Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherung BSV
Etat-major de direction DS - IT Management ITM

Communication eGov nº 043 du 01.01.2022

Adressé à:

- Organes d'exécution (OE) du 1er pilier/AFam

Concerne : Nouvelles recommandations relatives aux exigences minimales pour les systèmes d'information des organes d'exécution du 1er pilier/AFam (version 1.0:2022)

Les recommandations publiées ici sur le site Internet de l'OFAS consacré à l'exécution s'adressent aux organes d'exécution du 1er pilier/AFam. Elles sont publiées dans la perspective de l'entrée en vigueur probable, le 1er janvier 2024, d'une révision de la loi sur l'AVS actuellement traitée par le Parlement (message du Conseil fédéral du 20 novembre 2019 relatif à la modernisation de la surveillance dans le 1er pilier et à l'optimisation du 2e pilier de la prévoyance vieillesse, survivants et invalidité, projet de loi FF 2020 109).

Sur la base de cette révision de la loi, il faut s'attendre à ce que l'Office fédéral des assurances sociales (OFAS) émette des directives sur les exigences minimales dans le domaine de la sécurité de l'information et de la protection des données (SIPD) des systèmes d'information (SI) du 1er pilier/AFam. Les présentes recommandations visent à garantir dès à présent que les OE puissent se préparer de manière optimale aux prochaines directives de l'OFAS relatives aux exigences minimales SIPD. C'est pourquoi les représentants désignés des OE (projet eAVS/AI Information Security) ont été étroitement associés à l'élaboration de la présente version de la recommandation. Le 20.08.2020, il a été décidé au sein du comité eAVS/AI - en présence de l'OFAS en tant qu'invité- qu'une révision en deux étapes devait avoir lieu, étape 1 IT des OE, étape 2 revue des OE via les associations. En d'autres termes, après la publication de la présente version des recommandations, aura lieu la révision des associations, qui prendront position de manière définitive au plus tard à la mi-2022.

Jusqu'à l'entrée en vigueur probable de la révision de la loi sur l'AVS le 1.1.2024, la révision de la loi sur la protection des données (nLPD) du 25 septembre 2020 (FF 2020 7639), déjà adoptée, devrait également être applicable. Les dispositions de l'ordonnance relative à la nLPD ne sont pas encore définitives et seront connues après la publication des présentes recommandations. Les présentes recommandations tiennent déjà compte des dispositions de la nLPD, mais il faut s'attendre à ce que les ordonnances nLPD apportent encore des modifications de contenu, qui seront alors intégrées dans les directives relatives aux exigences minimales SIPD. Ces modifications seront également élaborées et discutées avec les représentants IT des OE (projet eAVS/AI Information Security) ainsi qu'avec les associations.

Les thèmes suivants seront particulièrement importants pour la suite de l'élaboration :

- **Documentation SIPD de base et étendue** (ch. 2.8.2 et 2.8.3 ou annexes 5 et 6) : les exigences minimales doivent être vérifiées quant à leur compatibilité avec les nouvelles ordonnances nLPD.

- **Mandat de tiers/sous-traitants** (ch. 2.15, 2e bulle) : en ce qui concerne l'intervention de sous-traitants (art. 9, al. 3 nLPD), l'autorisation du mandant est nécessaire. La directive à venir doit

également satisfaire à cette exigence légale. La recommandation actuelle devrait éventuellement être renforcée.

- **les personnes qui traitent les données à l'étranger** (ch. 2.15, 3e bulletin et annexe 5, let. E): selon cette recommandation, la conservation des données est en principe prévue en Suisse et les prestations de service pour l'entreprise doivent également être fournies en principe en Suisse et les exceptions doivent être justifiées. Si des données personnelles sont traitées par un sous-traitant à l'étranger, il y a communication de données à l'étranger et des dispositions complexes de la nLPD s'appliquent. L'intervention d'un tiers en tant que sous-traitant à l'étranger est très complexe et nécessite de très nombreuses clarifications juridiques pour les pays pour lesquels le Conseil fédéral n'a pas constaté qu'une protection adéquate était garantie conformément à l'art. 16, al. 1, nLPD. Les directives définitives (ch. 2.15) doivent contenir une mention relative aux restrictions selon la nLPD, qui doit en fin de compte être valable pour tous les OE (aucune exception n'est prévue pour les services cantonaux).

