## 3.6 Arrêt anticipé de la mesure

Les fournisseurs de prestations n'ordonnent les arrêts anticipés de la mesure qu'en concertation avec le CM. Cela vaut également pour l'arrêt pour raisons disciplinaires.

## 3.7 Contrôle de présence

Pendant la durée des mesures, les fournisseurs de prestations enregistrent la présence des clientes / des clients. Ils avisent le CM par écrit des problèmes de santé qui menacent l'atteinte des objectifs fixés ainsi que des absences de plus de 3 jours.

## 3.8 Stages externes

Les fournisseurs de prestations avisent rapidement le CM des stages externes, en précisant leur début et leur fin.

## 3.9 Obligation d'enregistrement

Les fournisseurs de prestations consignent au fur et à mesure par écrit les observations concernant l'évolution et le comportement de la cliente / du client.

### 3.10 Rapports

Les fournisseurs de prestations communiquent les rapports au CM dans les délais. Ils respectent les prescriptions de l'AIBE lors de leur établissement. S'il s'avère qu'un rapport présente des lacunes ou n'a pas été établi comme convenu, le CM exige une correction par écrit. Il peut fixer un délai à cet effet.

### 3.11 Prévention de la maltraitance et des violations de l'intégrité

Les réglementations énoncées dans la Charte pour la prévention des abus sexuels, de la maltraitance et d'autres formes de violation de l'intégrité s'appliquent par analogie.

## 4 Modalités de décompte et de versement

### 4.1 Nature et étendue de la rémunération

La rémunération des prestations s'effectue au moyen de forfaits par cas, horaires, journaliers, hebdomadaires ou mensuels. Tous les coûts en relation avec la mesure sont ainsi réputés réglés (notamment école professionnelle, cours de soutien, etc.). Sont également inclus les coûts de la scolarité et des cours externes dans tous les domaines de formation et pour tous les niveaux de formation (p. ex. cours interentreprises).

Une facturation supplémentaire à la cliente / au client ou à des tiers est exclue. Les prestations supplémentaires (p. ex. hébergement le week-end) ne relèvent pas de cette protection tarifaire. Les fournisseurs de prestations en règlent le financement directement avec la cliente / le client ou avec les tiers.

### 4.2 Mois d'entrée et de sortie dans le cas des forfaits mensuels

Les mois d'entrée et de sortie sont remboursés au prorata temporis en cas de forfaits mensuels: le forfait mensuel est divisé par 30, et le quotient multiplié par la durée effective (jours civils) au cours du mois correspondant.

### 4.3 Forfaits horaires et journaliers

L'office AI assignant fixe le nombre maximal de journées ou d'heures. Les journées et heures excédentaires ne sont pas rétribuées. Seules les prestations effectivement fournies sont payées, sous réserve du ch. 4.7.3.

### 4.4 Stage

Le forfait mensuel convenu est réglé pendant au plus 3 mois par année de formation, pendant un stage sur le marché primaire du travail considéré comme partie intégrante du programme de formation. Le tarif prévu dans la convention de prestations pour un stage sur le marché primaire du travail s'applique ensuite. L'AI ne verse aucun paiement aux entreprises de stage.

### 4.5 Courte interruption d'une mesure

Quand une mesure est interrompue pendant au plus 30 jours civils pour des raisons qui échappent à l'influence des fournisseurs de prestations, les forfaits par cas, hebdomadaires et journaliers sont intégralement payés. Dans le cas des forfaits horaires et journaliers, les heures et journées non effectuées ne sont pas payées.

### 4.6 Interruption prolongée et cessation imprévue d'une mesure

**4.6.1** Lorsqu'une interruption dure plus de 30 jours ou qu'il est établi que la mesure ne pourra pas être poursuivie (arrêt), les modalités décrites ci-après s'appliquent. Il importe peu que la mesure soit poursuivie à une date ultérieure ou non.

**4.6.2** Forfait mensuel: une rémunération est accordée jusqu'à la fin du mois suivant l'arrêt ou l'interruption,

mais au plus tard jusqu'à la fin planifiée de la mesure.

**4.6.3** Forfait hebdomadaire: le forfait hebdomadaire complet est payé pour la semaine où la mesure a été arrêtée ou interrompue et la semaine suivante.

