Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherung BSV
Direktionstab DS – IT Management ITM

Communication eGov n° 056 de 26.05.2025

A adresser à : Organes d'exécution du 1er pilier/AFam

Concerne : Directives relatives aux contrats avec des tiers

Avec la tendance à l'externalisation des services informatiques et les possibilités modernes d'approvisionnement, les organes d'exécution du 1er pilier/AFam ont de plus en plus souvent recours à des services informatiques fournis par des tiers.

La présente note a pour but de préciser les prescriptions existantes à la ch. 2.15.1 de la D-SIPD concernant les contrats avec des tiers.

Situation initiale et principe

Il existe différentes configurations pour les organismes d'exécution du 1er pilier/AFam avec différentes entreprises partenaires pour les prestations dans le domaine informatique et non informatique. Il convient de noter que les prescriptions de la D-SIPD s'appliquent à l'ensemble de la chaîne de livraison. Ainsi, si une entreprise partenaire d'un organisme d'exécution du 1er pilier/AFam conclut à son tour un contrat de prestations avec un ou plusieurs sous-traitants, les prescriptions de la D-SIPD s'appliquent également à tous les sous-traitants. C'est notamment le cas lorsqu'un tiers obtient des services d'un fournisseur de cloud public.
Le graphique ci-dessous illustre clairement les responsabilités correspondantes :

Organe d'exécution 1er pilier/AFam

- A une relation contractuelle avec un fournisseur informatique / un pool informatique / un prestataire externe.
- Est responsable du respect des conditions relatives à la protection des données conformément à la D-SIPD
- Évalue les dispositions relatives à la protection des données traitées par des tiers.
- La relation contractuelle avec le partenaire est conforme aux exigences de la D-SIPD.

Fournisseur informatique / pool informatique / prestataire externe

- Entretient, si nécessaire, des relations contractuelles avec un sous-traitant ou un fournisseur
- Est responsable de veiller à ce que toute relation contractuelle avec un sous-traitant soit conforme aux exigences de la D-SIPD (par exemple, cryptage supplémentaire avec une clé propre, conservation des données en Suisse, etc.)

Fournisseur de cloud public ou prestataire informatique/ sous-traitant

- Doit fournir le service convenu en Suisse
- Doit prendre en charge le cryptage à l'aide d'une clé contrôlée par le client pour les données personnelles sensibles

Exigences et spécifications

Dans le cadre du ch. 2.15.1de la D-SIPD, les exigences et prescriptions suivantes s'appliquent aux contrats conclus par les organes d'exécution du 1er pilier/AFam avec des tiers :

- **Exigences relatives aux dispositions de protection**
  Les organes d'exécution du 1er pilier/AFam doivent connaître les exigences en matière de protection des données qu'ils souhaitent transmettre à des tiers. Le cas échéant, il convient de procéder à une analyse préalable des risques et à une analyse d'impact relative à la protection des données (AIPD). Les exigences en matière de protection des données doivent être communiquées aux partenaires contractuels (tiers) qui doivent avoir accès aux données relevant du droit des assurances sociales. Cela permet aux partenaires contractuels de documenter à un stade précoce le respect des dispositions de protection et de prouver qu'ils respectent les exigences en matière de protection des données relatives aux données de l'organe d'exécution (protection de base et, le cas échéant, documentation SIPD étendue).
  La protection des données peut également être attestée par une certification ISO 27001 valide ou un rapport d'audit ISAE 3000 correspondant.

- **Sous-traitants**
  En principe, les contrats conclus avec des tiers doivent prévoir que la prestation convenue doit être fournie par le tiers lui-même. Si des tiers font appel à des sous-traitants, les organes d'exécution du 1er pilier/AFam doivent en être informés en tant que clients. Cela vaut en particulier pour les tiers qui agissent en tant que revendeurs de services cloud, tels que les fournisseurs d'applications spécialisées dans le modèle SaaS.
  En cas d'externalisation à des sous-traitants étrangers ou d'utilisation de services publics en nuage étrangers, les partenaires contractuels des organes d'exécution du 1er pilier/AFam doivent garantir, par des mesures appropriées telles qu'un cryptage supplémentaire, qu'aucun accès non autorisé (par exemple par le fournisseur de services en nuage) à des données personnelles sensibles ne puisse avoir lieu.

- **Traitement des données à l'étranger**
  Les prestations de services nécessaires à l'exploitation doivent en principe être fournies en Suisse. Les prestations de services fournies depuis l'étranger doivent être indiquées et justifiées. En principe, seuls les pays offrant un niveau adéquat de protection des données peuvent être pris en considération. Le traitement de données à l'étranger est notamment possible lorsqu'un revendeur de services cloud local agit en tant que partenaire contractuel des organes d'exécution du 1er pilier/AFam.

- **Traitement des données personnelles**
  Il convient de garantir en tout temps qu'aucune donnée personnelle d'assurés n'est traitée à l'étranger, sauf si ce traitement est lié à un échange international de données réglementé sur le plan légal (par ex. art. 32, al. 3, LPGA ou CIBIL ([Accords bilatéraux Suisse-UE. Convention AELE. Circulaire sur la procédure pour la fixation des prestations dans l'AVS/AI/PC]).
  Si des tiers agissant en tant que revendeurs de services cloud stockent des données auprès de fournisseurs de cloud public, les mesures de protection suivantes doivent être mises en œuvre :
  - Les données doivent être traitées dans un centre de données situé en Suisse
  - En outre, des mesures organisationnelles ou techniques appropriées (cryptage) doivent être mises en œuvre afin de garantir la protection contre tout accès non autorisé aux données.

Le secteur ITM

Pour toute autre question, veuillez vous adresser à egov@bsv.admin.ch