Annexe IV | Mémento : Instruction des fournisseurs de prestations

Le présent mémento, établi conformément au ch. 6.3 de la recommandation de la COAI, sert de guide pour garantir le respect des exigences en matière de protection des données et de sécurité de l'information dans le cadre de la mise en œuvre des mesures de l'assurance-invalidité confiée aux fournisseurs de prestations.

Le non-respect des exigences peut entraîner des audits extraordinaires et des conséquences contractuelles (notamment suspension des attributions de mandat, résiliation extraordinaire).

1. Fournisseur de prestations en tant qu'organe de droit public

L'exécution d'une mesure de l'assurance-invalidité est une tâche de droit public. Dans ce contexte, chaque fournisseur de prestations devient un « organe responsable » ou une autorité.

2. Législation applicable en matière de protection des données

Le fournisseur de prestations est ainsi soumis à la loi cantonale sur la protection des données, qui s'applique à l'office AI qui le mandate. Il traite les données personnelles pour la fourniture de ses prestations sous sa **propre responsabilité** et non en tant qu'auxiliaire de l'office AI qui le mandate. C'est pourquoi il doit s'assurer lui-même qu'il respecte la législation cantonale en matière de protection des données.

Ce mémento a été formulé dans une optique nationale. Les lois cantonales sur la protection des données peuvent, dans certains cas, s'écarter des exigences mentionnées dans le présent document. Ainsi, ce mémento n'a pas la prétention d'être exhaustive.

3. Obligations légales de garder le secret

En tant qu'organe public, le fournisseur de prestations est soumis à l'obligation de garder le secret en vertu de l'art. 33 de la loi fédérale sur la partie générale du droit des assurances sociales et au secret de fonction en vertu de l'art. 320 du code pénal.

Ces dispositions interdisent la **divulgation non autorisée** de données relatives aux assurés à des **personnes non habilitées**, telles que d'autres autorités, des hôpitaux, des journalistes ou des cybercriminels. Nous attirons expressément l'attention sur les éventuelles conséquences pénales de toute violation.

4. Traitement des données liées au contrat

Les tâches de droit public déléguées dans le cadre de la convention de prestations doivent être exécutées personnellement par le fournisseur de prestations ; leur transfert à des tiers n'est autorisé qu'à titre exceptionnel (cf. ch. 5.1.3 des CGC).

Le recours à des fournisseurs de prestations pour des activités de soutien, tels que des prestataires informatiques (p. ex. des fournisseurs de services cloud), est autorisé pour autant que (i) les prescriptions des CGC (voir annexe V de la recommandation de la COAI) soient respectées et que (ii) les prestataires ne traitent pas de données d’assurés à l’étranger.

5. Obligations des fournisseurs de prestations

En signant la convention de prestations, les fournisseurs de prestations confirment ce qui suit :

- **Concept de protection et de sécurité des données :** Il doit exister un concept écrit répondant aux exigences du mémento figurant à l'annexe III de la recommandation de la COAI.

- **Intégralité :** Le concept doit couvrir les mesures techniques (informatique) et organisationnelles (processus, formation).
- **Obligation de fournir des preuves :** Il faut garder les preuves à portée de main (p. ex. des journaux de données supprimées, des listes de droits d'accès, des preuves de cryptage).
- **Disponibilité pour des audits ad hoc :** En cas de soupçon fondé de violation de données, l'autorité de référence peut à tout moment procéder à un audit extraordinaire (interne ou externe) (voir ch. 1.9 des CGC).

6. Obligations spécifiques

- **Obligation de déclaration :** Le concept de protection et de sécurité des données doit être remis sans demande à l'organe de gestion du contrat.
- **Auto-audit :** Ils sont tenus d'effectuer un auto-audit selon la liste de contrôle Auto-audit pour les fournisseurs de prestations avant l'entretien qualité qui a lieu régulièrement.
- **Rapport :** Le résultat de l'auto-audit doit être communiqué à l'unité de gestion des contrats 14 jours calendaires avant l'entretien qualité.
- **Obligation d'information :** Les incidents liés à la protection et à la sécurité des données doivent en outre être annoncés immédiatement à l'organe de gestion des contrats (chiffre 1.8 CgC).

7. Remarques sur le risque d'audit ad hoc

Un « **soupçon concret »**, qui déclenche un audit extraordinaire, peut résulter d’éléments comme ceux-ci :

- Déclarations des personnes concernées (assurés)
- Irrégularités dans la communication
- Lacunes manifestes mises en évidence par les auto-évaluations