**4.6.4** Forfaits par cas: une rémunération complète est accordée lorsque la mesure est arrêtée ou interrompue le 10e jour civil à compter du début ou ultérieurement. La moitié du forfait est payée dans tous les autres cas.

**4.6.5** Forfaits horaires et journaliers: les heures et les journées non effectuées ne sont pas payées.

### 4.7 Mesure non débutée

**4.7.1** Lorsqu'une cliente / un client ne se présente pas à une mesure accordée, 25% des forfaits horaires et journaliers sont payés. Dans le cas des forfaits par cas, le paiement correspond à 25% du forfait.

**4.7.2** Les modalités ci-dessus s'appliquent également lorsqu'une mesure accordée est annulée 5 jours ouvrables avant sa date fixée ou ultérieurement. Si l'annulation intervient plus tôt, il n'y a pas de paiement.

**4.7.3** En cas d'annulation d'un rendez-vous dans le cadre d'une mesure accordée 24 heures avant son début ou plus tard ou en cas de non-présentation de la cliente / du client, les forfaits horaires sont payés en totalité et les forfaits journaliers à 50%.

**4.7.4** Seules les mesures pour lesquelles une prise en charge des coûts écrite selon le ch. 3.2 a été confirmée sont considérées comme des mesures accordées.

## 5 Facturation

### 5.1 Factures individuelles

Les fournisseurs de prestations facturent les mesures individuellement par cliente / client. Les factures collectives pour plusieurs clientes / clients ensemble sont interdites. Les fournisseurs de prestations adressent leurs factures par voie électronique à la CdC. Ils communiquent une copie à la cliente / au client.

### 5.2 Objet et teneur des factures

Les fournisseurs de prestations facturent exclusivement les prestations fournies. Aucun paiement d'avance n'est possible. Les factures contiennent les informations suivantes:

- numéro GLN (Global Location Number);
- adresse de la personne ou de l'institution qui établit la facture avec l'IBAN (numéro international de compte bancaire);
- adresse et numéro d'assuré (numéro AVS) de la cliente / du client;
- numéro de la communication ou de la décision et adresse de l'office AI assignant;
- type de mesure, avec indication de la durée (début et fin) et de la position tarifaire;
- tarif de la mesure, nombre d'unités tarifaires et montant de la facture.

## 6 Reporting

Les fournisseurs de prestations remettent chaque année à l'AIBE les documents suivants jusqu'au 31 mai au plus tard:

- comptes annuels approuvés (bilan et compte de résultat) avec rapport de révision. Dans son appréciation, le rapport de révision confirme que les comptes annuels de l'exercice écoulé ont été établis conformément à la législation suisse.
- autorisation d'exploiter actuelle et description du système de gestion de la qualité (certificat actuel);
- rapport annuel officiel.

Les fournisseurs de prestations remettent chaque année à l'AIBE la statistique des mesures convenues par contrat et fournies d'un point de vue qualitatif et quantitatif (selon le modèle de reporting):

- jusqu'au 31 août pour les mesures Formations et Logement
- jusqu'au 31 janvier pour toutes les autres mesures

# 7 Evaluation

L'AIBE évalue régulièrement ou sur la base d'événements particuliers le respect des bases contractuelles ainsi que la qualité et le résultat des mesures exécutées. Elle consigne les résultats par écrit et en discute avec le fournisseurs de prestations. L'AIBE tient compte de manière appropriée des feed-backs des autres offices AI assignants.

# 8 Confidentialité et protection des données

## 8.1 Obligation de garder le secret

Le fournisseur de prestations s'engage à préserver la confidentialité de toutes les informations confidentielles fournies par l'office AI qui le mandate (« l'office AI »). Cela vaut également pour son personnel, ses mandataires et ses sous-traitants. Aucune mesure susceptible de compromettre la confidentialité ne doit être prise.

## 8.2 Définition des informations confidentielles

Les informations confidentielles sont l'ensemble des données, des matériels et des informations, quelle que soit leur forme (numérique, papier, etc.). Il s'agit notamment des données personnelles des clientes / des clients et du personnel, ainsi que des informations relatives à l'organisation, aux finances, aux stratégies et aux systèmes de l'office AI.

