Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral des assurances sociales OFAS

Recommandations sur les exigences minimales relatives aux systèmes d'information des organes d'exécution du 1er pilier/des allocations familiales

Valable à partir du 1er janvier 2022

État : 1er janvier 2022

Remarques préliminaires

Les recommandations s'adressent aux organes d'exécution (OE) du 1er pilier/des allocations familiales (AF). Elles sont publiées en tenant compte du fait que la révision de la LAVS, actuellement débattue au Parlement (Message du Conseil fédéral du 20 novembre 2019 concernant la modernisation de la surveillance dans le 1er pilier et l'optimisation dans le 2e pilier de la prévoyance vieillesse, survivants et invalidité, projet de loi FF 2020 107), entrera probablement en vigueur le 1er janvier 2024.

Sur la base de cette révision, l'Office fédéral des assurances sociales (OFAS) publiera 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/ AF. Les présentes recommandations doivent permettre aujourd'hui déjà de garantir que OE pourront se préparer de manière optimale aux futures directives de l'OFAS concernant les exigences minimales SIPD. C'est pourquoi les représentants informatiques des OE (projet eAVS/AI Information Security) ont été étroitement impliqués dans l'élaboration de la présente version des recommandations.

La révision déjà approuvée de la loi sur la protection des données (nLPD) du 25 septembre 2020 (FF 2020 7397) devrait déployer ses effets jusqu'à l'entrée en vigueur vraisemblable de la révision de la LAVS le 1er janvier 2024. Les dispositions de l'ordonnance relative à la nLPD (nOLPD) ne sont pas encore définitives et seront connues après la publication des présentes recommandations. Celles-ci tiennent déjà compte des dispositions de la nLPD ; il faut toutefois partir du principe que la nOLPD pourrait apporter des modifications de fond qui influenceront par la suite les directives concernant les exigences minimales de SIPD. Ces modifications seront également traitées et discutées avec les représentants informatiques des OE (projet eAVS/AI Information Security).

Les thèmes suivants revêtiront une importance particulière pour les prochaines élaborations :

- **Documentation de base et élargie de la SIPD** (points 2.8.2 et 2.8.3, et annexes 5 et 6) : les exigences minimales doivent être soumises à un examen de compatibilité avec la nOLPD.
- **Mandat à des tiers/sous-traitants** (point 2.15, 2e élément) : concernant l'intervention de sous-traitants (art. 9, al. 3, nLPD), l'approbation du mandant est nécessaire. La directive à venir doit également satisfaire à cette exigence légale. La recommandation actuelle devrait éventuellement être renforcée.
- **Sous-traitant à l'étranger** (point 2.15, 3e élément et annexe 5, let. E) : conformément à cette recommandation, la conservation de données est en principe prévue en Suisse et les prestations pour les entreprises doivent normalement avoir lieu sur le territoire national, toute exception devant être justifiée. Le traitement de données personnelles par un sous-traitant étranger donne lieu à une communication de données à l'étranger, et des dispositions complexes de la nLPD s'appliquent. L'intégration d'un tiers en tant que sous-traitant à l'étranger est très complexe et requiert de très nombreuses clarifications juridiques pour les pays dont le Conseil fédéral n'a pas déterminé qu'ils garantissent un niveau de protection adéquat au sens de l'art. 16, art. 1, nLPD. Un renvoi aux restrictions selon la nLPD doit être fait dans les directives définitives (point 2.15), qui devra s'appliquer à tous les OE (aucune exception prévue pour les organes cantonaux).
- **Services cloud de tiers avec conservation de données en Suisse** (point 2.15) : il ne s'agit dans ce cas pas directement d'une livraison de données (de masse) et d'une sous-traitance à l'étranger, mais de la violation de la législation suisse sur la protection des données par un sous-traitant domicilié en Suisse. Le problème de base actuel est le traitement de données par le fournisseur Microsoft Suisse, qui, du point de vue national, est soumis au droit suisse, mais peut, en raison du Cloud-Act des États-Unis être obligé par les tribunaux américains à divulguer certaines données aux autorités américaines. La législation suisse autorise en principe la divulgation de données dans le cadre d'une instruction pénale (cf. par ex. art. 50, al. 1, let. d, LAVS). En raison du principe de territorialité, l'information ne parvient toutefois qu'aux autorités d'instruction suisses. Si une autorité d'instruction

étrangère souhaite obtenir des renseignements, elle doit demander les informations par la voie de l'entraide judiciaire, en s'appuyant sur la convention internationale correspondante. L'autorité suisse compétente s'adresse alors à l'organe d'exécution, une fois la demande d'entraide judiciaire examinée. Les requêtes d'entraide judiciaire pour des éléments constitutifs d'une infraction qui n'existe pas en droit suisse sont rejetées. S'agissant du Cloud-Act, cela signifie qu'en pratique, il existe une « entraide judiciaire d'office », de sorte que le principe de territorialité est neutralisé et que la procédure pénale américaine s'accélère. Sur la base de sa dernière analyse[1] et de la LPD actuellement en vigueur, le PFPDT parvient à une évaluation plutôt négative et détermine en particulier : ***« Si à la suite de l'analyse des risques, il existe des doutes sur la manière dont les données personnelles sont traitées dans le Cloud, il ne faut pas les délocaliser. »***

Dans la prise de position du PFPDT[2] sur la transmission de données personnelles aux États-Unis et d'autres États sans niveau de protection adéquat, au sens de l'art. 6, al. 1, nLPD du 8.9.2020, il est précisé que pour les accès des États-Unis, une part importante du mécanisme de protection reste vague et que les principes de traitement licite des données conformément à la LPD seraient violés. Pour les personnes en Suisse concernées par l'accès aux données par les autorités des États-Unis, cela se traduirait par une absence de droits exécutoires, à plus forte raison si l'efficacité du dénommé mécanisme d'ombudsman, qui devrait garantir un droit de recours applicable indirectement, ne peut être évaluée par manque de transparence et si la compétence décisionnelle de l'ombudsman vis-à-vis des services secrets américains et sa réelle indépendance reste invérifiée en l'absence d'informations suffisamment concrètes et pertinentes. Le PFPDT estime que ce manque de transparence et, partant, l'absence de garanties en cas d'ingérence des autorités américaines dans la sphère privée et le droit à l'autodétermination informationnelle des personnes en Suisse est incompatible avec le droit de ces personnes à une voie de recours au sens des art. 29 ss Cst. et de 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 de la licéité du traitement des données personnelles au sens de l'art. 4 LPD.

La problématique des services cloud est actuellement examinée en détail au sein de l'administration fédérale et il reste à espérer que la transparence nécessaire sera mise en place. Il faudrait pouvoir régler les questions juridiques lors des prochaines étapes, dans le cadre de la stratégie cloud de l'administration fédérale. Pour ce qui est des contrats entre la Confédération (OMC 20007, acquisition Public Clouds Confédération) et Microsoft, la procédure est toujours en cours. La Chancellerie fédérale est compétente en la matière. Dans ce contexte, il devrait être possible d'apporter un complément au thème des « mandats à des tiers » en lien avec des services cloud d'ici à l'entrée en vigueur des directives SIPD de l'OFAS.

[1] Voir les explications concernant l'informatique en nuage (cloud computing) (admin.ch)
[2] Voir la prise de position du PFPDT

1 Recommandations SIPD sur les exigences minimales

Point	Recommandations de l'OFAS sur la sécurité de l'information	Référence à DIN ISO/IEC 27001: 2015-03 (A=Annexe normatif)	Commentaire
1	**Objectif, but, objet, principes, champ d'application, principes et références dans le système juridique**		
1.1	**Objectif, but et objet** Compte tenu du message du 20 novembre 2019 du Conseil fédéral[3] et du projet de loi[4] concernant la modernisation de la surveillance dans le 1er pilier et l'optimisation dans le 2e pilier de la prévoyance vieillesse, survivants et invalidité, l'OFAS recommande aux organes d'exécution de tenir compte continuellement des conditions-cadres à venir, décrites ci-après, dans leurs systèmes d'information. L'une des principales préoccupations dans la révision de la loi en cours reste que les systèmes d'information du 1er pilier disposent de la stabilité et de la capacité d'adaptation nécessaires et garantissent la sécurité de l'information et la protection des données. Il relève en principe de la propre responsabilité des organes d'exécution de garantir la réalisation de ces objectifs (cf. art. 49a, al. 2, du projet de LAVS). Concernant la sécurité de l'information et la protection des données, les organes d'exécution devront toutefois satisfaire en plus, à l'avenir, aux exigences minimales fixées par les autorités de surveillance (art. 49a, al. 3, projet de LAVS). S'il advenait que pour mettre en œuvre les exigences minimales, les organisations spécialisées des organes d'exécution élaboraient, conformément à la nouvelle législation, des règles reconnues par l'autorité de surveillance (art. 49a, al. 4, projet de LAVS), ces règles reconnues de mise en œuvre devraient être appliquées par les organes d'exécution, pour autant que ces derniers y soient soumis (cf. point 1.2). Les présentes recommandations esquissent les futures exigences minimales relatives aux systèmes d'information en matière de sécurité de l'information et de protection des données (art. 49a, al. 3 en lien avec l'art. 72a, al. 2, let. b du projet de LAVS),		

[3] FF **2020** 1
[4] FF 2020 107

	auxquelles les organes d'exécution doivent satisfaire (tous les points du chapitre 2).		
1.2 **1.2.1**	**Champ d'application** Les présentes recommandations relatives aux exigences minimales du point 2 s'adressent à tous les organes d'exécution de l'AVS, de l'AI, des APG et des PC (cf. art. 66, al. 1, let. a du projet de LAI, art. 21, al. 2 du projet de LAPG, art. 26, al. 1, let. a du projet de LPC). Elles s'adressent également à toutes les agences au sens de l'art. 65 LAVS. Les recommandations s'appliquent en outre à la gestion des allocations familiales (art. 25, let. a en lien avec l'art. 27, al. 3 du projet de LAFam et art. 25 LFA).		
1.3	**Définition d'un système d'information (SI)** Un système d'information est un outil pour le traitement des données, la communication de données ainsi que le profilage (selon la nLPD) aux fins de l'exécution de tâches[5] et contient des éléments techniques et organisationnels. Il s'agit en particulier - des éléments techniques : matériel informatique, logiciels et composants du réseau, - de l'application et des volumes de données, - des éléments organisationnels : processus, tâches, compétences et responsabilité en matière de développement et d'exploitation. Un système d'information constitue toujours une valeur qu'il faut adéquatement protéger. Il s'agit ainsi d'un objet protégé (cf. point 2.8).	A.8.1.1	
1.4	**Principe de système de gestion de la sécurité de l'information (SGSI)** Les organes d'exécution doivent en premier lieu exploiter un système de gestion de la sécurité de l'information (SGSI) leur permettant de satisfaire aux exigences minimales. Celui-ci doit s'appuyer		L'art. 68a du projet LAVS ne s'applique pas à la LAFam (contrairement à la LFA). Les règles de révision des caisses et du contrôle des employeurs relèvent explicitement de la compétence

[5] au sens de l'art. 5, let. d à g, nLPD

	sur des normes nationales[6] et internationales[7] et répondre au moins aux critères suivants : Un SGSI se compose de critères, de rôles et de responsabilités, de processus et de procédures qui servent à réaliser les objectifs définis d'une organisation. Le SGSI fera vraisemblablement l'objet d'un contrôle de la part de l'organe de révision au sens de l'art. 68a, al. 2, let. c, projet de LAVS. L'organe de révision vérifiera si le SGSI de l'organe d'exécution répond aux exigences minimales définies dans les présentes recommandations. Les caisses de compensation pour allocations familiales au sens de l'art. 14, let. a, LAFam en sont exclues, sauf disposition contraire dans la loi cantonale sur les allocations familiales.		cantonale selon l'art. 17, al. 2, let. i, LAFam. Pour les organes d'exécution de l'AVS, qui assument également la gestion des allocations familiales en tant que tâche déléguée, la révision portera sur le SGSI, y compris les allocations familiales. L'établissement d'un rapport séparé, notamment au sens du point 3604 DRAT, est possible le cas échéant.
1.5 **1.5.1** **1.5.2** **1.5.3**	**Sécurité de l'information** La sécurité de l'information est un terme générique. Il englobe des mesures dont le but est d'assurer cette sécurité (du développement du projet jusqu'à la protection des appareils). La sécurité des données et une grande partie de la protection des données appartiennent à la sécurité de l'information. - La sécurité des données comprend, d'un point de vue pratique, toutes les mesures permettant de garantir la fiabilité, l'intégrité, la traçabilité et la disponibilité des informations. - La protection des données, quant à elle, inclut d'un point de vue pratique toutes les mesures visant à éviter un traitement indésirable de données personnelles et ses conséquences. La protection cible la personne et pas les données en soi. En principe, les prescriptions de sources de droit très différentes s'appliquent à la sécurité de		Il s'agit de mesures techniques et organisationnelles. Elles ne doivent pas être confondues avec les mesures techniques et organisationnelles au sens de l'art. 153d du projet de LAVS[8], qui doivent être uniquement respectées par les autorités, organisations et personnes autorisées à utiliser le numéro d'assuré AVS en dehors des assurances sociales.

