Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Directives sur les exigences en matière de sécurité de l'information et de protection des données des systèmes d'information des organes d'exécution du 1er pilier / des allocations familiales (D-SIPD)

Valable à partir du 1er janvier 2024

État au 17.12.2024

318.108.08 f D-SIPD

01.24

Suivi des modifications

VERSION	DATE	AUTEUR	REMARQUES
1.0	01.01.2024	OFAS	Version publiée
1.1	15.03.2024	Markus Moog (BSV)	Modifications de la mise en page/formatage
1.2	avril 2024	Michael Jeitziner (IG)	Création du suivi des modifications, mapping contrôle de la norme ISO/IEC 27001:2022, adaptation ch. 2.8.2
1.3	18.04.2024	Markus Moog (BSV) Michael Jeitziner (IG)	Insertion de la table des matières et du n° d'enregistrement. Ajout du texte du ch. 2.14
1.4	24.04.2024	Markus Moog (BSV)	Formatage, suppression de la note de bas de page 6, suppression de l'annexe 3 sur la sécurité de l'information, insertion du tableau d'aide et lien vers les téléchargements
1.5	30.04.2024	Markus Moog (BSV)	Renvois aux ch. et annexes, insertion et lien du tableau d'aide et des modèles
1.6	31.05.2024	Markus Moog (BSV)	Modification du titre 2.13, description des rôles (annexe 5)
1.7	30.07.2024	Markus Burri (BSV) Markus Moog (BSV)	Annexe 3 (nouveau) : analyse des besoins de protection et protection IT de base ; annexe 2 : insertion du nouveau processus d'annonce
1.8	04.11.2024	Markus Moog (BSV)	1.6 : insertion de la validité et du traitement des rapports d'audit selon ISO 27001 et ISAE, insertion du nouveau graphique du processus d'annonce, modification des liens d'aide et des modèles
1.9	11.11.2024	Markus Moog Markus Burri	Annexe 2 : insertion du nouveau processus d'annonce modélisé selon BPMN et d'exemples pour les groupes de protection et attributions (annexe 3), saisie commentaire sur la décision du comité de direction de l'OFAS concernant les services *cloud*, révision de l'ensemble du document
1.9.1	14.11.2024	Markus Moog Markus Burri	2.10.1 : reformulation de l'exemple 2.15.1 : compléter la description, explication que des tiers peuvent être des fournisseurs IT ou d'autres prestataires de services
1.9.2	15.11.2024	Markus Moog Markus Burri	Mise à jour de la description des services *cloud* et de l'avant-propos
2.0	17.12.2024	Markus Moog Markus Burri	Version finale Adoption par la CoCo eGov le 16.12.2024

Avant-propos

Les présentes directives s'adressent aux organes d'exécution du 1er pilier / des allocations familiales. Elles sont publiées dans la perspective de la révision de la loi sur l'AVS, qui entrera en vigueur le 1er janvier 2024. La surveillance de l'AVS, qui n'avait pratiquement pas changé depuis 1948, sera à l'avenir davantage axée sur les risques. La gouvernance sera renforcée, et les systèmes d'information du 1er pilier seront pilotés de manière adéquate.

À l'automne 2017, le Conseil fédéral avait adopté un projet de révision totale de la loi sur la protection des données. La nouvelle loi reflète l'évolution de la technologie et de la société et renforce les droits que les personnes concernées ont sur leurs données personnelles. Les présentes directives tiennent donc également compte de la loi révisée sur la protection des données et des dispositions d'exécution de la nouvelle ordonnance, qui sont entrées en vigueur le 1er septembre 2023.

Les recommandations du 1er janvier 2022 ont déjà permis aux organes d'exécution de se préparer de manière optimale aux directives de l'OFAS sur les exigences en matière de sécurité de l'information et de protection des données (SIPD). À cette fin, les représentants informatiques des organes d'exécution (projet eAVS/AI Information Security) ont été étroitement associés à l'élaboration des directives.