## 8.3 Traitement des données par le fournisseur de prestations

La conclusion de la convention délègue au fournisseur de prestations une tâche de droit public. Il devient ainsi un organe cantonal et est soumis à l'obligation de garder le secret prévu à l'art. 33 de la loi fédérale sur la partie générale du droit des assurances sociales et au secret de fonction prévu à l'art. 320 du code pénal. Les conséquences pénales en cas de violation sont expressément mentionnées. Le fournisseur de prestations traite les données personnelles dans le cadre de la fourniture de ses prestations sous sa propre responsabilité et non en tant qu'auxiliaire de l'office AI.

## 8.4 Obligations des fournisseurs de prestations

a) Les informations confidentielles ne doivent être utilisées que pour les tâches convenues et uniquement dans la mesure nécessaire. Elles ne peuvent pas être copiées ou distribuées d'une quelconque autre manière sans autorisation.

b) Le personnel du fournisseur de prestations n'a accès qu'aux informations confidentielles nécessaires à l'accomplissement de ses tâches (principe du « besoin d'en connaître ») et doit être tenu à la confidentialité.

c) La transmission d'informations confidentielles à des tiers (p. ex. à des consultants externes) est soumise aux dispositions légales en matière de confidentialité mentionnées ci-dessus au ch. 8.3 « Traitement des données par le fournisseur de prestations ». La transmission d'informations confidentielles à des sous-traitants n'est autorisée qu'en conformité avec le ch. 9 Sous-traitance. Les tiers et les sous-traitants doivent respecter des règles de confidentialité et de protection des données équivalentes aux dispositions du présent contrat.

## 8.5 Publication légale

Si le fournisseur de prestations est tenu de divulguer des informations confidentielles en vertu d'une loi ou

d'une décision judiciaire, il en informe immédiatement l'office AI au préalable, dans la mesure où cela est légalement autorisé. Seules les données strictement nécessaires sont transmises.

### 8.6 Traitement des données clients à l'étranger

En ce qui concerne le traitement des données personnelles des clientes / des clients en dehors de la Suisse, les dispositions correspondantes de la directive de l'Office fédéral des assurances sociales sur les exigences en matière de sécurité de l'information et de protection des données (D-SIPD) s'appliquent. Les dispositions de la D-SIPD s'appliquent même si l'étranger offre une protection des données adéquate et s'appliquent également aux prestataires de services informatiques ayant accès aux données à l'étranger.

### 8.7 Mesures de protection

Le fournisseur de prestations confirme avoir pris des mesures techniques et juridiques pour protéger les données. Ceux-ci sont décrits en détail dans l'annexe 1.

### 8.8 Obligation d'informer en cas d'incident

Le fournisseur de prestations informe immédiatement l'office AI de toute violation de la protection des données ou de toute faille de sécurité. Il doit en outre signaler immédiatement s'il n'est plus en mesure de remplir les obligations qui lui incombent en vertu de la présente convention.

### 8.9 Preuves et audits

En signant la convention de prestations, le fournisseur de prestations confirme qu'il dispose d'un concept de protection et de sécurité des données qui satisfait a minima aux exigences du mémento « Concept de protection et de sécurité des données » (annexe 2).

Le fournisseur de prestations soumet spontanément (obligation de soumission) son concept de protection et de sécurité des données à l'office AI afin que celui-ci puisse vérifier sa conformité avec le mémento « Exigences relatives au concept de protection et de sécurité des données des fournisseurs de prestations ». La mise en œuvre du concept de protection et de sécurité des données est vérifiée par l'office AI, le cas échéant, dans le cadre des entretiens d'assurance-qualité périodiques.

Les certificats (tels que ISO 27001) ou les rapports d'audit doivent être envoyés spontanément à l'office AI. L'office AI peut en outre, après préavis, effectuer ou faire effectuer un audit (contrôle sur place) une fois par an. Les frais sont à la charge de chaque partie.

En cas de soupçon concret de violation de la protection ou de la sécurité des données, ou s'il est prouvé qu'une telle violation a eu lieu, l'office AI est en outre habilité à effectuer, en dehors du cycle régulier des entretiens d'assurance-qualité, un audit distinct axé sur la protection des données auprès du fournisseur de prestations, ou à faire procéder à un tel audit par un service spécialisé externe ou par l'autorité cantonale de surveillance de la protection des données.

Le fournisseur de prestations est tenu de donner à l'office AI ou à l'organisme externe spécialisé accès à toutes les informations nécessaires à la réalisation des audits.

