OCAS Genève

Liste de contrôle pour l'auto-évaluation des fournisseurs de prestations

Objet : Preuve du respect des obligations découlant de la législation sur la protection des données et du droit des assurances sociales dans le cadre de l'exécution de la convention de prestations du

Société :

Période de contrôle :

Date de l'évaluation :

Évaluateur :

Cette liste de contrôle s'adresse aux fournisseurs de prestations et sert d'attestation d'auto-évaluation.

En remettant la liste de contrôle remplie, les fournisseurs de prestations confirment de manière juridiquement contraignante l'exactitude des informations fournies dans la liste de contrôle :

1. Documentation et bases

☐ **Actualité :** Il existe un concept écrit de protection des données qui reflète l'état des dispositions légales applicables en matière de protection des données.

☐ **Conformité :** Les exigences spécifiques du *mémento Exigences relatives au concept de protection et de sécurité des données des fournisseurs de prestations* ont été intégrées dans le concept.

☐ **Responsabilité :** Une personne responsable compétente en matière de protection des données a été désignée et ses coordonnées sont à jour.

Notes et commentaires :

2. Légalité

☐ **Aucune violation de droits :** Au cours de la période sous contrôle, il n'y a pas eu de procédure devant un tribunal ou une autorité dans laquelle il a été constaté une violation des obligations applicables en matière de protection des données (y c. la sécurité des données) et / ou une violation du secret de fonction et/ou de l'obligation de garder le secret prévu par le droit des assurances sociales et/ou du secret professionnel.

☐ **Aucune procédure en cours :** Au moment de la remise du rapport d'auto-évaluation, il n'existait aucune procédure ouverte devant un tribunal ou une autorité alléguant une violation des obligations applicables en matière de protection des données (y c. la sécurité des données) et/ou une violation du secret de fonction et/ou de l'obligation de garder le secret prévu par le droit des assurances sociales et/ou du secret professionnel.

☐ **Droits des personnes concernées :** Au cours de la période sous contrôle, [...] demandes ont été reçues de la part de personnes concernées, dans lesquelles elles faisaient valoir leurs droits d'accès, de rectification, de suppression ou de blocage en vertu de la législation sur la protection des données. Toutes les demandes ont reçu une réponse dans le délai légal.

☐ **Étranger :** Aucune donnée relative aux assurés n'est traitée à l'étranger.

☐ **Aucune violation de la confidentialité et de la sécurité des données :** Aucune violation de la protection et/ou de la sécurité des données n'a eu lieu au cours de la période sous contrôle.

Notes et commentaires :

3. Mesures techniques et organisationnelles (MTO)

☐ **Confidentialité :** Les mesures convenues par contrat sont respectées et correspondent aux normes de sécurité actuelles.

☐ **Contrôles de la saisie :** Les mesures convenues par contrat sont respectées et correspondent aux normes de sécurité actuelles.

☐ **Disponibilité, intégrité et résistance :** Les mesures convenues par contrat sont respectées et correspondent aux normes de sécurité actuelles.

☐ **Vérification :** Les mesures convenues par contrat sont respectées, répondent aux normes de sécurité actuelles et sont contrôlées et testées à intervalles appropriés.

Notes et commentaires :

4. Obligation d'établir un procès-verbal

☐ **Non applicable :** Non requis selon la loi cantonale sur la protection des données applicable.

☐ **Journaux système :** Le logiciel utilisé (p. ex. gestion des données des assurés) établit automatiquement un protocole d'accès aux données.

☐ **Journaux administrateur :** Les actions des personnes disposant de droits informatiques spéciaux (administrateurs) sont consignées.

☐ **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.

☐ **Concept de suppression des journaux :** Les protocoles sont automatiquement supprimés après le délai de garde.

Notes et commentaires :

5. Sous-traitants

☐ **Contrôle du contrat :** Tous les sous-traitants qui ont accès aux données personnelles ont signé des contrats de traitement des données liées au contrat.

☐ **Contrôle :** Les principaux prestataires de services sont soumis à des contrôles aléatoires portant sur leurs engagements en matière de sécurité.

Notes et commentaires :

6. Gestion des incidents

☐ **Chaîne de déclaration :** Les collaborateurs·trices savent à qui il faut immédiatement signaler en interne une violation (présumée) des données.

☐ **Processus de déclaration :** Il est garanti qu'une communication à l'office AI, aux autorités et aux personnes concernées peut être effectuée en temps utile.

☐ **Définition des seuils :** Il existe des critères clairs pour classer les incidents.

Notes et commentaires :

7. Droits des personnes concernées

☐ **Transparence, obligation d'information :** La déclaration relative à la protection des données est à jour et contient toutes les informations légalement nécessaires.

☐ **Processus de demande de renseignements :** Il est garanti qu'une demande de renseignements peut recevoir une réponse correcte dans le délai prévu par la loi.

☐ **Suppression :** Les données dont le délai de garde a expiré ont été physiquement supprimées ou rendues anonymes au cours de la dernière année.

Notes et commentaires :

8. Résultat de l'auto-évaluation

☐ **Aucune anomalie constatée.**

☐ **Plan d'action établi :** Les points suivants seront corrigés d'ici le :

1.
2.
3.

Signature :

Lieu/date :