Les thèmes suivants ont été pris en compte pour le réexamen des recommandations :

- **Documentation de base et élargie de la SIPD** (ch. 2.8.2 et 2.8.3 ou annexes 3 et 4) **:** la compatibilité des exigences avec la nouvelle ordonnance sur la protection des données (OPDo) a été vérifiée.
- **Mandat de tiers / sous-traitance** (ch. 2.15, 2e élément) **:** l'intervention de sous-traitants (art. 9, al. 3, LPD) requiert l'approbation du mandant.
- **Sous-traitant à l'étranger** (ch. 2.15, 3e élément, et annexe 3, let. E) : selon cette recommandation, les données devraient normalement être conservées en Suisse ; les prestations de service pour l'exploitation doivent également être fournies en Suisse, et les exceptions doivent être justifiées. Le traitement de données personnelles par un sous-traitant à l'étranger entraîne une communication de données à l'étranger ; des dispositions complexes de la LPD s'appliquent dans ce cas. L'intervention d'un tiers en tant que sous-traitant à l'étranger est très complexe. Elle requiert de nombreuses clarifications juridiques dans le cas des pays pour lesquels le Conseil fédéral n'a pas déterminé qu'ils garantissent un niveau de protection adéquat au sens de l'art. 16, al. 1, LPD. Le ch. 2.15 contient un renvoi aux restrictions prévues par la LPD, qui doit en fin de compte s'appliquer à tous les organes d'exécution (aucune exception n'est prévue pour les services cantonaux). Des données personnelles ne peuvent être communiquées à l'étranger que si un code de conduite ou une certification garantit un niveau de protection approprié (art. 12, al. 1, OPDo).
- **Services cloud de tiers avec conservation des données en Suisse** (ch. 2.15.2, 4e élément) : dans ce cas, il ne s'agit 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 principal problème qui se pose actuellement est le traitement de données par le fournisseur Microsoft Suisse, soumis au droit suisse, mais qui, en vertu du Cloud Act des États-Unis et du FISA, peut être obligé par les tribunaux américains à divulguer certaines données aux autorités américaines.
- La législation suisse autorise la communication de données dans le cadre d'une instruction pénale (voir, par ex., art. 50, al. 1, let. d, LAVS). Cependant, en raison du principe de territorialité, les renseignements ne sont communiqués qu'aux autorités d'instruction suisses. Si une autorité d'instruction étrangère souhaite obtenir des renseignements, elle doit les demander 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, mais seulement après avoir examiné la requête d'entraide judiciaire. Les requêtes concernant des infractions qui n'existent pas en droit suisse sont rejetées. Or,

le Cloud Act et le FISA instaurent en pratique une « entraide judiciaire d'office », qui court-circuite le principe de territorialité et accélère la procédure pénale américaine En raison des développements récents, les prescriptions ont été analysées et les prescriptions de l'administration fédérale relatives à l'utilisation de services cloud ont été intégrées dans les présentes directives. La responsabilité du traitement des données incombe aux organes d'exécution. Ils doivent toutefois procéder aux évaluations des risques requises par la présente directive et se conformer aux directives de l'administration fédérale en matière de cloud computing (voir ch. 2.15.2).

Table des matières

Exigences SIPD

Ch.	Directives de l'OFAS sur la sécurité de l'information	Références à la norme DIN ISO/IEC 27001: 2022 (A = Annexe normative)	Commentaire
	1 Objectif, but, objet, principes, champ d'application et références dans le système juridique		
1.1	**1.1 Objectif, but et objet** Compte tenu de la modification de la loi fédérale sur l'assurance-vieillesse et survivants, de la modernisation de la surveillance dans le 1er pilier et de l'optimisation dans le 2e pilier de la prévoyance vieillesse, survivants et invalidité, l'OFAS demande aux organes d'exécution de tenir compte en permanence, dans leurs systèmes d'information, des nouvelles conditions générales décrites ci-après. Un objectif essentiel de la révision de la loi est que les systèmes d'information du 1er pilier disposent de la stabilité et de la capacité d'adaptation nécessaires et qu'ils garantissent la sécurité de l'information et la protection des données. Il est de la responsabilité des organes d'exécution de garantir la réalisation de ces objectifs (cf. art. 49*a*, al. 2, LAVS). La mise en œuvre exacte en termes de portée et de taille de l'organisation SGSI dépend notamment aussi de l'évaluation des risques et de la gouvernance des organes de mise en œuvre. En ce qui concerne la sécurité de l'information et la protection des données, les organes d'exécution doivent en outre satisfaire aux exigences fixées par l'OFAS (art. 49*a*, al. 3, LAVS). Ils doivent les respecter dans la mesure où elles relèvent de leur champ d'application (cf. ch. 1.2). Les présentes directives donnent un aperçu des exigences relatives aux systèmes d'information pour la sécurité de l'information et la protection des données (art. 49*a*, al. 3, en relation avec l'art. 72*a*, al. 2, let. b, LAVS) que doivent respecter les organes d'exécution (tous les chiffres du chap. 2).		
1.2	**1.2 Champ d'application** Les présentes directives relatives aux exigences visées au ch. 2 s'adressent à tous les organes d'exécution de l'AVS, de l'AI, du régime des APG et des PC (cf. art. 66, al. 1, let. a, LAI ; art. 21, al. 2, LAPG ; art. 26, al. 1, let. a, LPC), ainsi qu'à toutes les agences visées à l'art. 65 LAVS. Elles s'appliquent également à l'exécution des allocations familiales (art. 25, let. a, en relation avec l'art. 27, al. 3, LAFam ; art. 25 LFA).		