Le fournisseur de prestations est en outre tenu, à la demande de l'office AI, de réaliser une auto-évaluation avant chaque entretien d'assurance-qualité à l'aide de la liste de contrôle fournie par l'office AI et de communiquer au préalable le résultat à l'office AI.

### 8.10 Restitution et suppression

Les données ne sont conservées que pendant la durée nécessaire à l'exécution du mandat. À la fin du contrat, toutes les informations sont restituées ou supprimées, à moins qu'une obligation légale de conservation ne s'applique. La suppression doit être confirmée à l'office AI. Les données restantes restent soumises à la confidentialité conformément aux dispositions du présent contrat.

### 8.11 Sanctions

En cas d'une violation des dispositions du présent chiffre Confidentialité et protection des données, le fournisseur de prestations peut être passible d'une peine pouvant atteindre CHF 10'000.- en fonction de la gravité de l'incident, à moins qu'il ne prouve qu'aucune faute ne lui est imputable. Cette peine est due même sans preuve d'un dommage. Cela n'affecte en rien les autres demandes de dommages-intérêts, la peine étant, le cas échéant, imputée sur les dommages-intérêts à verser.

En outre, tout manquement grave aux obligations prévues au présent chiffre de la part du fournisseur de prestations peut entraîner la résiliation extraordinaire de la convention de prestations par l'office AI.

## 9 Sous-traitance

### 9.1 Recours à des sous-traitants

Le fournisseur de prestations doit fondamentalement exécuter lui-même le mandat. Le recours à des sous-traitants (y c. des prestataires informatiques ayant accès aux données) est autorisé, à condition que le fournisseur de prestations informe l'office AI par écrit, au moins 30 jours à l'avance, de la sous-traitance prévue. L'office AI a le droit de s'y opposer dans ce délai pour un motif grave (droit de veto). Il y a motif grave notamment dans les cas suivants:

- il existe des doutes quant aux compétences ou à la fiabilité du sous-traitant;
- le respect des exigences en matière de protection des données n'est pas garanti sans faille;
- les intérêts du mandant sont mis en danger par l'office AI.

En l'absence de contestation dans ce délai, l'autorisation est réputée accordée à ce sous-traitant spécifique.

### 9.2 Obligations en cas de recours à des sous-traitants

Les services doivent fondamentalement être fournis en Suisse. Les prestations provenant de l'étranger doivent être justifiées et indiquées. L'office AI peut s'y opposer à tout moment. Il est expressément fait référence au (ch. 8.6) *Interdiction de traiter des données d'assurés à l'étranger*. Le fournisseur de prestations est tenu d'imposer par écrit aux sous-traitants toutes les obligations découlant de la présente convention (en particulier la confidentialité, la protection des données et les droits d'audit). Il est responsable du comportement du sous-traitant comme si c'était le sien.

## 10 Particularités

### 10.1 Autorisations

Les fournisseurs de prestations possèdent les autorisations nécessaires pour la conduite de leur entreprise et pour la réalisation des mesures proposées.

### 10.2 Protection des jeunes travailleurs

Les fournisseurs de prestations s'engagent à garantir la protection des jeunes travailleurs lors de toutes les mesures réalisées par eux-mêmes. Si les mesures incluent des interventions sur le marché primaire du travail, les fournisseurs de prestations doivent également garantir la protection des jeunes travailleurs lors de ces interventions.

### 10.3 Protection contre les accidents

Les fournisseurs de prestations accomplissent les tâches comme employeur selon les art. 91 ss de la loi fédérale sur l'assurance-accidents (LAA) pour les personnes assujetties à l'assurance obligatoire selon l'art. 1*a*, al. 1, let. a LAA.

### 10.4 Responsabilité

L'AI n'est pas responsable des dommages que la cliente / le client occasionne au fournisseurs de prestations dans le cadre d'une mesure. Les fournisseurs de prestations sont responsables des dommages que la cliente / le client occasionne à des tiers dans le cadre d'une mesure, conformément à la responsabilité de l'employeur selon l'art. 55 du Code des obligations (CO). Ils assurent ce risque dans le cadre d'une assurance responsabilité civile d'entreprise correspondante.

### 10.5 Taxe sur la valeur ajoutée

Les fournisseurs de prestations sont responsables du respect des prescriptions en vigueur concernant la TVA ainsi que de la mise en œuvre de mesures relatives à l'exonération fiscale.