[6] en particulier les critères de protection informatique de base dans l'administration fédérale ou la loi sur la sécurité de l'information (LSI) du 18 décembre 2020 (FF 2020 9665) après son entrée en vigueur

[7] ISO/IEC 27001, 2013 + Cor 1:2014) Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences (avec annexe 1 normative concernant les objectifs et mesures de références, qui dérivent de la norme ISO/IEC 27002 (Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information [ISI/IEC27002 : 2013 + Cor 1:2014 + Cor 2:2015]).

[8] Conformément au message relatif à la modification de la loi fédérale sur l'assurance-vieillesse et survivants (utilisation systématique du numéro AVS par les autorités [FF 2019 6993])

	l'information et doivent être prises en compte par les organes d'exécution (cf. annexe 1 : Aperçu des sources nationales de droit, normes ISO). La présente directive se concentre sur les exigences à remplir par un SGSI et n'aborde aucune question de protection des données qui pourrait surgir de la relation directe entre la personne assurée et l'organe d'exécution. Pour de tels cas, la circulaire sur l'obligation de garder le secret et sur la communication des données dans le domaine de l'AVS/AI/APG/PC/AFA/AF (COGSC) continue de s'appliquer. Toutefois, les questions de protection des données sont prises en considération dans cette recommandation destinée aux organes d'exécution, les exigences de protection des données devant être vérifiées lors de l'élaboration d'une documentation de base du SGSI pour la sécurité de l'information (cf. partie lettre a, conformément au point 2.8.2). Pour les questions de conservation des données, il convient de se référer en outre à la directive sur la gestion des dossiers dans les domaines AVS/AI/APG/PC/AFA/AF (DGD).		
2	**Exigences minimales**		
2.1	**Système de gestion de la sécurité de l'information (SGSI)**[9] Chaque organe d'exécution dispose d'un SGSI (cf. point 1.4).	4.4	
2.2	**Structure de base du SGSI de l'organe d'exécution**		
a	Les organes d'exécution déterminent dans leur SGSI quels sont les thèmes pertinents pour l'exécution de leurs tâches selon l'art. 63 LAVS (RS 831.10), l'art. 57 LAI (RS 831.20) et leurs activités dans le cadre de la LAPG (RS 834.1), la LPC (RS 831.30), la LFA (RS 836.1) et la LAFam (RS 836.2).	4.1	
b	Ils identifient les services impliqués et analysent leurs exigences en lien avec la sécurité de l'information sur la base des modèles de domaines techniques standardisés de l'OFAS (cf. annexe 2).	4.2	
c	Ils disposent d'un aperçu à jour de tous les systèmes d'information et des activités pertinentes pour l'informatique (cf. inventaire selon le chif. 2.8), dont la structure se base sur les modèles de domaines techniques standardisés de l'OFAS	A.8.1.1	

[9] Pour mettre sur pied le SGSI, les guides suivants sont recommandés :
- Guide ISACA : https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_i_gesamt_web.pdf (en allemand)
- Il existe en outre aujourd'hui des systèmes d'information/outils sur le marché qui aident à élaborer un SGSI numérique (voir l'exemple https://swissgrc.com/)

	(systèmes d'information exploités, projets informatiques et adaptations continues des applications existantes) intégrés dans le SGSI.		
d	Ils déterminent en parallèle les domaines auxquels les exigences minimales ne s'appliquent pas (par ex. les organes d'exécution qui assument des tâches en dehors du champ du 1er pilier/des AF doivent déterminer quels champs d'application sont exclus). Si aucune délimitation n'est réalisée, le SGSI s'applique à l'ensemble de l'organisation.	4.3	
e.	Les organes d'exécution assurent la mise à jour et l'amélioration régulières du SGSI (y compris la gestion de la continuité des affaires (BCM), cf. point 2.17) et de ses composants (cf. image de l'annexe 3). Ils procèdent au minimum à une vérification annuelle de la mise à jour.	4.4	
2.3	**Lignes directrices relatives à la sécurité de l'information** La direction de l'organe d'exécution publie des lignes directrices relatives à la sécurité de l'information qui s'appuient sur la structure de base du SGSI (chif. 2.2) et s'assure de leur communication au sein de l'organe d'exécution et auprès des services externes impliqués, ainsi que de leur mise à jour régulière.	A.5.1 / A.5.1.1	
	Les lignes directrices relatives à la sécurité de l'information intègrent le principe de séparation des tâches et contiennent les éléments suivants : 1. La définition de l'organisation de la sécurité de l'information et ses interfaces avec les éléments prescrits suivants (art. 66, projet LAVS) : a. système de contrôle interne (SCI), b. système de gestion de la qualité (en particulier l'amélioration continue), c. système de gestion des risques. 2. La réglementation de l'information adéquate de la direction et des autres services impliqués (cf. point 2.2, let. b et d) ainsi que, le cas échéant a. du PFPDT, selon l'art. 24 nLPD (en cas de violation correspondante de la sécurité des données), ou du responsable de la protection des données selon le droit cantonal ; b. de l'OFAS, par l'organisation de la sécurité de l'information et la description d'un processus de traitement des incidents en lien avec la sécurité de l'information. (cf. annexe 4 à titre d'exemple). 3. La réglementation de l'information adéquate de l'OFAS (et/ou des autorités de surveillance	A.6.1.2	

	compétentes) sur les incidents en lien avec la sécurité de l'information doit être prévue au minimum pour les cas suivants, lorsque • il est nécessaire d'informer le PFPDT ou le responsable cantonal de la protection des données ; • il existe un risque que l'incident nuise au système d'information d'autres organes d'exécution ; • l'incident concerne les intérêts des assurés au-delà de quelques cas isolés ou remet en question l'exécution des tâches de l'organe d'exécution ; • l'incident peut causer d'importants dégâts financiers ; • l'image de l'assurance peut se dégrader au-delà d'un cas mineur (par ex. importante perte ou manipulation de données) ; • il est possible que le fonctionnement de l'organisation de la sécurité de l'information de l'organe d'exécution ne soit pas assuré dans un futur proche ou ait été entravé par le passé.		
2.4	**Exigences relatives à l'organisation de la sécurité de l'information** L'organisation de la sécurité vise au minimum à ce que l'organe d'exécution désigne un responsable de la sécurité de l'information et d'autres personnes qui assument un rôle clé dans la mise en œuvre de la sécurité de l'information. Le responsable de la sécurité de l'information assume les tâches suivantes : • Il coordonne les aspects de sécurité de l'information au sein de l'organe d'exécution ainsi qu'avec les éventuels fournisseurs de prestations mandatés (par ex. responsable informatique, fournisseurs, etc.) • Il est l'interlocuteur des responsables de la sécurité de l'information des fournisseurs informatiques. • Il est l'interlocuteur vis-à-vis de l'OFAS pour les incidents relatifs à la sécurité de l'information qui doivent être signalés à l'OFAS (point 2.3, chif. 3) selon les lignes directrices relatives à la sécurité de l'information publiées par l'organe d'exécution. • Il vérifie la documentation relative à la sécurité de l'information (en particulier la documentation du SIPD, cf. points 2.8.2 et 2.8.3) et à la mise en œuvre des exigences minimales ainsi que des règles de mise en œuvre reconnues	A 6.1 (A.6.1.1-A.6.1.3)	Règles particulières pour les CAF (éventuellement canton)

	établies par l'organisation spécialisée de l'organe d'exécution dans le domaine de la sécurité de l'information. Pour les CAF, au sens de l'art. 14, let. a, LAFam, la documentation en lien avec les règles de mise en œuvre reconnues ne doit être vérifiée que si les dispositions cantonales le prévoient. • Il informe régulièrement la personne responsable de l'organe d'exécution sur l'état actuel des aspects de sécurité de l'information dans son organisation. • Il émet des recommandations à l'attention de la direction de l'organe d'exécution.		
2.5	**Exigences à remplir par les projets dans le domaine des systèmes d'information** Un projet dans le domaine des systèmes d'information est limité dans le temps, il contient des objectifs définis et une organisation spécifique dont le principal but est d'introduire ou d'adapter une application, ou encore de construire ou améliorer des infrastructures du système d'information. Les organes d'exécutions règlent le déroulement des projets dans le domaine des systèmes d'information. Ils tiennent toujours compte des aspects suivants : 1. la procédure doit suivre une méthode de gestion de projet définie, qui assure la traçabilité lors du pilotage, de la direction et de la réalisation de projets ayant différentes caractéristiques et complexités. La méthode de gestion de projet utilisée est conforme à la norme suisse de l'association eCH ou équivalente (www.ech.ch). 2. il convient d'élaborer une documentation relative à la sécurité de l'information et à la protection des données (documentation de base SIPD selon le point 2.8.2) et, si nécessaire, une documentation élargie du SIPD, selon le point 2.8.3.[10]	A.6.1.5 A.8.1.3 A.8.2 (A.8.2.1, A.8.2.2, A.8.2.3 Chiffre 2 loi nationale LPD	
2.6	**Sécurité de l'information pour les appareils mobiles et le télétravail** Les organes d'exécution règlent	A.6.2.1, A.6.2.2	

[10] En cas d'utilisation d'Hermes en tant que méthode de gestion de projet, les critères d'analyse d'impact de la protection des données selon la nLPD (cf. point 2.8.2, let. h et point 2.8.3, let. c) sont en principe remplis (cf. message du 15 septembre 2017 du Conseil fédéral concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales (FF 2017 6565)).