Ch.	Directives de l'OFAS sur la sécurité de l'information	Références à la norme DIN ISO/IEC 27001: 2022 (A = Annexe normative)	Commentaire
1.3	**1.3 Définition d'un système d'information (SI)** Un système d'information est un outil pour le traitement des données, la communication des données et le profilage (au sens de la LPD) aux fins de l'exécution des tâches[1]. Il contient des éléments techniques et organisationnels. Ces tâches comprennent notamment : - 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 responsabilités en matière de développement et d'exploitation. Un système d'information est toujours un bien devant faire l'objet d'une protection adéquate. Il s'agit donc d'un objet à protéger (voir ch 2.8).	A.5.9	
1.4	**1.4 Principe du système de gestion de la sécurité de l'information (SGSI)** Les organes d'exécution doivent exploiter un système de gestion de la sécurité de l'information (SGSI) leur permettant de satisfaire aux exigences minimales. Un SGSI est un outil de gestion qui sert à planifier, mettre en œuvre, vérifier et améliorer de manière systématique la sécurité de l'information. Il comprend les règles et les procédures nécessaires et permet de savoir à qui les tâches, les compétences et les responsabilités sont attribuées au sein de l'organisation. Le terme « SGSI » fait implicitement référence à la norme ISO/IEC 27001, qui fait autorité dans le secteur privé et, de plus en plus, dans les administrations publiques. Le SGSI s'appuie sur les normes nationales[2] et internationales[3] et doit au moins satisfaire aux prescriptions suivantes. Il fait l'objet de la vérification par l'organe de révision prévue à l'art. 68*a*, al. 2, let. c, LAVS. L'organe de révision vérifie que le SGSI de l'organe d'exécution répond aux exigences définies dans les présentes directives. Les caisses de compensation pour allocations familiales visées à l'art. 14, let. a, LAFam en sont exclues, sauf disposition contraire dans la loi cantonale sur les allocations familiales.		L'art. 68*a* LAVS ne s'applique pas à la LAFam (contrairement à la LFA). Les règles de la révision des caisses et du contrôle des employeurs relèvent explicitement de la compétence des cantons en vertu de l'art. 17, al. 2, let. i, LAFam. Pour les organes d'exécution de l'AVS qui gèrent également les allocations familiales en tant que tâche déléguée, la révision s'étendra au SGSI, y compris les allocations familiales. Le cas échéant, il est possible d'établir un rapport séparé

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

[2] notamment les directives sur la protection informatique de base au sein de l'administration fédérale ou la loi sur la sécurité de l'information LSI

[3] ISO/EC 27001:2022 concernant la sécurité de l'information, la cybersécurité et la protection des données – systèmes de gestion de la sécurité de l'information – exigences et ISO/IEC 27002:2022 concernant la sécurité de l'information, la cybersécurité et la protection de la sphère privée – mesures de sécurité de l'information qui explique les mesures normatives de sécurité de l'information décrites dans ISO/CEI 27001:2022, Annexe A, et émet des propositions en vue de leur mise en œuvre.

Ch.	Directives de l'OFAS sur la sécurité de l'information	Références à la norme DIN ISO/IEC 27001: 2022 (A = Annexe normative)	Commentaire
			comme le prévoit le ch. 3604 des Directives sur la remise d'autres tâches aux caisses de compensation (DRAT).
1.5	**1.5 Sécurité de l'information** La sécurité de l'information est un terme générique, qui couvre 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. 1. 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. 2. La protection des données, quant à elle, inclut 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. Des prescriptions provenant de sources de droit très différentes s'appliquent à la sécurité de l'information et doivent être prises en compte par les organes d'exécution (cf. annexe 1 : Aperçu des sources de droit nationales, normes ISO). Les présentes directives se concentrent sur les exigences applicables à un SGSI et ne traitent pas des questions de protection des données telles qu'elles résultent de la relation directe entre un assuré et un organe d'exécution. 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 dans de tels cas. Les présentes directives destinées aux organes d'exécution prennent néanmoins en considération les questions de protection des données, car les exigences en la matière doivent être vérifiées lors de l'élaboration d'une documentation de base du SGSI pour la sécurité de l'information (cf. let. a du ch. 2.8.2). Pour les questions relatives à la conservation des données, il convient en outre de se référer aux Directives sur la gestion, la conservation et la destruction des dossiers dans les domaines AVS/AI/APG/PC/Ptra/AFamAgr/AFam (DGD).		Il s'agit de mesures techniques et organisationnelles. Il ne faut pas les confondre avec les mesures techniques et organisationnelles prévues à l'art. 153*d* LAVS[4], qui doivent uniquement être respectées par les autorités, organisations et personnes autorisées à utiliser le numéro d'assuré AVS en dehors des assurances sociales.