### 10.6 Renseignements

Les fournisseurs de prestations fournissent en tout temps à l'AIBE tous les renseignements importants pour l'exécution du contrat. Sur demande, ils lui accordent un droit de regard sur l'exploitation, la comptabilité et les documents afférents.

### 10.7 Communication relative à la cessation d'activité et aux changements personnels

Les fournisseurs de prestations informent l'AIBE dès que possible par écrit d'une cessation prévue de leur activité. L'information inclut des indications relatives aux clientes / clients concernées par la cessation de l'activité.

Les fournisseurs de prestations déclarent à l'AIBE les changements de personnel importants en lien direct avec la réalisation des mesures.

### 10.8 Procédure en cas de litiges

Les fournisseurs de prestations et l'AIBE tentent de résoudre les différends à l'amiable dans le cadre de négociations. En cas d'échec, la procédure visée à l'art. 27$^{bis}$ al. 1 LAI s'applique. Est compétent le tribunal arbitral du canton dans lequel le fournisseur de prestations a une installation permanente ou exerce sa profession (art. 27$^{bis}$ al. 2 LAI).

## 11 Entrée en vigueur

Les présentes CCG entrent en vigueur le 1$^{er}$ septembre 2026. Veuillez noter que les nouvelles conditions contractuelles au 01.09.2026 remplacent toutes les versions précédentes.

## Annexe 1: Mesures techniques et organisationnelles (MTO)

Cette annexe décrit les mesures mises en œuvre par le fournisseur de prestations afin de garantir la confidentialité, l'intégrité et la disponibilité des informations confidentielles ainsi que la protection des données clients et des autres données personnelles.

*[Commentaire: Les mesures doivent être adaptées à chaque fois aux circonstances concrètes.]*

## 1. Confidentialité

**1.1 Contrôle d'entrée:** mesures visant à interdire aux personnes non autorisées l'accès physique aux installations de traitement des données:

- Sécurisation des locaux commerciaux par des serrures de porte et des systèmes de contrôle d'accès électroniques (p. ex. des cartes à puce).
- Distribution réglementée et protocolée de clés/badges.
- Séparation spatiale claire entre les zones de traitement internes et les zones de visite accessibles au public.
- Réglementation obligatoire pour les visiteurs (inscription, accompagnement par le personnel).

**1.2 Contrôle d'accès:** mesures visant à empêcher que les systèmes de traitement des données ne soient utilisés par des personnes non autorisées:

- Utilisation de comptes d'utilisateurs personnels (pas de logins collectifs).
- Directives strictes en matière de mots de passe (longueur minimale, caractères spéciaux, complexité)
- Utilisation de méthodes de cryptage modernes pour les identifiants et les mots de passe.
- Blocage automatique des sessions en cas d'inactivité ou de saisie répétée d'un mot de passe erroné.
- Gestion centralisée du cycle de vie des utilisateurs (création, modification, suppression).
- Utilisation de pare-feu et d'un logiciel antivirus toujours à jour.

**1.3 Contrôle d'accès aux données:** mesures visant à garantir que les personnes autorisées n'accèdent qu'aux données de leur niveau:

- Concept d'autorisation basé sur le principe « Besoin d’en connaître » ainsi que sur des profils basés sur les rôles.
- Authentification obligatoire à deux facteurs (2FA) pour les systèmes critiques et l'accès à distance.
- Enregistrement complet des procédures d'inscription ainsi que de l'utilisation, de la modification et de la suppression des données à des fins de traçabilité.

**1.4 Contrôle de la séparation:** mesures visant à traiter séparément les données ayant des finalités différentes:

- Séparation logique et/ou physique des bases de données clients.
- Séparation des environnements système (développement, test, production).
- Séparation des fonctions grâce à des droits d'accès différenciés.

**1.5 Contrôle de la transmission:** mesures de protection des données lors de leur transmission, de leur transport et de leur stockage:

- Cryptage de la transmission des données au moyen d'un VPN (connexion tunnel) et de protocoles modernes (TLS).
- Cryptage obligatoire des courriels dont le contenu doit être protégé.
- Cryptage complet des supports de données (ordinateurs portables, supports mobiles).
- Réglementations relatives au transport physique sécurisé des supports de données.
- Procédures réglementées pour la destruction sécurisée des supports de données (p. ex. déchiquetage selon la norme DIN).