- **Services Cloud de tiers avec conservation des données en Suisse** (ch. 2.15): il ne s'agit pas ici d'une livraison (en masse) directe de données - et d'un traitement de données à l'étranger, mais d'une violation de la protection des données suisse par une entreprise de traitement de données domiciliée en Suisse. Le problème fondamental actuel est le traitement de données sur mandat par des entreprises qui, du point de vue suisse, sont soumises au droit suisse, mais qui, en vertu du Cloud Act américain, peuvent être contraintes par des tribunaux américains de divulguer certaines données aux autorités américaines. Il est probable que des problèmes similaires existent avec le droit d'autres pays (par exemple la Chine). En principe, la législation suisse autorise la communication de données dans le cadre d'une enquête pénale (voir par exemple l'art. 50, al. 1, let. d, LAVS). En raison du principe de territorialité, l'information ne va toutefois qu'à une autorité d'enquête suisse. Si une autorité d'enquête étrangère souhaite obtenir des informations, elle doit les demander par la voie de l'entraide judiciaire - sur la base des accords internationaux correspondants. L'autorité suisse compétente s'adressera alors à l'organe d'exécution. Mais seulement après avoir examiné la demande d'entraide judiciaire. Les demandes d'entraide judiciaire concernant des infractions qui n'existent pas en droit suisse ne seront pas acceptées. En ce qui concerne le Cloud Act, cela signifie dans la pratique une "entraide judiciaire arbitraire", de sorte que le principe de territorialité est supprimé et que la procédure pénale américaine est plus rapide. Dans son évaluation actuelle[1] et sur la base de la LPD actuellement en vigueur, le PFPDT parvient à une appréciation plutôt négative et déclare notamment : "Si, sur la base de l'évaluation des risques, il existe des doutes quant au traitement de données personnelles dans le cloud, il convient de renoncer à une externalisation des données".

  Dans sa prise de position du 8 septembre 20202 sur la transmission de données personnelles aux Etats-Unis et dans d'autres Etats ne disposant pas d'un niveau de protection des données adéquat au sens de l'art. 6, al. 1, nLPD, le PFPDT explique qu'en cas d'accès par les Etats-Unis, un mécanisme de protection essentiel n'est pas clair et que les principes du traitement licite des données selon la LPD sont violés. Pour les personnes concernées en Suisse en cas d'accès aux données par les autorités américaines, il manquerait des droits juridiques exécutables, d'autant plus que l'efficacité du mécanisme dit du médiateur, censé garantir une voie de recours indirectement exécutable, ne peut pas être évaluée faute de transparence et que les compétences décisionnelles du médiateur vis-à-vis des services secrets américains ainsi que son indépendance effective restent non démontrées en l'absence d'informations suffisamment concrètes et concluantes. Le PFPDT considère que ce manque de transparence et l'absence de garanties qui en découle en cas d'ingérence des autorités américaines dans la sphère privée et l'autodétermination informationnelle de personnes en Suisse sont incompatibles avec le droit de ces personnes à une voie de droit selon les art. 29 ss. Cst. et à l'art. 15 LPD pour faire valoir les droits qui leur sont conférés par l'art. 13, al. 2, Cst. et l'art. 8 CEDH ; avec les principes d'un traitement licite des données personnelles au sens de l'art. 4 LPD.

[1] Voir Erläuterungen zu Cloud Computing (admin.ch)
[2] Voir la prise de positiondu PFPDT

Au sein de l'administration fédérale, la problématique des services Cloud est toutefois actuellement examinée de manière approfondie, ceci dans le cadre du projet "Public Cloud Bund". En ce qui concerne les contrats entre la Confédération et les cinq fournisseurs de cloud (OMC 20007, Acquisition du cloud public fédéral), il s'agit d'une procédure encore en cours. La Chancellerie fédérale est compétente en la matière. Dans cette mesure, il devrait être possible de compléter le thème des "mandats à des tiers" en ce qui concerne les services de cloud jusqu'à l'entrée en vigueur des directives OFAS SPID.

On peut déjà constater, dans l'état actuel du projet, que les données personnelles ne pourront vraisemblablement pas être stockées ou traitées d'une autre manière dans le nuage de fournisseurs problématiques (p. ex. Cloud-Act). Dans cette mesure, le recours aux services d'informatique Cloud dans le cadre des assurances sociales ne peut être recommandé dans un avenir prévisible que s'il s'agit de fournisseurs qui offrent la garantie que la transmission directe de données à des autorités étrangères peut être exclue.

Nous vous remercions de la prise en considération de ce message, ainsi que de sa mise en application au sein de votre organe d'exécution.

Le secteur DS/ITM

Pour toute question, l'adresse email suivante est à votre disposition egov@bsv.admin.ch