[4] 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)

Ch.	Directives de l'OFAS sur la sécurité de l'information	Références à la norme DIN ISO/IEC 27001: 2022 (A = Annexe normative)	Commentaire
1.6	**1.6 Validité et traitement des rapports d'audit selon ISO 27001 et ISAE 3000 de type 1 et de type 2** Selon cette directive, les rapports d'audit rédigés selon les normes ISO 27001 et ISAE de type 1 ou de type 2 et démontrant la conformité avec les directives D-SIPD sont considérés comme suffisants si au moins une des exigences suivantes est remplie : 1. **Certification ISO 27001 :** les organes d'exécution présentent leur rapport de certification à l'organe de révision. Il n'est pas nécessaire de procéder à un nouvel examen complet si : • Le champ d'application du SGSI certifié englobe toutes les unités organisationnelles et tous les processus d'affaires pertinents des organes d'exécution. • La déclaration d'applicabilité du SGSI n'exclut aucune des mesures de sécurité exigées par les directives D-SIPD. • Lors de l'audit de (re)certification, toutes les mesures de sécurité exigées par les directives D-SIPD ont été vérifiées. 2. **ISAE 3000 de type 1 :** Le rapport d'audit se base sur toutes les conditions fixées dans les directives D-SIPD et se réfère à toutes les exigences fixées par les directives D-SIPD. 3. **ISAE 3000 de type 2 :** Le rapport d'audit (efficacité) est établi avec une certitude suffisante, contrôlé dans le temps et vérifié selon les contrôles définis par les directives D-SIPD.		

	2 Exigences	Norme ISO	Commentaire
2.1	**2.1 Système de gestion de la sécurité de l'information (SGSI)[5]** Chaque organe d'exécution dispose d'un SGSI (cf. ch. 1.4).	4.4	
2.2	**2.2 Structure de base du SGSI de l'organe d'exécution**		
a	Les organes d'exécution fixent dans leur SGSI les thèmes pertinents pour l'exécution de leurs tâches visées aux art. 63 LAVS (RS 831.10) et 57 LAI (RS 831.20) et pour leurs activités dans le cadre de la LAPG (RS 834.1), de la LPC (RS 831.30), de la LFA (RS 836.1) et de la LA-Fam (RS 836.2).	4.1	
b	Ils identifient les services impliqués et analysent leurs exigences en matière de sécurité de l'information.	4.2	
c	Ils disposent d'une vue d'ensemble actualisée de tous les systèmes d'information et de toutes les activités pertinentes pour l'informatique (cf. inventaire visé au ch. 2.8), intégrés dans le SGSI.	A.5.9	
d	Ils déterminent en parallèle les domaines auxquels les exigences ne s'appliquent pas (par ex., les organes d'exécution qui assument des tâches en dehors du champ du 1er pilier / des allocations familiales doivent déterminer quels champs d'application sont exclus). En l'absence de délimitation, le SGSI s'applique à l'ensemble de l'organisation. Par exemple, un établissement d'assurances sociales doit déterminer s'il établit un SGSI pour l'ensemble de l'organisation ou pour chaque organe d'exécution/unité organisationnelle séparément. De même, la Centrale de compensation (CdC) détermine si elle établit un SGSI pour l'ensemble de la CdC ou si les organes d'exécution de la CdC (conformément à l'ordonnance sur la CdC) établissent leur propre SGSI.	4.3	
e	Les organes d'exécution assurent l'actualisation et l'amélioration régulières du SGSI (y c. la gestion de la continuité des activités, cf. ch. 2.17) et de ses composants. Ils vérifient son actualité au moins une fois par année.	4.4	
2.3	**2.3 Lignes directrices relatives à la sécurité de l'information** La direction de l'organe d'exécution adopte des lignes directrices relatives à la sécurité de l'information qui s'appuient sur la structure de base du SGSI (ch. 2.2). Elle veille à leur diffusion au sein de l'organe d'exécution et auprès des services externes impliqués, ainsi qu'à leur actualisation régulière.	A.5.1	
	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 LAVS) : a. système de contrôle interne (SCI)	A.5.3	