## 2. Contrôle de la saisie

Mesures de contrôle a posteriori du traitement des données:

- Enregistrement systématique de l'introduction, de la modification et de la suppression des données personnelles.
- Utilisation d'un système de gestion des documents pour le contrôle des versions.
- Archivage des données de protocole avec protection contre les révisions pour la traçabilité administrative.

## 3. Disponibilité et intégrité

Mesures de protection contre la perte, contre la destruction et pour la récupérabilité:

- Concept de sauvegarde: sauvegardes régulières et automatisées (en continu avec des points de contrôle); mise en miroir des données dans un centre de données séparé et géographiquement distinct (à l'intérieur de la Suisse).
- Procédures de récupération réglementées pour une reprise rapide des activités.
- Plans d'urgence établis et procédures de notification définies en cas d'incidents de sécurité.
- Gestion des correctifs: cycle défini pour l'installation régulière de mises à jour de sécurité pour les systèmes d'exploitation et les applications.

## 4. Procédure de contrôle régulier (gouvernance)

Mesures d'évaluation de l'efficacité des MTO:

- Gestion établie de la protection des données pour le contrôle de la conformité.
- Sensibilisation et formation régulières des collaborateurs à l'utilisation des données.
- Protection des données par défaut: utilisation de paramètres par défaut favorables à la protection des données dans tous les systèmes.
- Gestion structurée des incidents pour documenter et réagir aux événements de sécurité.

## 5. Contrôle des sous-traitants

Mesures visant à garantir le niveau de protection des sous-traitants:

- Choix minutieux des sous-traitants, comme les partenaires informatiques (p. ex. l'hébergement).
- Conclusion d'accords écrits garantissant le respect de MTO équivalentes.
- Surveillance et instruction régulières des sous-traitants.

## Annexe 2: Mémento Exigences relatives au concept de protection et de sécurité des données des fournisseurs de prestations

Le présent mémento donne aux fournisseurs de prestations un aperçu des contenus possibles d'un concept de protection et de sécurité des données pour les fournisseurs de prestations.

Remarque: ce mémento a été formulé dans une optique nationale. Les lois cantonales sur la protection des données sont toutefois pertinentes dans les cas individuels. Ce mémento n'a donc pas la prétention d'être exhaustif, ce qui est précisé dans le document en question.

| Thème | Contenu | Indications pour la mise en œuvre |
|---|---|---|
| **Gouvernance** | Champ d'application du concept | Si le concept de protection des données ne s'applique qu'à certains départements, services ou domaines, il convient de le préciser. |
| | Bases légales et autres dispositions contraignantes | Le fournisseur de prestations se voit déléguer une tâche publique, raison pour laquelle il agit en tant qu'organe cantonal dans l'exécution du contrat.<br><br>Il convient de clarifier quelle loi cantonale sur la protection des données est applicable. Si le fournisseur de prestations reçoit des mandats de plusieurs offices AI, plusieurs lois cantonales sur la protection des données peuvent s'appliquer.<br><br>Les bases légales spéciales applicables qu'il y a lieu de respecter lors du traitement de données doivent être énumérées (p. ex. LAI, RAI, etc.).<br><br>Il faut tenir compte du fait que le secret de fonction (art. 320 CP) et l'obligation de garder le secret prévue par le droit des assurances sociales (art. 33 LPGA) s'appliquent.<br><br>Les directives de l'Office fédéral des assurances sociales qui ont des répercussions directes ou indirectes sur l'activité du fournisseur de prestations doivent également être prises en compte (p. ex. Directive sur les exigences en matière de sécurité de l'information et de protection des données des systèmes d'information des organes d'exécution du 1er pilier / des allocations familiales [D-SIPD] et Directive sur la gestion, la conservation, l'archivage et la destruction des documents dans les domaines AVS/AI/APG/PC/Ptra/AFamAgr/AFam [DGD]). |
| **Responsabilité** | Responsabilité du respect des obligations légales et contractuelles dans le domaine de la protection et de la sécurité des données (y c. les obligations légales de garder le secret) | La responsabilité du respect de la protection et de la sécurité des données ainsi que du respect des obligations légales de garder le secret doit être réglée à tous les niveaux de l'entreprise.<br><br>Les rôles possibles auxquels une responsabilité concrète est attribuée sont énumérés ci-après à titre d'exemple:<br><br>– Conseil d'administration<br>– Direction<br>– Conseiller·ère à la protection des données ou délégué·e à la protection des données |