	• Les conditions-cadres qui régissent le télétravail et l'utilisation d'appareils mobiles pour le personnel concerné. • L'utilisation professionnelle sûre d'appareils mobiles privés et professionnels, en tenant compte de la possibilité de perte, de vol ou de dégâts. Sont exclues les possibilités d'accès anonyme et personnalisé à des applications conçues sous forme de site Internet public de l'organe d'exécution. Il convient d'assurer une protection équivalente en cas d'utilisation d'appareils privés. • L'exercice sûr du télétravail grâce à des mesures de sécurité auxiliaires pour protéger les informations auxquelles les collaborateurs ont accès depuis les postes de télétravail ou qui doivent y être traitées ou sauvegardées. Les appareils privés utilisés dans un contexte professionnel doivent être soumis au moins aux mêmes conditions en matière de sécurité de l'information et de protection des données que celles applicables aux appareils mis à disposition par l'organe d'exécution.		
2.7	**Sécurité de l'information et personnel**		
2.7.1	**Sécurité du personnel** Les organes d'exécution règlent l'engagement de leur propre personnel et du personnel des tiers mandatés pour la période avant, pendant et après l'engagement de manière à garantir la sécurité de l'information. Il convient de prévoir en particulier un processus pour le contrôle de sécurité adéquat du responsable de la sécurité de l'information et des autres rôles clés dans l'organisation de la sécurité de l'information (cf. point 2.4), qui permette d'identifier les risques en lien avec l'intégrité personnelle et d'adopter des mesures adéquates.	A.7 (A.7.1-A.7.3)	Il faut garantir que les dispositions ne soient pas incompatibles avec d'autres prescriptions (par ex. règlement du personnel)
2.7.2	**Information et formation** Les organes d'exécution veillent à ce que le personnel engagé soit régulièrement informé sur les obligations en matière de sécurité de l'information et y soit sensibilisé.	A.7.2	
2.7.3	**Changement de situation** Les droits d'utilisateur du personnel engagé concernant l'accès (cf. point 2.11.1) et les autorisations aux systèmes d'information (cf. point 2.9) doivent être tenus à jour. Ils doivent être immédiatement adaptés aux changements de situation lorsque l'engagement, le mandat ou une convention d'utilisation correspondante sont	A.7.1-A.7.3	

	modifiés ou prennent fin. Il convient de mettre en place un processus pour gérer les comptes inutilisés.		
2.8	**Objets protégés du SI : inventaire, documentation SIPD et autres exigences**	A.8.1	
2.8.1	Les organes d'exécution disposent d'un **inventaire** de tous les systèmes d'information (cf. point 2.2, let. c). Celui-ci est mis à jour régulièrement. Un système d'information constitue toujours une valeur qu'il faut adéquatement protéger. Il s'agit donc d'un objet protégé.	A.8.1.1	
2.8.2	**Documentation de base du SIPD** 1. Il convient de réaliser une analyse de la sécurité de l'information et de la protection des données préalablement à tout projet SI (point 2.5). 2. La documentation de base du SIPD doit au minimum couvrir les thèmes suivants en lien avec la sécurité de l'information et la protection des données : a. clarification des conditions-cadres applicables en droit de la protection des données, en particulier concernant la conformité au droit du traitement des données selon la LPD et les éventuelles lois cantonales de protection des données en vigueur, ainsi que les dispositions des lois régissant les assurances sociales ; b. classification des exigences de disponibilité (y compris évaluation de l'objet protégé en lien avec la classification en tant qu'application essentielle) ; c. classification des exigences de confidentialité ; d. classification des exigences d'intégrité et de traçabilité (concernant l'accès aux données en mode écriture) ; e. lieu de conservation des données ; f. description de l'objet protégé ; g. clarification des règles d'inscription dans le registre d'activités ou de notification au PFPDT (art. 12, al. 4, nLPD). Les organes d'exécution qui sont des organismes cantonaux clarifient l'inscription auprès d'un registre cantonal, conformément à la loi cantonale de protection des données ; h. clarification de la nécessité d'une analyse d'impact relative à la protection des données au sens de l'art. 22 nLPD ;	A.8.1.3 A.8.2 (A.8.2.1, A.8.2.2, A.8.2.3)	

	i. attribution à un groupe de protection. 3. Si, sur la base de l'analyse du chiffre 2, il est établi que des données personnelles sensibles ou d'autres données soumises à des exigences particulières de confidentialité sont traitées avec l'objet protégé, il faut élargir la documentation de base SIPD conformément au point 2.8.3. 4. La documentation de base du SIPD doit s'orienter sur le modèle de l'annexe 5, que ce soit sous un aspect qualitatif ou quantitatif.		
2.8.3	**Documentation SIPD élargie** La documentation SIPD élargie doit être élaborée lorsque des données personnelles sensibles sont traitées avec l'objet protégé (point 2.8.2, chif. 3). Elle doit englober au moins les thèmes suivants : a. résumé des événements pertinents de la documentation de base du SIPD ; b. description sécuritaire du système ; b.1 interlocuteurs/responsabilités b.2 description de l'ensemble du système b.3 description des données à traiter (règlement du traitement avec concept de rôles et gestion des supports de données) b.4 esquisse d'architecture/matrice de communication b.5 description de la technologie sous-jacente c. analyse de risque (avec analyse d'impact relative à la protection des données pour autant que ce soit nécessaire), mesures de protection et risque résiduel (le cas échéant avec prise de position du PFPDT) ; d. rétablissement de l'activité/concept d'urgence (prévision des catastrophes, crises) ; e. respect/contrôle/adoption des mesures de protection ; f. mise hors service. 3. La documentation SIPD élargie doit s'orienter sur le modèle de l'annexe 6, que ce soit sous un aspect qualitatif ou quantitatif.	A.8.1.3 A.8.2 (A.8.2.1, A.8.2.2, A.8.2.3)	
2.8.4	**Mise à jour de la documentation SIPD** Les systèmes d'information existants (en exploitation) doivent disposer d'une documentation SIPD (points 2.8.2 et 2.8.3) qui corresponde aux relations effectives.		

2.8.5	**Responsable application** Les organes d'exécution désignent pour chaque système d'information utilisé individuellement ou en commun un responsable d'application. Celui-ci détermine avec le responsable de la sécurité de l'information les exigences de sécurité pour le système d'information. Le responsable application répond de la mise en œuvre des mesures de sécurité.	A.8.1.2	
2.9	**Gestion de l'accès aux systèmes d'information** Les organes d'exécution gèrent l'accès à leurs systèmes d'information. Le concept de gestion de l'accès contient au moins a. une gestion des utilisateurs avec une identification univoque des utilisateurs ; b. un modèle d'autorisation selon les fonctions/tâches des utilisateurs ; c. des processus d'octroi, de mutation et de retrait de comptes utilisateurs et d'autorisations ; et assure que d. l'ensemble des accès (y compris les processus automatisés avec accès machine-to-machine) aux systèmes d'information soient protégés par une authentification correspondant au besoin de protection et, si nécessaire, par des mesures cryptographiques adéquates (ISO A.10) conformément à la matrice d'accès (cf. aussi point 2.13.2) ; e. les utilisateurs reçoivent uniquement les droits d'accès aux systèmes d'informations nécessaires pour l'exécution de leurs tâches ; f. l'exactitude et la pertinence des droits d'accès octroyés sont contrôlées au moins une fois par an par le responsable application.	A.9 (A.9.1, A.9.2, A.9.3, A.9.4)	
2.10	**Cryptographie**		
2.10.1	- Les procédures et méthodes cryptographiques mises en place par les organes d'exécution doivent correspondre à l'état de la technique. En cas d'utilisation de systèmes de cryptage asymétriques, les certificats doivent être établis par une autorité de certification (AC) reconnue, en fonction du cas d'application et des exigences juridiques correspondantes. On peut mentionner les cas d'application suivants, non exhaustifs, à titre d'exemple : - Certificats reconnus par Mozilla pour des solutions technologiques WEB, etc.	A.10.1.1	

	- Certificats reconnus par SAS pour des signatures électroniques, conformément à l'ordonnance sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (OSCSE RS 943.032)[11]. - La solution choisie doit être décrite dans la documentation SIPD (points 2.8.2 ou 2.8.3). - Les organes d'exécution garantissent la gestion sûre et la validité des clés cryptographiques.	A.10.1.2	
2.11 2.11.1	**Protection physique** **Dispositif de sécurité pour les locaux** Les organes d'exécution possèdent un dispositif de sécurité pour protéger physiquement leurs systèmes d'information. Différentes mesures sont à prévoir afin de garantir la protection individuelle adéquate des objets protégés, en tenant compte des résultats du contrôle SIPD (points 2.8.2 ou 2.8.3) concernant les groupes de protection (cf. point 2.8.2, chif. 2, let. i). Les mesures de protection prévues dans le dispositif de sécurité doivent se rapporter aux points suivants : • périmètre de sécurité physique (situation de l'environnement et mesures architecturales) ; • gestion de l'accès physique ; • protection des bureaux, salles et installations ; • protection contre les menaces externes et environnementales.	A.11.1.1-A.11.1.4	
2.11.2	**Mesures pour les appareils et les équipements d'entreprise** Les organes d'exécution et leurs fournisseurs (cf. point 2.15) disposent de mesures documentées visant à protéger les appareils et les équipements d'entreprise contre la perte, les dégâts, le vol ou la mise en danger. Les mesures prévues pour les appareils doivent se rapporter aux points suivants : • placement et protection des appareils et des équipements d'entreprise ; • installations de services publics ; • sécurité du câblage ; • maintenance des appareils et des équipements d'entreprise ;	A.11.2.1-11.2.9	

[11] cf. à ce propos le site Internet de l'OFCOM

	• suppression des valeurs ; • sécurité des appareils, équipements d'entreprise et valeurs en dehors des locaux ; • élimination sûre ou réutilisation d'appareils et d'équipements d'entreprise ; • appareils d'utilisateurs sans surveillance ;directives pour un environnement professionnel propre et verrouillages des écrans		
2.12	**Mesures en faveur de la sécurité d'entreprise** Les organes d'exécution et leurs fournisseurs (cf. point 2.15) disposent de mesures documentées en faveur de la sécurité d'entreprise. Les mesures prévues doivent se rapporter aux points suivants : A. Processus et responsabilités dans l'entreprise • procédures opérationnelles documentées ; • gestion des modifications ; • gestion des capacités ; • séparation des environnements de développement, de test et d'exploitation. B. Protection contre des logiciels malveillants par des mesures adaptées C. Sécurité des données D. Enregistrement et surveillance • enregistrement des résultats ; • protection des informations enregistrées ; • activités des administrateurs et des utilisateurs ; • synchronisation des horloges ; E. Gestion des logiciels pour installer des logiciels sur les systèmes en exploitation F. Faiblesses techniques • gestion des faiblesses techniques ; • restriction d'installation de logiciels ; G. Contrôle d'intégrité en cas de besoin accru de protection (cf. annexe 5, documentation SIPD élargie, let. D) H. Contrôle des systèmes d'information • mesures pour les contrôles des systèmes d'information afin de minimiser les conséquences négatives des activités de contrôle. En effet, les activités de contrôle, comme le test d'intrusion et les tests de prévention de crise peuvent avoir des conséquences négatives sur les systèmes d'information, les données et les utilisateurs. C'est pourquoi des mesures correspondantes, dont une planification détaillée, la communication, etc. doivent être prévues afin de diminuer ce type de conséquences.	A.12 A.12.1(A.12.1.1-A.12.1.4) A.12.2 A.12.3 A.12.4 A.12.5 A.12.6. A.12.7	