[5] Pour mettre sur pied le SGSI, le guide suivant est recommandé :
- ISACA Leitfaden «Implementieren eines ISMS nach ISO/IEC 27001:2022»

	b. système de gestion de la qualité (en particulier l'amélioration continue) c. système de gestion des risques 2. la réglementation concernant les bonnes pratiques en matière d'information de la direction et des services impliqués (cf. ch. 2.2, let. b et d) ainsi que, le cas échéant : a. du PFPDT conformément à l'art. 24 LPD (en cas de violation de la sécurité des données) ou du responsable de la protection des données prévu par 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 liés à la sécurité de l'information (par ex. cf. annexe<*SP*/>2). 3. Il faut prévoir une réglementation de l'information adéquate de l'OFAS (ou des autorités de surveillance compétentes) sur les incidents liés à la sécurité de l'information dans les cas suivants : • 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 des dommages financiers importants. • L'image de l'assurance peut être sérieusement écornée au-delà d'un cas mineur (par ex. perte ou manipulation de données importante). • 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.	A.5.5 A.5.24	voir Processus d'annonce
2.4	**2.4 Exigences relatives à l'organisation de la sécurité de l'information** L'organisation de la sécurité vise au moins à ce que l'organe d'exécution désigne un préposé à 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 préposé à 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 et avec les éventuels prestataires mandatés (par ex. responsable informatique, fournisseurs, etc.). • Il est l'interlocuteur des préposés à la sécurité de l'information des prestataires informatiques. • Il est l'interlocuteur de l'OFAS pour les incidents relatifs à la sécurité de l'information pour lesquels les lignes directrices édictées par l'organe d'exécution prévoient une information à l'OFAS (ch. 2.3, point 3).	A.5.2	

	• Il vérifie la documentation relative à la sécurité de l'information (en particulier la documentation du SIPD, cf. ch. 2.8.2 et 2.8.3) et à la mise en œuvre ultérieure des exigences. • Il informe régulièrement la direction de l'organe d'exécution sur l'état 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.		Règles particulières pour les CAF (éventuellement canton)
2.5	**2.5 Exigences applicables aux projets dans le domaine des systèmes d'information** Un projet dans le domaine des systèmes d'information est limité dans le temps. Il implique des objectifs définis et une organisation spécifique, dont le but principal est soit d'introduire ou d'adapter une application, soit de construire ou d'améliorer des infrastructures du système d'information. Les organes d'exécution sont chargés de définir la nécessité d'un projet dans le domaine des systèmes d'information et de réglementer son déroulement. Ils tiennent toujours compte des aspects suivants : 1. La manière de procéder 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 aux caractéristiques et aux degrés de complexité divers. La méthode de gestion de projet utilisée est conforme ou équivalente à la norme suisse de l'association eCH (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 de la SIPD visée au ch. 2.8.2) et, si nécessaire, une documentation élargie de la SIPD visée au ch. 2.8.3.	A.5.8	
2.6	**2.6 Sécurité de l'information pour les appareils mobiles et le travail mobile** Les organes d'exécution définissent : • les conditions générales régissant le travail mobile 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 travail mobile grâce à des mesures de sécurité auxiliaires pour protéger les informations auxquelles les collaborateurs ont accès depuis les appareils mobiles en dehors des espaces de travail ou qui doivent y être traitées ou sauvegardées. Lors du traitement d'informations professionnelles depuis des appareils privés, ceux-ci doivent remplir les mêmes conditions en matière de sécurité des informations et de protection des données que les appareils fournis par les organes d'exécution.	A.8.1, A.6.7	