| Thème | Contenu | Indications pour la mise en œuvre |
|---|---|---|
| | | – Responsable de la sécurité de l'information<br>– Supérieur·e hiérarchique<br>– Collaborateurs·trices<br>Il convient de désigner une personne de contact pour les questions relatives à la protection des données. |
| **Obligations en matière de documentation** | Preuve de la conformité aux exigences légales | Exemples (si la loi le prévoit)<br>– Répertoires de traitement / registres des fichiers de données<br>– Études d'impact sur la protection des données<br>– Contrôle préalable auprès de l'autorité cantonale de surveillance de la protection des données<br>– Documentation des incidents liés à la sécurité des données, y compris la notification à l'autorité de surveillance |
| **Principes de traitement** | Principes à respecter lors du traitement de données et d'informations reçues et/ou produites par l'institution elle-même dans le cadre de l'exécution de la convention de prestations | Exemples:<br>– Légalité, principe de légalité: les données relatives aux clientes / clients ne peuvent être traitées que si cela est nécessaire et approprié pour l'exécution de la tâche publique confiée.<br>– Affectation à un but précis: les données des clientes / clients ne peuvent être traitées que pour l'exécution de la convention de prestations. Le traitement à d'autres fins est interdit.<br>– Proportionnalité ou minimisation des données, y compris la suppression des données<br>– Confidentialité, y compris obligations légales de garder le secret<br>– Sécurité des données, y compris procédure en cas de violation de la sécurité des données |
| **Droits des personnes concernées et obligations d'information** | Devoir d'information<br>Droits d'accès, de rectification, de blocage et de suppression | Les clientes / clients doivent être informées du traitement des données qui les concernent (p. ex. dans une déclaration relative à la protection des données ou d'une autre manière appropriée).<br>Il convient de régler la manière dont il est garanti que les demandes correspondantes des clientes / clients sont traitées conformément aux dispositions légales et dans les éventuels délais impartis. |
| **Recours à des sous-traitants** | Externalisation du traitement des données à des sous-traitants<br>Lieu de traitement des données | Contrats avec les sous-traitants<br>Interdiction du traitement des données des assurés à l'étranger (DGD et D-SIPD) |

| | | |
|---|---|---|
| **Sécurité des données, y compris la gestion des violations de la sécurité des données** | Mesures techniques et organisationnelles (MTO) pour la protection de la confidentialité, de l'intégrité et de la disponibilité des données (voir annexe V Modifications des CGC pour plus d'informations)<br><br>Procédure en cas de violation de la sécurité des données | Exemples de MTO:<br>– Octroi restrictif des droits d'accès<br>– Mesures physiques telles que le contrôle d'accès au bâtiment et/ou aux locaux<br>– Mesures techniques telles que protection antivirus, pare-feu, etc.<br><br>La journalisation (qui fait partie des MTO):<br><br>Dans la mesure où la loi cantonale sur la protection des données l'exige, il convient de procéder comme suit:<br>– Journaux système: y est consigné qui a consulté quelles données, quand et quelle action (lecture, modification, suppression, copie) a été effectuée.<br>– Processus de contrôle: il existe un processus interne qui définit qui vérifie ces journaux pour détecter les abus et à quel moment il le fait.<br><br>Violation de la sécurité des données:<br>– Détection des violations de la sécurité des données<br>– Compétences internes<br>– Mesures pour remédier à la situation<br>– Annonce à l'autorité cantonale de protection des données (si la loi l'exige)<br>– Obligation d'information selon le ch. 10.8 CGC |
| **Formation et sensibilisation** | Concept de formation | Formation et sensibilisation à la protection et à la sécurité des données |
| **Contrôle** | Contrôle interne du traitement de données<br><br>Contrôle des sous-traitants | Compétences<br><br>Planification<br>– Basé sur les risques, avec une attention particulière portée aux risques des personnes concernées |
| **Tolérance et participation aux audits** | Droit d'audit de l'office AI compétent ainsi que, le cas échéant, de l'autorité cantonale de surveillance de la protection des données et de l'Office fédéral des assurances sociales (OFAS) | Réglementation des compétences et des responsabilités en cas d'audits externes<br><br>Formation des collaborateurs·trices |