2.13	**Sécurité des communications (transfert d'informations)**		
2.13.1	**Documentation de l'architecture** Les organes d'exécution disposent d'une documentation d'architecture qui porte sur l'environnement de leurs systèmes d'information. Celle-ci renseigne sur • les topologies de réseaux propres et externes sous-jacentes des réseaux utilisés dans le cadre de leur inventaire de valeurs (cf. chif. 2.8.1) ; • les topologies de réseaux sous-jacentes, y compris ses composants actifs et leurs configurations.		
2.13.2	**Matrice d'accès** Les organes d'exécution disposent d'une matrice d'accès contraignante qui détermine la manière dont les personnes et les processus automatisés (machines/logiciels) peuvent accéder aux systèmes d'information exploités dans les différentes zones du réseau (cf. chif. 2.13.3) ou la manière dont elles doivent être authentifiées et éventuellement autorisées (cf. chif. 2.10, cryptographie)		
2.13.3	**Sécurité et documentation réseau** 1. Les organes d'exécution doivent prévoir des directives relatives à la sécurité réseau et déterminer les responsabilités en matière de gestion des réseaux et connexions entre les réseaux. 2. Les organes d'exécution disposent, pour les réseaux sous leur responsabilité, d'un règlement d'utilisation qui définit au moins les points suivants : • raccordement d'appareils de communication externes ; • règlement des connexions entre réseaux ; • accès à distance. 3. Les organes d'exécution doivent assurer la protection des données en lien avec le 1er pilier à l'aide d'une structure réseau adéquate (par ex. zonage et segmentation), d'une construction adaptée et d'une bonne configuration. 4. Les organes d'exécution protègent les réseaux sous leur responsabilité contre les attaques et les accès non autorisés.	A.13.1 A.13.1, A.13.2 A.13.1.2	

	5. Pour les réseaux qui ne sont pas de la responsabilité des organes d'exécution et dont l'utilisation ne peut être contractuellement réglée (Internet), il faut mettre en œuvre des mesures de sécurité. 6. Il convient de documenter les structures réseau ainsi que les responsabilités.	A.13.1.2	
2.13.4	**Transfert protégé d'informations** Concernant le transfert d'informations, les organes d'exécution prennent des mesures qui garantissent que les données soient suffisamment protégées conformément aux exigences de protection des données et de sécurité des données (sécurité de l'information, point 2.8.2/2.8.3), indépendamment du fait qu'ils utilisent un réseau propre, un réseau régi par un contrat ou un réseau externe pour l'échange de données. Les organes d'exécution veillent à ce que les différents niveaux de protection (cf. points 2.8.2 et 2.8.3) soient connus des collaborateurs en cas de transfert de données et que ceux-ci utilisent des moyens de transfert correspondants (par ex. courrier électronique crypté).	A.13.2 (A.13.2.1-A.13.2.4)	
2.14	**Achat, développement et maintenance des systèmes d'information** Les organes d'exécution s'assurent que la sécurité fait partie intégrante des systèmes d'information durant l'ensemble de leur cycle de vie. Il convient de prendre en considération les exigences de sécurité spécifiques qui dérivent de la sécurité de l'information et de la protection des données (cf. points 2.5, 2.8.2 et 2.8.3). La documentation SIPD (points 2.8.2 ou 2.8.3) doit être mise à jour en cas de modification. Si aucune modification n'a été apportée au système d'information, l'actualité de la documentation SIPD doit être vérifiée au moins une fois tous les cinq ans. Les exigences qui, selon le point 2.5, s'appliquent aux nouveaux projets sont également valables pour les modifications des systèmes d'information. Cela permet de s'assurer que les exigences de sécurité sont prises en compte lors du développement des systèmes d'information. Il convient également de respecter les exigences du point 2.12, let. a, point 4 concernant la séparation des environnements de	A.14.1 A.14.2 A.14.3	

	développement, de test et d'exploitation, et de garantir la protection des données utilisées pour les tests.		
2.15	**Contrats avec des tiers (relations avec les fournisseurs)** • Si les organes d'exécution concluent des contrats avec des tiers pour la fourniture de prestations qui **impliquent un potentiel accès à des données relevant du droit des assurances sociales ou concernent le traitement de telles données**, ils fixent contractuellement l'ensemble des prescriptions relatives à la protection (devoir de confidentialité, traitement des données, etc.) ainsi que les exigences minimales à respecter et qui concernent concrètement les prestations. Ils incluent également dans le contrat les mesures de contrôle correspondantes ainsi que les peines conventionnelles en cas de violation de ces prescriptions. • En principe, les contrats avec des tiers doivent prévoir que le contrat doive être exécuté par le tiers lui-même, et qu'un transfert (partiel ou total) des obligations assumées est uniquement admissible si les organes d'exécution ont la possibilité de s'y opposer et de résilier le contrat en cas de non-respect de leur vote conformément aux règles du contrat de base. Même en cas de transfert des obligations, il faut s'assurer par des accords que les exigences minimales sont totalement respectées. Cela s'applique expressément à l'obligation de tenir un inventaire (point 2.8.1). • En principe les prestations pour l'exploitation doivent être réalisées sur le territoire national. Il est nécessaire de déclarer et de justifier les prestations pour l'exploitation réalisées à l'étranger. • Il convient de garantir en tout temps qu'aucune donnée personnelle d'assurés n'est traitée à l'étranger, sauf s'il s'agit d'un traitement lié légalement à un échange international de données (par ex. art. 32, al. 3, LPGA ou CIBIL [cf. Accord bilatéral Suisse-UE. Convention AELE. Circulaire sur la procédure pour la fixation des prestations dans l'AVS/AI/PC]).	A.15.1, A.15.2	Voir lien stratégie d'informatique en nuage de l'administration fédérale (si le cloud public dispose de mesures protectrices correspondantes, le traitement de données sensibles est également admis moyennant la communication aux services compétents, par ex le PFPDT pour la Confédération). Voir également l'exemple de la FINMA : Autorité fédérale de surveillance des marchés financiers (FINMA) Suisse - Microsoft Compliance | Microsoft Docs

2.16	**Gestion des incidents relatifs à la sécurité de l'information** Le responsable de la sécurité de l'information s'assure que les notifications concernant des incidents de sécurité en lien avec les systèmes d'information sont adéquatement traitées, documentées et évaluées, dans le but de réduire la probabilité d'occurrence ou les conséquences de futurs incidents. Il dispose d'un plan de réaction et de communication pour les incidents de sécurité, ce qui permet d'assurer que les mesures appropriées sont prises par les personnes compétentes.	A.16.1	
2.17	**Maintien de la sécurité de l'information (gestion de la continuité des activités)** Les organes d'exécution disposent - conformément au besoin de leurs objets protégés des SI (cf. points 2.8.2 et 2.8.3) - de plans testés pour maintenir et restaurer l'exploitation des objets protégés des SI en cas de perturbations, d'urgences et de catastrophes.	A.17.1, A.17.2	
2.18	**Conformité avec les directives** Les organes d'exécution veillent à ce que les lacunes en lien avec les systèmes d'information, identifiées grâce à leur système de contrôle interne, leur gestion de la qualité ou leur gestion du risque (cf. aussi point 2.3) soient comblées, indépendamment du fait qu'elles aient déjà été découvertes lors d'un contrôle relevant du droit de la surveillance.	A.18.1, A.18.2	

Référence au droit sur le thème de la sécurité de l'information

Annexe 1

1. Sources nationales du droit

Les bases légales de la sécurité de l'information (et les thèmes y relatifs de protection des données et de sécurité des données) se trouvent dans différentes sources du droit.

A. Au niveau fédéral

- La Constitution fédérale garantit avec l'art. 13, al. 2 la protection contre l'emploi abusif de données personnelles et oblige en définitive les organes d'exécution, dans l'art. 35, à contribuer à la réalisation de ce droit fondamental.
- La **loi formelle sur la protection des données** (LPD, RS 235.1) et l'ordonnance OLPD (RS 235.11)
    - règlent les aspects formels (définition des données personnelles, des données personnelles sensibles, du profilage, etc.) ;
    - instaurent des restrictions au traitement et à la divulgation de données personnelles (conformité au droit, proportionnalité, conformité au but, exactitude des données, etc.) ;
    - garantissent aux individus certains droits liés aux données (droit d'accès) ;
    - exigent des moyens « organisationnels et techniques » en lien avec la sécurité des données (confidentialité, intégrité, disponibilité).
- La **législation spéciale du droit des assurances sociales**
    - permet grâce à ses normes d'autorisations (en lien avec la LPD) le traitement de données personnelles sensibles (et un profilage) dans les assurances sociales et le flux de données nécessaire à l'utilisation de systèmes d'information ;
    - met en place nouvellement les présentes exigences minimales pour les systèmes d'information d'un point de vue technique et organisationnel ;
    - garantit (aussi en lien avec la PA [172.021]) certains droits d'information individuels et liés à la procédure (par ex. consultation des pièces) ;
- Pour autant qu'il s'agisse de systèmes d'information des autorités fédérales (par ex. la CdC), de nombreuses autres dispositions s'appliquent (LOGA RS 172.10, OIAF RS 172.010.58, ordonnance sur la protection contre les cyberrisques dans l'administration fédérale OPCy RS 120.73 et d'autres dispositions du Centre national pour la cybersécurité NCSC[2]). Une réglementation supplémentaire s'ajoute au cadre juridique avec l'entrée en vigueur de la loi sur la sécurité de l'information (LSI)[12] du 18 décembre 2020.

B. Au niveau des cantons

Des règles cantonales peuvent être déterminantes tant pour la sécurité de l'information que pour la protection des données.

C. Validité de la LPD pour les organes d'exécution

Concernant le champ d'application, il convient d'établir que les organes d'exécution

- doivent appliquer toutes les normes de la législation des assurances sociales. La LPD couvre non seulement les organes d'exécution qui appartiennent à l'administration fédérale, mais aussi les organes d'exécution organisés sous forme d'association, qui sont assimilés aux organes fédéraux ;
- sont soumis à la législation cantonale en matière de protection des données en tant qu'organes d'exécution cantonaux.

2. Normes ISO et leur importance

L'Organisation internationale de normalisation (ISO) est l'association internationale des organisations de normalisation et élabore des normes internationales. Les normes ISO 27001 et 27002 concernent les technologies de l'information et les techniques de sécurité informatique. Elles accordent une place centrale à la gestion de la sécurité de l'information et définissent les exigences qu'un tel système de gestion doit remplir. Ces exigences portent toujours sur des objectifs et des mesures, qui sont numérotés en continu. Cela permet de mettre à disposition un système de numéros de référence.
Comme les technologies de l'information et les techniques de sécurité informatique ne se limitent pas à un thème national, des entreprises, organismes gouvernementaux et organisations à but non lucratif du monde entier s'appuient sur ces normes. Cela a