2.7	**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 un processus spécifique pour le contrôle de sécurité du préposé à la sécurité de l'information et des autres rôles clés dans l'organisation de la sécurité de l'information (cf. ch. 2.4), qui permette d'identifier les risques liés à l'intégrité personnelle et de prendre des mesures adéquates. Il est recommandé de contrôler les extraits du registre des poursuites et du casier judiciaire tous les cinq ans.	A.6.1, A.6.2, A.6.3, A.6.4, A.6.5	
2.7.2	**Information et formation** Les organes d'exécution veillent à ce que le personnel engagé soit informé au moins une fois par année sur les obligations en matière de sécurité de l'information et qu'il y soit sensibilisé.	A.5.4, 6.3, 6.4	
2.7.3	**Changement de situation** Les droits d'utilisateur du personnel engagé concernant l'accès (cf. ch. 2.11.1) aux systèmes d'information et les autorisations (cf. ch. 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 sont modifiés ou prennent fin. Il convient de mettre en place un processus pour gérer les comptes inutilisés.	A.6.5	
2.8	**2.8 Objets du SI à protéger : inventaire, documentation de la SIPD et autres exigences**	A.5.9, A.5.10	
2.8.1	Les organes d'exécution disposent d'un **inventaire** de tous les systèmes d'information (cf. ch. 2.2, let. c). Celui-ci est mis à jour régulièrement. Un système d'information est toujours un bien devant faire l'objet d'une protection adéquate. Il s'agit donc d'un objet à protéger.	A.5.9	
2.8.2	**Documentation de base de la SIPD** 1. Tout projet de SI sera précédé d'une analyse de la sécurité de l'information et de la protection des données (ch. 2.5). L'examen préalable des risques peut être utilisé comme modèle (voir annexe 6). 2. La documentation de base de la SIPD doit couvrir au moins les thèmes suivants en lien avec la sécurité de l'information et la protection des données : a. clarification du cadre juridique de la protection des données, en particulier en ce qui concerne la conformité légale du traitement des données au regard de la LPD et, le cas échéant, d'autres lois cantonales sur la protection des données et d'autres dispositions de lois sur les assurances sociales (voir guide à l'annexe 3) ; b. classification de l'objet à protéger selon la disponibilité (y c. évaluation de l'objet à protéger en lien avec la classification en tant qu'application essentielle) ; c. classification de l'objet à protéger selon la confidentialité ;	A.5.10, A.5.12, 5.13	Aides et modèles [annexe 6]

	d. classification de l'objet à protéger selon l'intégrité et la traçabilité (en ce qui concerne les accès aux données en mode écriture) ; e. lieu de conservation des données ; f. description de l'objet à protéger ; g. clarification des règles d'inscription dans le registre d'activités ou d'annonce au PFPDT (art. 12, al. 4, LPD). Les organes d'exécution qui sont des organismes cantonaux clarifient l'inscription dans 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 personnelles visée à l'art. 22 LPD ; i. attribution à un groupe de protection. 3. Si, sur la base de l'analyse visée au point 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 à protéger, il faut élargir la documentation de base de la SIPD visée au ch. 2.8.3. 4. Que ce soit sous l'angle qualitatif ou quantitatif, la documentation de base de la SIPD suit le modèle de l'annexe 3.		
2.8.3	**Documentation élargie de la SIPD** La documentation élargie de la SIPD doit être élaborée lorsque des données personnelles sensibles sont traitées avec l'objet à protéger, c'est-à-dire lorsque leur traitement peut entraîner un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées (ch. 2.8.2, point 3). Elle doit englober au moins les thèmes suivants : a. résumé des événements pertinents de la documentation de base de la SIPD ; b. Description du système du point de vue de la sécurité b.1 interlocuteurs / responsabilités ; b.2 description de l'ensemble du système ; b.3 description des données à traiter (règlement du traitement avec définition des 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, mesures de protection et risque résiduel (le cas échéant avec prise de position du PFPDT) ; d. rétablissement de l'activité / plan d'urgence (prévision des catastrophes, crises) ; e. Respect / contrôle / adoption des mesures de protection f. Mise hors service	A.5.10, A.5.12, 5.13	

	La documentation élargie de la SIPD doit s'inspirer du modèle proposé dans l'annexe 4, que ce soit sous un aspect qualitatif ou quantitatif.		
2.8.4	**Actualisation de la documentation de la SIPD** Les systèmes d'information existants (en exploitation) doivent disposer d'une documentation de la SIPD (ch. 2.8.2 et 2.8.3) qui corresponde aux relations effectives.		Modifications des systèmes d'information voir ch. 2.14
2.8.5	**Responsable de l'application** Les organes d'exécution désignent un responsable de l'application pour chaque système d'information utilisé individuellement ou en commun. Celui-ci fixe, avec le préposé à la sécurité de l'information, les exigences de sécurité pour le système d'information. Le responsable de l'application répond de la mise en œuvre des mesures de sécurité.	A.5.9	
2.9	**2.9 Gestion de l'accès aux systèmes d'information** Les organes d'exécution gèrent l'accès à leurs systèmes d'information. Le modèle de gestion de l'accès contient au moins a. une gestion des utilisateurs avec une identification univoque ; b. un modèle d'autorisation selon les fonctions ou les tâches des utilisateurs ; c. des processus d'octroi, de mutation et de retrait de comptes d'utilisateur et des autorisations ; et assure que d. l'ensemble des accès aux systèmes d'information (y c. les processus automatisés avec accès machine-to-machine) soient protégés par une authentification correspondant au degré de protection nécessaire et, si besoin, par des mesures cryptographiques adéquates (ISO A.8.24) conformément à la matrice d'accès (cf. aussi ch. 2.13.2) ; e. les utilisateurs reçoivent uniquement les droits d'accès aux systèmes d'information nécessaires pour l'exécution de leurs tâches ; f. une journalisation des accès est opérée conformément à l'art. 4 OPDo (voir annexe 3, ch. 7) ; g. le responsable de l'application contrôle au moins une fois par an l'exactitude et la pertinence des droits d'accès.	A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.4, A.8.5	
2.10	**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 reconnue, en fonction du cas d'application et des exigences juridiques correspondantes.	A.8.24	

	Les certificats reconnus par SAS pour des signatures électroniques, conformément à l'ordonnance sur la signature électronique (OSCSE ; RS 943.032)[6]. La solution choisie doit être décrite dans la documentation de la SIPD (ch. 2.8.2 ou 2.8.3). Les organes d'exécution garantissent la gestion sécurisée et la validité des clés cryptographiques.		
2.11	**2.11 Protection physique**		
2.11.1	**Dispositif de sécurité pour les locaux** Les organes d'exécution possèdent un dispositif de sécurité pour protéger physiquement leurs systèmes d'information. Ils doivent prévoir diverses mesures garantissant une protection individuelle adéquate des objets à protéger, en tenant compte des résultats du contrôle de la SIPD (ch. 2.8.2 ou 2.8.3) en ce qui concerne les groupes de protection (cf. ch. 2.8.2, point 2, let. i). Les mesures de protection à prévoir dans le dispositif de sécurité doivent porter sur les points suivants : • périmètre de sécurité physique (situation de l'environnement et mesures architecturales) ; • gestion de l'accès physique ; • protection des bureaux, locaux et installations ; • protection contre les menaces externes et environnementales.	A.7.1, A.7.2, A.7.3, A.7.5	
2.11.2	**Mesures pour les appareils et les équipements** Les organes d'exécution et leurs fournisseurs (cf. ch. 2.15.1) disposent de mesures documentées visant à protéger les appareils et les équipements contre la perte, les dégâts, le vol ou la mise en danger. Les mesures à prévoir pour les appareils doivent porter sur les points suivants : • emplacement et protection des appareils et des équipements ; • dispositifs d'alimentation ; • sécurité du câblage ; • maintenance des appareils et des équipements ; • retrait des valeurs ; • sécurité des appareils, équipements et valeurs en dehors des locaux ; • élimination sûre ou réutilisation des appareils et des équipements ; • appareils d'utilisateurs sans surveillance • directives pour un environnement de travail propre et verrouillages des écrans	A.7.7 - A.7.14, A.8.1	

[6] voir le site de l'OFCOM

2.12	**2.12 Mesures de sécurité opérationnelle** Les organes d'exécution et leurs fournisseurs (cf. ch. 2.15) disposent de mesures documentées permettant d'assurer la sécurité opérationnelle. Les mesures à prévoir doivent porter sur les points suivants : A. Procédures et responsabilités opérationnelles • procédures opérationnelles documentées ; • gestion des modifications ; • gestion des capacités ; • séparation des environnements de développement, de test et d'exploitation. B. Protection contre les logiciels malveillants par des mesures adaptées C. Sécurité des données D. Enregistrement et surveillance • enregistrement des événements ; • protection des informations enregistrées ; • activités des administrateurs et des utilisateurs ; • synchronisation des horloges. E. Gestion des logiciels pour l'installation des logiciels sur les systèmes en exploitation F. Vulnérabilités techniques • gestion des vulnérabilités techniques ; • restriction d'installation de logiciels. G. Contrôle de l'intégrité en cas de besoin de protection accru (cf. annexe 4, documentation élargie de la SIPD, let. D) H. Contrôle des systèmes d'information mesures pour les contrôles des systèmes d'information permettant 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 pour atténuer ces conséquences.	A.5.37, A.8.6, A.8.31, A.8.32 A.8.7 A.8.13, A.8.15, A.8.17 A.8.19 A.8.19 A.8.8 A.8.34	