[12] FF 2020 9665

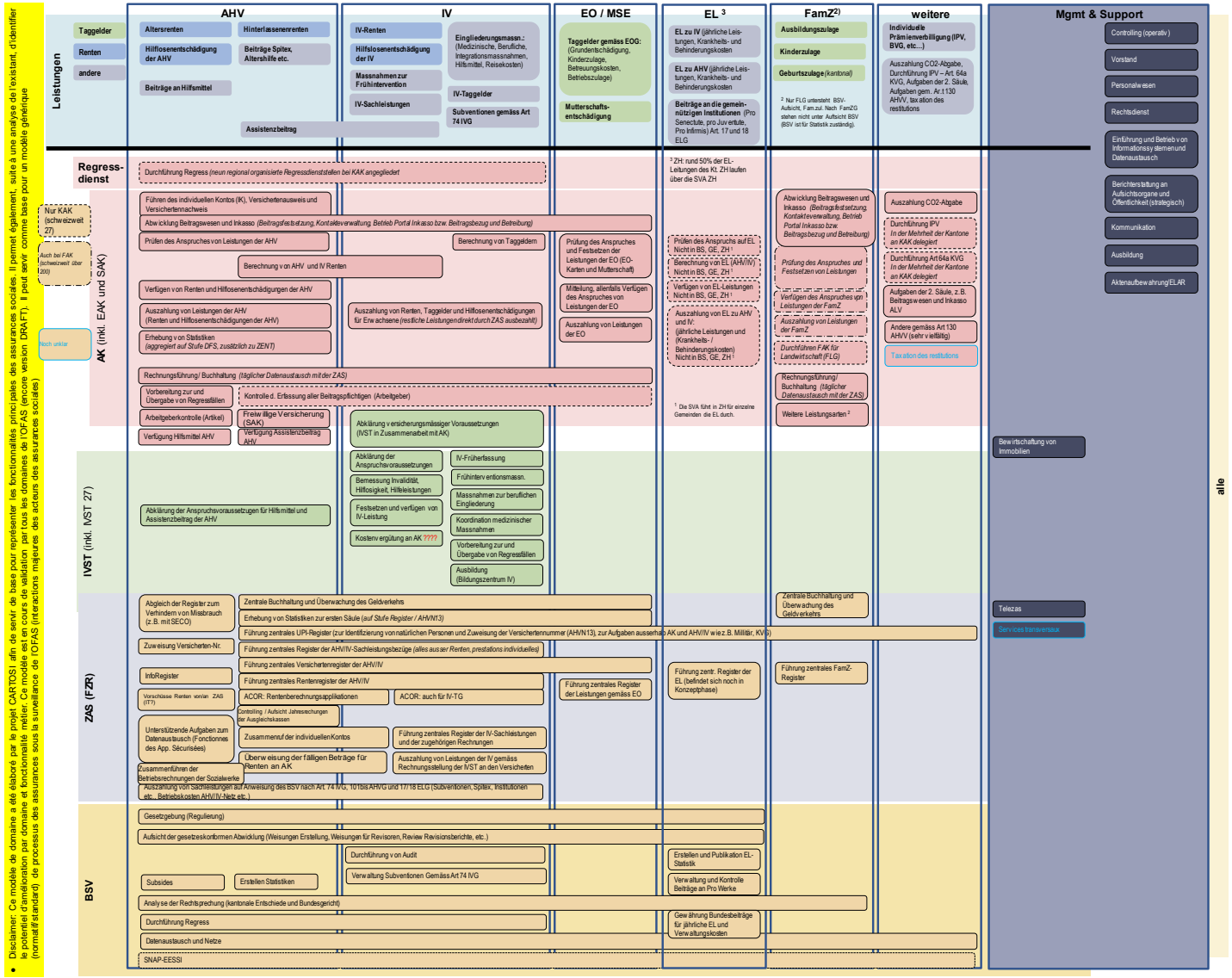
pour conséquence en Suisse que le contenu des normes ISO est intégré dans la législation et sa mise en œuvre. On peut citer comme exemples

- les critères de protection informatique de base dans l'administration fédérale, qui se réfèrent à la norme ISO ;
- la certification, au sens de l'art. 11 LPD (qui est par ex. obligatoire pour le service de réception des données des assureurs maladie conformément à l'art. 59a, al. 6, OAMal[13]), qui dépend en particulier du respect de la norme ISO 27001 (cf. chif. 4 des directives sur les exigences minimales applicables à un système de gestion de la protection des données du 19 mars 2014). Les directives sur les exigences minimales applicables à un système de gestion de la protection des données et ses annexes créent un lien entre les dispositions nationales de protection des données (LPD et OLPD), qui concordent thématiquement avec les normes ISO et la numérotation des normes ISO en se basant sur le système de numérotation ISO (cf. en particulier le chif. 4 des directives et la let. g de l'annexe sur le thème de la sécurité des données conformément à l'art. 7 LPD). Les mesures supplémentaires reposant uniquement sur la législation nationale sont explicitement structurées de manière analogue aux normes ISO 27002.

[13] Ordonnance du 27 juin 1995 sur l'assurance-maladie, RS 832.102

Modèle de domaine technique 1er pilier/AF (état févr. 2021)

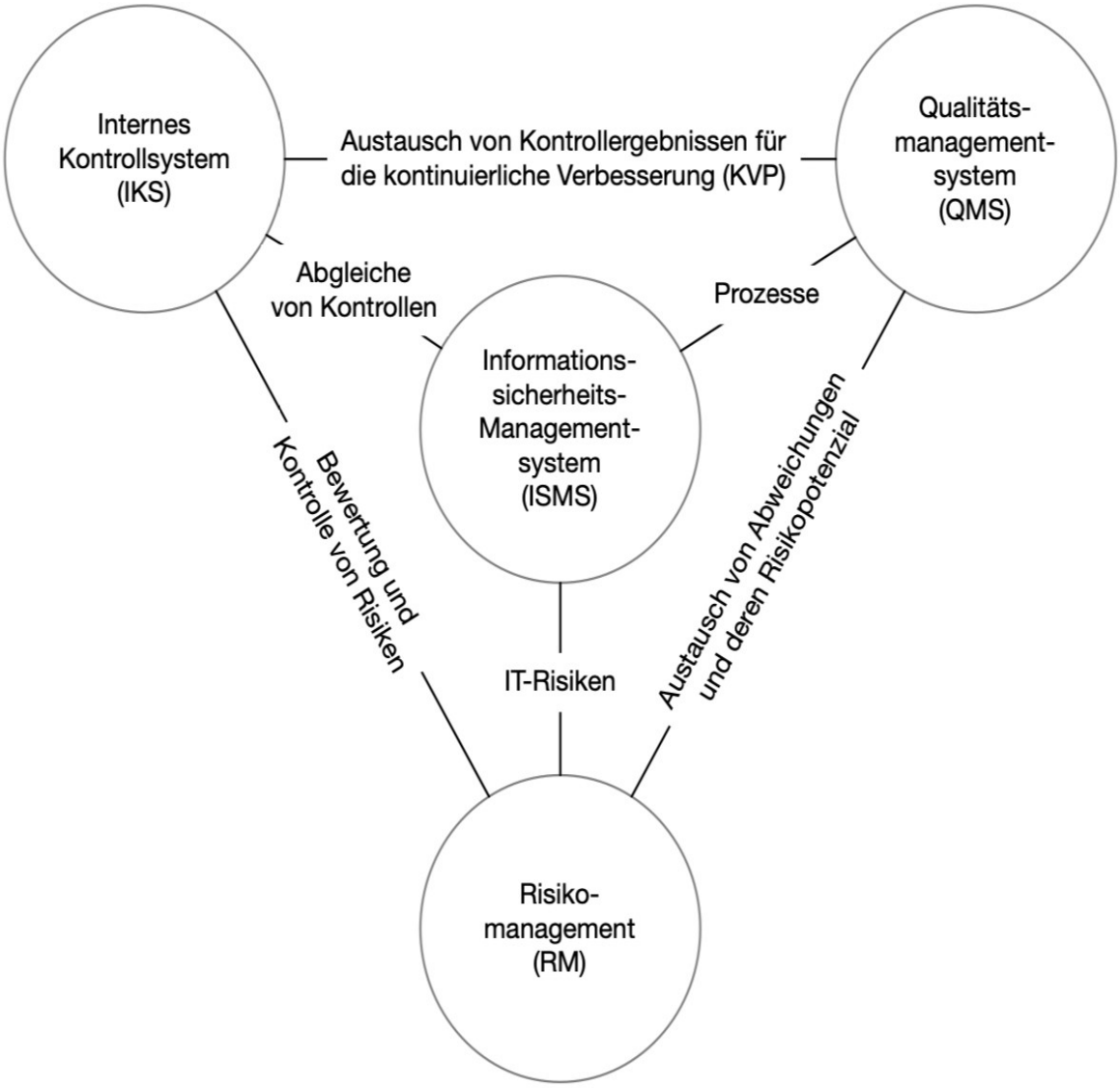
Annexe 2



Disclaimer: Ce modèle de domaine a été élaboré par le projet CARTOS! afin de servir de base pour représenter les fonctionnalités principales des assurances sociales. Il permet également, suite à une analyse de l'existant, d'identifier le potentiel d'amélioration par domaine et fonctionnalité métier. Ce modèle est en cours de validation par tous les domaines de l'OFAS (encore version DRAFT). Il peut servir comme base pour un modèle générique (normatif standard) de processus des assurances sous la surveillance de l'OFAS (interactions majeures des acteurs des assurances sociales)

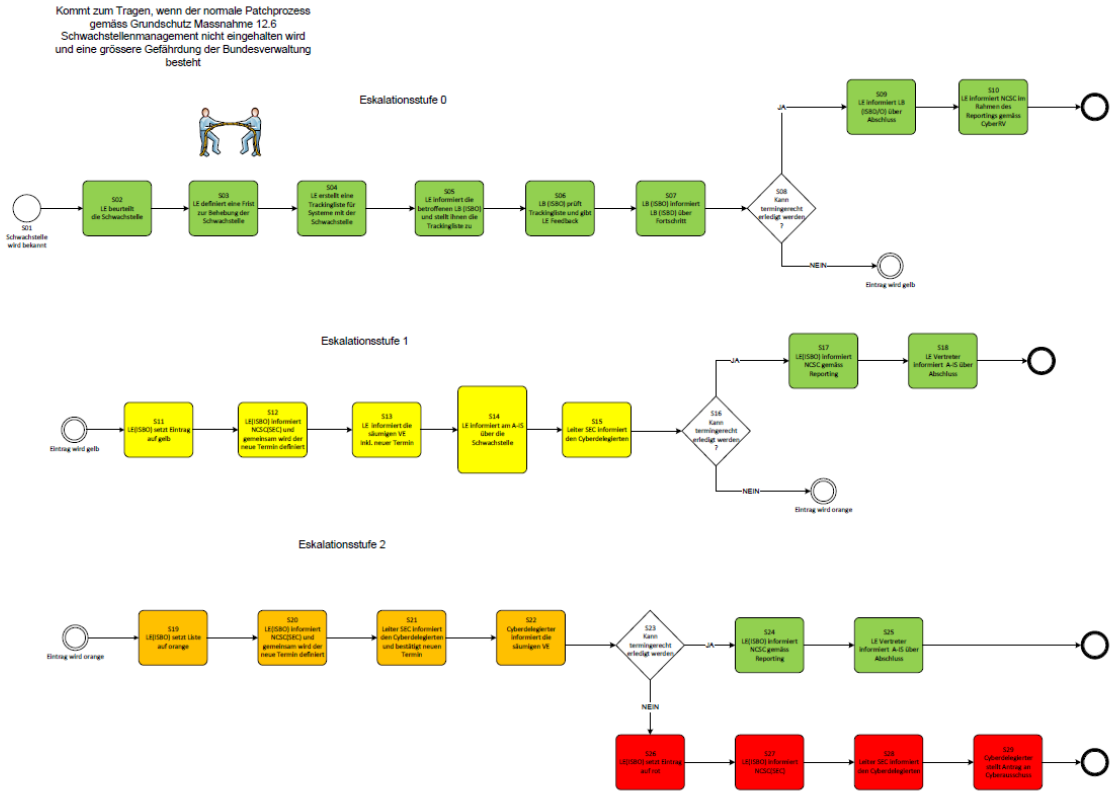
Annexe 3

Source : eAVS/AI information sur le concept de sécurité



Annexe 4

Exemple de procédure de gestion d'incident de sécurité selon le chif. 2.3 ; le processus doit contenir les décisions d'information de l'OFAS et du PFPDT (l'exemple définitif suivra).



Annexe 5

Modèle de documentation de base SIPD

A. Schéma de clarification des conditions-cadres juridiques selon point 2.8.2, let. a

Remarques préliminaires générales/explications

Chaque organe d'exécution est l'organe d'une assurance sociale régie par le droit fédéral et, dans ce contexte, il est habilité et tenu d'exécuter les tâches légalement prévues (principe de légalité). La loi spécifique correspondante (LAVS, LAI, etc.) sert de base à ses activités. S'il met en place des systèmes d'information afin de remplir ses tâches, des éléments juridiques d'autres branches s'ajoutent au cadre de la loi spécifique. La LPGA s'applique, d'une part, par exemple à l'assistance administrative (art. 32 LPGA), l'obligation de garder le secret (art. 33 LPGA) et l'échange électronique de données (art. 76bis du projet de LPGA). Il faut, d'autre part, tenir compte des dispositions sur la sécurité de l'information ou sur la protection et la sécurité des données issues de la LPD ou de la législation cantonale. Celles-ci s'appliquent régulièrement à la gestion des données et à leur sécurité de la façon suivante :

- Les organismes fédéraux actifs dans le 1er pilier (par ex. la Caisse fédérale de compensation ou la Caisse suisse de compensation) ainsi que les organes d'exécution pris en considération par la LPD en tant qu'« organes fédéraux » (donc tous les organes d'exécution qui ne sont pas cantonaux) doivent par exemple respecter les dispositions sur le registre de leurs activités de traitement (art. 12 nLPD), sur la réalisation d'une analyse d'impact relative à la protection des données (art. 22 nLPD) ou sur l'annonce de violations de la sécurité des données (art. 24 nLPD).
- Pour autant que la législation cantonale en matière de protection des données prévoie des règles similaires, les organes d'exécution cantonaux doivent vérifier quelles obligations en découlent.

Schéma modèle pour les conditions-cadres juridiques et la clarification de la conformité au droit du traitement des données

	Question/thème	**Base légale**	**Conséquence, exemple**
1	Respect des principes de protection des données : • licéité du traitement conformément à l'art. 6, al. 1, nLPD ; • proportionnalité et adéquation de l'acquisition et du traitement des données, dans le respect du principe de bonne foi et de l'art. 6, al. 2 et 3, nLPD	L'art. 49b LAVS et le nouvel art. 49f du projet de LAVS autorisent les organes d'exécution à traiter des données personnelles, y compris des données sensibles, et à effectuer du profilage, pour autant que cela soit nécessaire pour leurs tâches attribuées par la loi. Cette autorisation est également valable pour tous les autres organes d'exécution (art. 66a LAI ou art. 66 du projet de LAI, art. 25 LAFam, art. 25, al. 2, LFA, art. 29 LAPG, art. 26 LPC). Une base légale adéquate suffit pour le domaine d'activité des organes d'exécution (art. 34 ss nLPD)	Il faut vérifier dans la documentation de base SIPD si le système d'information sera véritablement employé pour l'exécution d'une tâche attribuée par la loi, s'il est adéquat et s'il est adapté à l'exécution de la tâche. **Licéité** : indications sur les bases légales du traitement des données (par ex. art. 49b LAVS) **Adéquation** : quelle est la tâche légale exécutée (loi ou ordonnance) ? **Proportionnalité :** est-il possible d'atteindre le même but avec un traitement moins intense des données, tout en garantissant la même qualité ?

	Question/thème	Base légale	Conséquence, exemple
			Bonne foi : si une personne concernée ne doit s'attendre en aucun cas au traitement de ses données dans le cas d'espèce, le principe est violé. **Exemple de classement d'une application de courrier électronique d'une caisse de compensation AVS privée dans la documentation de base SIPD :** Les courriers électroniques sont régulièrement utilisés par les assurés pour obtenir des renseignements ou des conseils au sens de l'art. 27 LPGA. Les données utilisées peuvent être sensibles. Il convient de tenir compte de cet aspect lors de la classification (cf. schéma, let. C et D) d'un point de vue technique. Le traitement des données doit **en principe être licite** en raison de l'art. 49a (à l'avenir 49f du projet de LAVS). Pour autant que seules les données pertinentes pour le cas particulier soient indiquées dans les courriers électroniques, **l'adéquation, la proportionnalité et le principe de bonne foi sont assurés.**
2	Entrée de données (acquisition de données), sortie de données (divulgation de données) et obligation de garder le secret	Tant l'acquisition de données que leur divulgation font l'objet de restrictions juridiques particulières et toute acquisition découle d'une divulgation. Formellement, la divulgation de données constitue aussi un traitement (art. 5, let. d, nLPD). L'acquisition de données sera certes restreinte par la nLPD (dans l'art. 6, al. 3 et l'art. 19), cependant ces restrictions sont superflues en présence d'une base légale correspondante (en particulier art. 20 nLPD). Dans le cadre de l'obligation de collaboration et d'annonce, une partie de l'entrée de données est toutefois souvent réglée dans les lois régissant les assurances sociales. Il faut y ajouter l'envoi automatisé de notifications	Il convient de vérifier dans la documentation de base SIPD si l'entrée et la sortie de données sont juridiquement admissibles. Pour les systèmes d'information qui prévoient une entrée et/ou une sortie automatique de données, il est nécessaire de déterminer et de documenter la base légale. **Exemple de classement d'une application de courrier électronique d'une caisse de compensation AVS privée dans la documentation de base SIPD :** Les courriers électroniques servent exclusivement au transfert de données au cas par cas. L'utilisateur

	Question/thème	Base légale	Conséquence, exemple
		en raison de réglementations relatives à certains systèmes d'information (par ex. notification d'état civil à l'AVS). Pour terminer, la LPGA garantit l'assistance administrative dans des cas particuliers. L'art. 36, al. 1, nLPD dispose qu'il faut prévoir à nouveau une base légale pour la divulgation de données (comme pour le traitement des données). Les différentes lois régissant les assurances sociales règlent en détail la divulgation de données dans leurs propres catalogues sur la divulgation des données, en distinguant notamment les sorties de données au cas par cas des processus de masse. Ce faisant, elles dérogent régulièrement à l'obligation générale de garder le secret prévue par l'art. 33 LPGA.	formé concerné doit vérifier la validité juridique de l'entrée et de la sortie de données. Il faut s'assurer que les utilisateurs pourront recevoir une formation correspondante et seront en mesure de clarifier l'identité du destinataire des données avec l'aide éventuelle de mesures techniques et organisationnelles.
3	Exactitude et rectification des données (art. 6, al. 5 et art. 41, al. 2, nLPD)	La LPD exige lors du traitement de données • une vérification de l'exactitude des données ; • des mesures adaptées pour garantir l'exactitude des données ; • la rectification des données erronées.	Il est nécessaire d'analyser dans la documentation de base SIPD quelles sont les garanties de l'exactitude des données, quelles sont les possibilités de confirmer la plausibilité et les méthodes de vérification, et comment sont faites les corrections nécessaires. Il convient d'établir des processus à cet effet. **Exemple de classement d'une application de courrier électronique d'une caisse de compensation AVS privée dans la documentation de base SIPD :** Les données utilisées dans les courriers électroniques sont liées au cas particulier et ne sont systématiquement pas vérifiables. Il appartient à l'utilisateur, si nécessaire, de vérifier leur caractère plausible par une clarification du cas spécifique. Il faut s'assurer que les utilisateurs reçoivent une formation correspondante et utilisent les données correctes avec l'aide éventuelle de mesures techniques et organisationnelles.

	Question/thème	Base légale	Conséquence, exemple
4	Droit d'accès (art. 25 nLPD)	L'art. 25 nLPD octroie un droit d'accès à chaque personne, qui oblige le responsable à fournir des informations. Ce droit d'accès est limité par les art. 26 et 27 nLPD. La personne peut en outre demander le transfert des données, encore une fois sous certaines conditions (art. 28 et 29 nLPD).	Il convient d'analyser dans la documentation de base SIPD comment l'ensemble des données à attribuer à une personne peuvent être obtenues dans le système d'information. Le processus de gestion des demandes d'accès doit être documenté. Il faut clarifier dans la documentation de base SIPD si le système d'information peut contenir des données sur la santé qui, avec le consentement de la personne concernée, sont transmises par le professionnel de la santé désigné par celle-ci (art. 25, al. 3, nLPD). **Exemple de classement d'une application de courrier électronique d'une caisse de compensation AVS privée dans la documentation de base SIPD :** Il faut s'assurer, dans le cadre de la documentation de base SIPD, qu'il est possible d'accéder aux courriers électroniques d'une personne déterminée. On peut également s'en assurer par la définition d'un processus pour un autre système d'information ou d'une gestion d'entreprise. Il faut y faire référence dans la documentation de base SIPD sur l'application de courrier électronique.
5	Clarification de l'enregistrement dans le registre ou notification à une autorité de protection des données	Les organismes fédéraux actifs dans le 1er pilier (par ex. la Caisse fédérale de compensation ou la Caisse suisse de compensation) ainsi que les organes d'exécution pris en considération par la LPD en tant qu'« organes fédéraux » (donc tous les organes d'exécution qui ne sont pas cantonaux) doivent respecter les dispositions sur le registre de leurs activités de traitement et déclarer leurs registres au PFPDT (art. 12 nLPD).	

B. Modèle de classification des exigences de disponibilité (selon point 2.8.2, let. b)

	Question ou exigence	**Critère**	**Besoin de protection accru ? > documentation SIPD élargie selon le point 2.8.3 nécessaire ?** *(analyses du risque et exigences de sécurité notamment, à la place de la documentation)*
1	Durée max. admissible par panne	Durée de panne max. 2 heures	**Oui**
		Durée de panne de plus de 2 heures	**Non**
2	Perte de données max. par panne	Perte de données de moins de 1 heure	**Oui**
		Perte de données de plus de 1 heure	**Non**
3	Processus critique/pertinent pour l'exploitation ? (en raison du point 2.8.2, chif. 2, let. b) : faut-il prendre des mesures de prévention contre les catastrophes pour les objets protégés ?	Mesures de prévention contre les catastrophes nécessaires	**Oui**
		Mesures de prévention contre les catastrophes pas nécessaires	**Non**

C. Modèle pour les exigences de confidentialité (selon point 2.8.2, let. c)

Il est nécessaire de classifier les données dans la documentation de base SIPD pour déterminer un éventuel besoin de protection supplémentaire et donc la nécessité d'une documentation élargie (point 2.8.3).

Question ou exigence	**Critère**	**Besoin de protection accru ? > documentation SIPD élargie selon le point 2.8.3 nécessaire ?** *(analyses du risque et exigences de sécurité notamment, à la place de la documentation)*	**Mesures de protection**
Les données sont-elles traitées conformément à la législation sur la protection des données ? Si oui, quel type de données personnelles est concerné ?	Aucune donnée personnelle	Non	Définition des mesures de protection de base actuelles
	Données personnelles	Non	Définition des mesures de protection actuelles
	Données personnelles sensibles (art. 5, let. c, nLPD) ?	Oui Oui	Définition des mesures de protection particulières

	Et/ou profilage (évaluation automatisée ; cf. art. 5, let. f, nLPD) ?[14] Si oui profilage : à risque élevé (cf. art. 5, let. g, nLPD) ?	Oui	
Dans quel niveau de classification se trouvent les données des objets protégés ?	Public Interne Confidentiel Hautement confidentiel	Non Non Oui Oui	La classification devrait être définie dans une prochaine version.

[14] Profilage : conformément au message du 15 septembre 2017 du Conseil fédéral concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, on entend par profilage : « Le profil de la personnalité (qui n'est plus terminologiquement défini par la loi)(qui n'est plus terminologiquement défini par la loi) est le résultat d'un traitement et traduit ainsi quelque chose de statique. À l'inverse, filage désigne une forme particulière de traitement, et constitue donc un processus dynamique. Ce dernier est par ailleurs toujours orienté vers une finalité particulière. Compte tenu des avis recueillis lors de la consultation, le terme de profilage est adapté, sur le fond, à la terminologie européenne et ne recouvre plus que le traitement automatisé de données personnelles. Il est défini comme l'évaluation de certaines caractéristiques d'une personne sur la base de données personnelles traitées de manière automatisée, afin notamment d'analyser ou de prédire son rendement au travail, sa situation économique, sa localisation, sa santé, son comportement, ses préférences ou ses déplacements. L'analyse de ces caractéristiques peut par exemple avoir pour but de déterminer si une personne est indiquée pour une certaine activité.L'analyse de ces caractéristiques peut par exemple avoir pour but de déterminer si une personne est indiquée pour une certaine activité. Autrement dit, le profilage se caractérise par le fait qu'on procède à une évaluation automatisée de données personnelles afin de pouvoir évaluer, d'une manière également automatisée, les caractéristiques de la personne. On est ainsi en présence d'un profilage uniquement lorsque le processus d'évaluation est entièrement automatisé. On entend par évaluation automatisée toute évaluation fondée sur des techniques d'analyse informatisées. Le recours à des algorithmes est possible, mais non constitutif du profilage. En revanche, l'évaluation automatisée des données est indispensable. La simple accumulation de données n'est pas assimilée au profilage. L'évaluation automatisée vise en particulier à analyser ou à prédire certains comportements de la personne. La loi cite quelques exemples de caractéristiques personnelles, telles que le rendement au travail, la situation économique ou la santé. »

B. Modèle de classification des exigences d'intégrité et de traçabilité (selon point 2.8.2, let. d) :

Classification	**Description**	**Mesures**	**Documentation SIPD élargie selon le point 2.8.3 nécessaire ?**
Intégrité normale	Pour les domaines des technologies de l'information et de la communication (TIC) qui sont classés dans le niveau « intégrité normale », on peut renoncer à des mesures particulières pour conserver l'intégrité.	Les mesures générales pour les appareils et les équipements d'entreprise (points 2.11.2 et 2.12.2) doivent garantir l'« intégrité normale ».	Non
Intégrité sécurisée	Pour les domaines des TIC qui sont classés dans le niveau « intégrité sécurisée », on doit mettre en place des mesures de protection contre les modifications par des tiers non autorisés.	La documentation de base SIPD permet d'examiner l'importance des conséquences de modifications incorrectes apportées aux systèmes d'information (nouvelle version). Les critères pour évaluer l'importance des conséquences sont par exemple la perturbation de l'exécution des tâches, les impacts externes négatifs, les conséquences financières pour l'assurance.	Oui Afin de pouvoir corriger les conséquences de possibles erreurs, il faut tester et documenter les modifications de manière approfondie (selon l'importance des possibles conséquences) et les effectuer de sorte qu'elles correspondent aux exigences des projets, en particulier aux critères de gestion de la qualité et du risque applicables (cf. point 2.5, point 1 et point 2.14, al. 3).
Intégrité vérifiable	Pour les domaines des TIC qui sont classés dans le niveau « intégrité vérifiable », on mettra en œuvre des fonctionnalités supplémentaires qui déterminent et constatent les violations de l'intégrité.		La version définitive suivra.
Intégrité signée	Pour les domaines des TIC qui sont classés dans le niveau « intégrité signée », on mettra en place en plus des signatures numériques.		La version définitive suivra.

E. Conservation de données

Concernant la conservation de données, il convient de décrire au moins les éléments suivants :

- informations géographiques (lieu en Suisse, avec adresse) ;
- organisation responsable ;
- mention du responsable de la sécurité de l'information

F. Description de l'objet protégé/du projet

- Objectif et but
- Processus soutenus
- Type et étendue des données
- Utilisateurs
- Quantification de l'utilisation

G. Obligation de registre/d'annonce

Selon le point 2.8.1, il existe en principe une obligation d'inventaire pour tous les systèmes d'information. Une obligation de registre s'applique également, conformément à l'art. 12 nLPD. Cette dernière vise les organes fédéraux/organes d'exécution (tous sauf les organes d'exécution cantonaux), tout comme l'obligation d'annonce au PFPDT. Une éventuelle obligation cantonale de registre et d'annonce s'applique aux organes d'exécution cantonaux. La documentation de base du SIPD doit déterminer si et quelles obligations de registre et d'annonce s'appliquent et doit documenter la manière dont ces obligations sont remplies.

H. Nécessité d'une analyse d'impact relative à la protection des données

Conformément au message du 15 septembre 2017 du Conseil fédéral concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales[15], l'analyse d'impact relative à la protection des données est un instrument visant à identifier et évaluer les risques qui peuvent exister pour les personnes concernées en raison de certains traitements de données. Cette analyse doit permettre de définir, le cas échéant, des mesures adéquates pour gérer ces risques pour les personnes concernées.

La documentation de base du SIPD doit en premier lieu déterminer s'il existe un besoin à cet égard.

La réglementation de la nLPD (art. 22) s'applique ici aussi aux organes d'exécution (sauf les organes d'exécution cantonaux). Une éventuelle obligation cantonale d'analyse d'impact relative à la protection des données s'applique aux organes d'exécution cantonaux.

Il convient donc dans un premier temps de fixer dans la documentation de base si les normes sur l'analyse d'impact entrent en considération. **Les organes d'exécution des cantons** déterminent la nécessité d'une analyse d'impact relative à la protection des données dans la documentation de base en fonction de la législation cantonale correspondante.

La documentation de base du SIPD doit, **sur la base des autres clarifications conformément au point 2.8.2, chif. 2, let. a-g**, expressément indiquer s'il existe une nécessité de procéder à une analyse d'impact relative à la protection des données. Les aspects suivants sont déterminants à cet égard :

- Existe-t-il un traitement particulièrement poussé de données sensibles ?
- De nouvelles technologiques sont-elles utilisées ?
- Le traitement de données décrit implique-t-il un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées (cf. art. 22, al. 1 à 3, nLPD) ?
- Est-il prévu de prendre des mesures déjà connues ou à développer pour protéger la personnalité et les droits fondamentaux°?

[15] Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales (admin.ch), FF 2017 6565

I. Attribution à un groupe de protection

Les organes d'exécution disposent d'une définition des groupes de protection (en général 3 ou 4) qui tient compte des différents besoins de protection. Il convient de procéder à une attribution en fonction des résultats selon le point 2.8.2, chif. 2.

Annexe 6

Modèle pour la documentation SIPD élargie selon le point 2.8.3

a. **Résumé des événements pertinents de la documentation de base SIPD**
Le résumé sert de base pour le concept SIPD avec **analyse du risque** et s'étend au classement des objets protégés du point de vue de la confidentialité, de la disponibilité, de l'intégrité/de la traçabilité, de la conservation des données, de la description de l'objet protégé, des résultats portant sur le registre des activités de traitement (le cas échéant avec annonce au PFPDT ou au conseiller à la protection des données) et sur l'analyse d'impact relative à la protection des données.

b. Description sécuritaire du système
Description détaillée des éléments de sécurité issus du système, des applications, des données existantes et traitées, et des processus y relatifs.

b.1 Interlocuteurs/responsabilités

Responsable	Nom
Responsable application	
Propriétaire des données	
Fournisseur de prestations FP (exploitant du système)	
Responsable de projet de l'organe d'exécution	
Interlocuteur chez le FP	
Responsable de la sécurité de l'information	
Cercle d'utilisateurs	
Autres services concernés	

b.2 Description de l'ensemble du système
Description des fonctions de sécurité comme le contrôle des accès (cf. point 2.9), la sécurité d'exploitation (cf. point 2.12) et les prestations de tiers (cf. point 2.15).
Il est également possible de faire référence à la documentation correspondante (par ex. sécurité et documentation du réseau, cf. 2.13.3).

La description doit offrir à une personne externe une vue d'ensemble en restant à la fois compréhensible et claire.

b.3 Description des données à traiter
Description des données et des structures (par ex., bases de données utilisées) et détermination de la licéité du traitement de données prévu conformément à l'annexe 5, let. A, en particulier :
- respect d'une éventuelle obligation d'annonce au responsable de la protection des données du canton ou au PFPDT ;
- élaboration d'un règlement de traitement
  Vous trouverez de l'aide à cet égard dans le modèle https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/dokumentation/vorgaben/prozesse/p042/P042-Hi04-Bearbeitungsreglement_V2-1-f.docx.download.docx/P042-Hi04-Bearbeitungsreglement_V2-1-f.docx ainsi que dans l'ordonnance relative à la LPD et sur le lien *Guide relatif aux mesures techniques et organisationnelles de la protection des données*
  Le règlement du traitement doit respecter les prescriptions d'archivage de l'OFAS (cf. DGD)

b.4 Esquisse d'architecture/matrice de communication

Le concept contient une esquisse d'architecture et une matrice de communication, à défaut de quoi il faut faire référence au document en vigueur correspondant.

b.5 Description de la technologie sous-jacente
Description des technologies utilisées comme la plateforme serveur, le(s) système(s) d'exploitation, l'environnement système, les réseaux utilisés, les fonctions cryptographiques, etc. Elles doivent être décrites avec exhaustivité et de manière compréhensible et claire pour une personne externe.
À défaut de cela, il faut faire référence au document correspondant actuellement en vigueur

c. Analyse du risque (éventuellement avec analyse d'impact relative à la protection des données), mesures de protection et risque résiduel

Le concept SIPD renseigne sur le risque résiduel qui subsiste après une analyse du risque et les mesures de protection prises en compte. Pour autant que la nécessité d'une analyse d'impact relative à la protection des données ait été déterminée dans la documentation de base du SIPD, l'analyse du risque tient compte du risque (élevé) pour la personnalité ou les droits fondamentaux des personnes concernées en raison

- de l'utilisation d'une nouvelle technologie ;
- de l'ampleur du traitement de données personnelles sensibles ;
- de la nature, des circonstances et du but du traitement des données.

Les facteurs de risques pertinents concernant les conséquences en matière de disponibilité, de confidentialité, d'intégrité et de traçabilité sont évalués dans l'analyse du risque. Les résultats sont présentés sous forme de liste des risques évalués et de matrice du risque.

Analyse d'impact relative à la protection des données
L'analyse contient, conformément à la loi (art. 22, al. 3, nLPD)

- une description du traitement envisagé ;
- une évaluation des risques pour la personnalité ou les droits fondamentaux des personnes concernées ;
- les mesures prévues pour protéger la personnalité et les droits fondamentaux.

Si, sur la base de l'analyse, il ressort qu'un traitement poussé de données personnelles sensibles a lieu, l'analyse d'impact doit être intégrée à l'analyse du risque. Il faut évaluer les problèmes qui viennent des traitements concrets en lien avec
La protection de la personnalité (droit privé ; art. 28 CC)
La personnalité englobe toutes les valeurs physiques, psychiques, morales et sociales d'une personne qui lui sont attribuées en vertu de son existence.[16] Il existe donc un vaste champ de possibles violations, et il faut évaluer l'importance du risque que la personne concernée subisse une atteinte et les mesures qui peuvent éventuellement l'éviter.

Exemple : risque que des personnes non autorisées découvrent des atteintes à la santé, ce qui constitue en soi déjà une atteinte morale, mais altérerait également les chances sur le marché du travail si l'information parvenait à un possible employeur (et causerait des dommages financiers).

Mesures possibles : le consentement des personnes concernées est systématiquement recueilli avant la transmission de données à un employeur.

La protection des droits fondamentaux (de droit public)
Les droits fondamentaux sont définis aux art. 7 à 35 de la Constitution fédérale. Il est nécessaire d'évaluer, en lien avec les systèmes d'information, l'ampleur du risque d'une atteinte aux droits fondamentaux en raison d'un traitement de données et les mesures pouvant être prises pour y remédier.

[16] Fey Marco, in : Baeriswyl Bruno/Pärli Kurt (ed.), Datenschutzgesetz (DSG), Berne 2015, Art. 1 N 16)

Exemple : égalité des droits avec l'interdiction de discrimination conformément à l'art. 8 Cst.

Risque que des personnes non autorisées apprennent le mode de vie d'une certaine personne (par ex. partenariat pour un couple de même sexe) et que celle-ci subisse de la discrimination sur le lieu de travail.

Mesures possibles : le consentement des personnes concernées est systématiquement recueilli avant la transmission de données à un employeur.

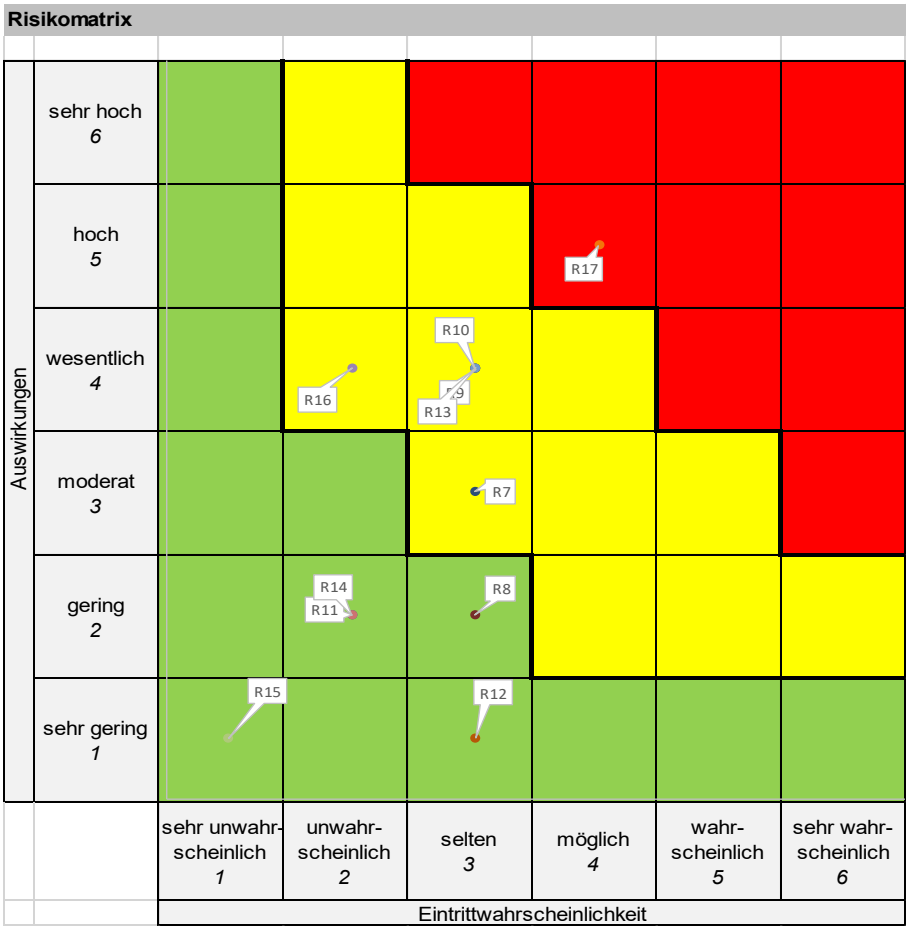
Aides/informations supplémentaires

Fiche d'information sur l'analyse d'impact relative à la protection des données du canton de SG (en allemand)

ou

Https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/publikationen/formulare-merkblaetter/formular_dsfa.docx (en allemand)

- Matrice des risques



L'analyse de risque détaillée peut être réalisée sur la base d'un fichier Excel du NCSC. L'analyse doit déboucher sur la définition de mesures de protection et la description des risques résiduels. Les risques qui ne sont pas réduits, ou qui le sont insuffisamment (marqués en rouge ou en jaune dans la matrice des risques) doivent être mentionnés dans le concept SIPD. Si, lors de l'analyse d'impact relative à la protection des données, il subsiste des risques importants pour la personnalité ou les droits fondamentaux des personnes concernées, il est nécessaire de consulter le PFPDT conformément à l'art. 23 nLPD.

La décision d'encourir les risques résiduels connus revient à l'organe d'exécution. Les risques résiduels doivent être inclus dans le système de gestion des risques (cf. point 2.3, chif. 1.c).

d. Rétablissement de l'activité/plan d'urgence (source : modèle SIPD du NCSC)

Il convient d'élaborer un plan d'urgence pour un objet à protéger compatible avec des processus d'affaires critiques. Le plan d'urgence décrit la planification des cas d'urgence et la poursuite des activités liées à l'objet à protéger afin de garantir le maintien et le rétablissement des activités dans les situations extraordinaires. Le plan d'urgence doit également comporter un contrôle des accords de niveau de service (SLA) conclus avec le fournisseur de prestations et assurer leur mise à jour si des modifications s'avèrent nécessaires.
Il convient dans tous les cas de faire référence aux documents BCM (cf. point 2.17) au niveau de l'organe d'exécution.

e. Respect/contrôle/adoption des mesures de protection

Il est nécessaire de décrire comment le respect des mesures de protection sera contrôlé. Cela vaut pour les révisions enregistrées et non enregistrées ainsi que pour les contrôles des activités en matière de sécurité de l'information dans le projet, puis dans l'exploitation.

Kurzbeschreibung	Elektronisches Datenaustauschsystem zwischen den Sozialversicherungsträgern in der Schweiz und mit der EU. Electronic Exchange of Social Security Information (EESSI).
Umgebung	ABN
URL(s)	https://backend-rina02-a.bsv.admin.ch/cms/index.php?id=rina-home-page
Scan-User	CHA021cBaertschi
Test-Szenario 1	User Admin
Datum des Tests	26.06.2019
Datum der Analyse	27.06.2019

ssus

ıtrôles

4.1.2).

WAWS Bericht - Webinspect

Résumé des contrôles réalisés (qui, quand, quoi, résultat).

f. Mise hors service

Décrit les points à observer lors de la mise hors service en tenant compte des prescriptions d'archivage (cf. directives DGD).

Liste des abréviations utilisées

Abréviation	**Désignation**	**Lien**
Al.	Alinéa	
AVS	Assurance-vieillesse et survivants	
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants, RS 831.10	https://www.fedlex.admin.ch/eli/cc/63/837_843_843/fr
RAVS	Règlement sur l'assurance-vieillesse et survivants, RS 831.101	https://www.fedlex.admin.ch/eli/cc/63/1185_1183_1185/fr
CC	Caisse de compensation	
Art.	Article	
LPGA	Loi fédérale sur la partie générale du droit des assurances sociales, RS 830.1	https://www.fedlex.admin.ch/eli/cc/2002/510/fr
AV	Responsable application	
FF	Feuille fédérale	
BCM	Gestion de la continuité des activités	
OIAF	Ordonnance sur l'informatique et la télécommunication dans l'administration fédérale, RS 172.010.58	https://www.fedlex.admin.ch/eli/cc/2011/844/fr
OFIT	Office fédéral de l'informatique et de la communication	
Cst.	Constitution fédérale de la Confédération suisse, RS 101	https://www.fedlex.admin.ch/eli/cc/1999/404/fr
AC	Autorité de certification	
OE	Organes d'exécution	
LPD	Loi fédérale sur la protection des données, RS 235.1	https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/fr#a5
eAVS/AI	Association des organes d'exécution de l'AVS et de l'AI	https://www.eahv-iv.ch/fr/
Projet LAVS	Projet de révision de la LAVS (FF 2020 107) conformément au message concernant la révision de la loi fédérale sur l'assurance-vieillesse et survivants (Modernisation de la surveillance dans le 1er pilier et optimisation dans le 2e pilier de la prévoyance vieillesse, survivants et invalidité (FF 2020 1)	
Projet d'art.	Projet d'article	
eCH	Association de développement de normes dans la cyberadministration	https://www.ech.ch/fr
PFPDT	Préposé fédéral à la protection des données et à la transparence	https://www.edoeb.admin.ch/edoeb/fr/home.html
PC	Prestations complémentaires	

Abréviation	Désignation	Lien
LPC	Loi fédérale sur les prestations complémentaires à l'assurance-vieillesse, survivants et invalidité, RS 831.30	https://www.fedlex.admin.ch/eli/cc/2007/804/fr.
APG	Allocations pour perte de gain	
LAPG	Loi sur les allocations pour perte de gain, RS 834.1	https://www.fedlex.admin.ch/eli/cc/1952/1021_1046_1050/fr
LAFam	Loi fédérale sur les allocations familiales, RS 836.2	https://www.fedlex.admin.ch/eli/cc/2008/51/fr
OAFam	Ordonnance fédérale sur les allocations familiales, RS 836.21	https://www.fedlex.admin.ch/eli/cc/2008/52/fr
LFA	Loi fédérale sur les allocations familiales dans l'agriculture, RS 836.1	https://www.fedlex.admin.ch/eli/cc/1952/823_843_839/fr
SCI	Système de contrôle interne	
SI	Système d'information	
Responsable de la sécurité de l'information	Responsable de la sécurité de l'information (au sens des présentes recommandations)	
SIPD	Sécurité de l'information et protection des données	
LSI	Loi fédérale sur la sécurité de l'information du 18 décembre 2020	FF 2020 9665
SGSI	Système de gestion de la sécurité de l'information	
ISO	Organisation internationale de normalisation	
ISO 27001	ISO/IEC 27001, 2013 + Cor 1:2014) Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences (avec annexe 1 normative concernant les objectifs et mesures de références, qui dérivent de la norme ISO/IEC 27002)	
ISO 27001	ISO/IEC27002 : 2013 + Cor 1:2014 + Cor 2:2015, Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information	
TIC	Technologies de l'information	
AI	Assurance-invalidité	
LAI	Loi fédérale sur l'assurance-invalidité, RS 831.20	https://www.fedlex.admin.ch/eli/cc/1959/827_857_845/fr
COGSC	Circulaire sur l'obligation de garder le secret et sur la communication des données dans le domaine de l'AVS/AI/APG/PC/AFA/AF	https://sozialversicherungen.admin.ch/fr/d/6435#
OAMal	Ordonnance du 27 juin 1995 sur l'assurance-maladie, RS 832.10	https://www.fedlex.admin.ch/eli/cc/1995/3867_3867_3867/fr

Abréviation	**Désignation**	**Lien**
FP	Prestataire de services	
NCSC	Centre national pour la cybersécurité	Procédure de sécurité (admin.ch)
nLPD	Révision de la loi fédérale sur la protection des données (nLPD) du 25 septembre 2020 (FF 2020 7397)	FF 2020 7397 - Loi fédérale sur la protection des données (loi sur la protection des données, LPD) (admin.ch)
nOLPD	Nouvelle ordonnance sur la nouvelle loi sur la protection des données	Révisions de l'OLPD pas encore adoptées
SMQ	Système de gestion de la qualité	
SGR	Système de gestion des risques	
LOGA	Loi sur l'organisation du gouvernement et de l'administration, RS 172.10	https://www.fedlex.admin.ch/eli/cc/1997/2022_2022_2022/fr.
OLPD	Ordonnance relative à la loi fédérale sur la protection des données, RS 235.11	https://www.fedlex.admin.ch/eli/cc/1993/1962_1962_1962/fr
Règlement	Ordonnance	
Directives NCSC[2]	Le centre national pour la cybersécurité (NCSC) a publié différentes directives.	Sécurité (admin.ch)
PA	Loi fédérale sur la procédure administrative, RS 172.021	https://www.fedlex.admin.ch/eli/cc/1969/737_757_755/fr
DGD	Directive sur la gestion des dossiers dans les domaines AVS/AI/APG/PC/AfamAgr/Afam	https://sozialversicherungen.admin.ch/fr/d/12739/download
CdC	Centrale de compensation	
SCSE	Loi fédérale sur la signature électronique, RS 943.03	https://www.fedlex.admin.ch/eli/cc/2016/752/fr