2.13	**2.13 Gestion des réseaux et de la communication**		
2.13.1	**Documentation de l'architecture** Les organes d'exécution disposent d'une documentation de l'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. ch. 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 façon dont les personnes et les processus automatisés (machines/logiciels) peuvent accéder aux systèmes d'information exploités dans les différentes zones du réseau (cf. ch. 2.13.3) ou la façon dont elles doivent être authentifiées et éventuellement autorisées (cf. ch. 2.10, cryptographie).		
2.13.3	**Sécurité et documentation du réseau** 1. Les organes d'exécution doivent prévoir des directives relatives à la sécurité du réseau et définir les responsabilités en matière de gestion des réseaux et de connexions entre les réseaux. 2. Les organes d'exécution disposent, pour les réseaux relevant de 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 relevant de leur responsabilité contre les attaques et les accès non autorisés. 5. Pour les réseaux qui ne relèvent pas de la responsabilité des organes d'exécution et dont l'utilisation ne peut pas être contractuellement réglée (Internet), il faut mettre en œuvre des mesures de sécurité. 6. Il convient de documenter les structures du réseau et les responsabilités.	A.8.20 - A.8.22 A.5.14, A.6.6 A.8.21	
2.13.4	**Transfert protégé d'informations** 1. 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 et de sécurité des données (sécurité de l'information,	A.5.14, A.6.6	

	ch. 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 (cf. ch. 2.10 Cryptographie). 2. Les organes d'exécution veillent à ce que les collaborateurs (cf. ch. 2.7.2) connaissent les différents niveaux de protection (cf. ch. 2.8.2 et 2.8.3) en cas de transfert de données et qu'ils utilisent des moyens de transfert correspondants (par ex. courrier électronique crypté). 3. Concernant l'échange de données électroniques notamment des données personnelles sensibles (selon la LPD) entre les organes d'exécution et la Centrale de compensation (CdC), il existe plusieurs solutions techniques : 1 Réseau sedex : voir les directives de l'OFAS sur la plateforme informatique d'échange de données entre caisses de compensation AVS et offices AI (318.106.07 PED). 2 Transmission cryptée (par ex. Incamail, que tous les organes d'exécution ont adopté comme norme commune via l'association eAVS/AI). 3 Envoi directement depuis l'application au lieu d'un e-mail.		
2.14	**2.14 Modifications 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. ch. 2.5, 2.8.2 et 2.8.3). La documentation de la SIPD (ch. 2.8.2 ou 2.8.3) doit être actualisée en cas de modification. Si aucune modification n'a été apportée au système d'information, l'actualité de la documentation de la SIPD doit être vérifiée au moins une fois tous les cinq ans. Les exigences qui, selon le ch. 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 en outre de respecter les exigences énoncées au ch. 2.12, let. A, 4e élément, concernant la séparation des environnements de développement, de test et d'exploitation, et de garantir la protection des données utilisées pour les tests. Si les organes d'exécution ne sont pas eux-mêmes responsables de la mise en œuvre des modifications de leurs systèmes d'information, les exigences doivent être communiquées aux tiers chargés des modifications et le respect de ces exigences doit être surveillé et contrôlé.	A.5.8, A.8.26 A.8.25, A.8.27, A.8.29 - A.8.32 A.8.33 A.8.30	

2.15	**2.15 Contrats avec des tiers**		
2.15.1	• 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 qui concernent le traitement de telles données, ils fixent contractuellement l'ensemble des règles de protection (devoir de confidentialité, traitement des données, etc.) et les exigences applicables aux prestations. Ils précisent également dans le contrat les mesures de contrôle correspondantes et, pour les tiers qui ne sont pas contrôlés par les organes d'exécution, les peines conventionnelles prévues en cas de violation de ces dispositions. Ces contrats peuvent être aussi bien des relations avec les fournisseurs dans le domaine IT que des prestations ne relevant pas du domaine IT. • En principe, un contrat avec un tiers doit prévoir que ce dernier l'exécutera lui-même et que l'organe d'exécution doit pouvoir s'opposer à tout transfert éventuel (partie ou total) des engagements. Même en cas de transfert des engagements, il faut s'assurer par des accords que les exigences minimales seront pleinement respectées. Ce principe s'applique expressément à l'obligation de tenir un inventaire (ch. 2.8.1). • Les prestations relatives à l'exploitation doivent être réalisées sur le territoire national. Il est nécessaire de déclarer et de justifier les prestations relatives à 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 si ce traitement est lié à un échange international de données réglementé sur le plan légal (par ex. art. 32, al. 3, LPGA ou CIBIL ([Accords bilatéraux Suisse-UE. Convention AELE. Circulaire sur la procédure pour la fixation des prestations dans l'AVS/AI/PC]).	A.5.19 - A.5.21	Indications sur : - Heures de service exigées - Exigences Disponibilité Les organes d'exécution déterminent le besoin de protection des données qui doivent être traitées par des tiers et, si nécessaire, établissent l'évaluation préalable des risques et l'AIPD. Sur la base de la documentation ainsi établie, les tiers potentiels documentent la manière dont ils respectent les prescriptions en matière de protection des données concernant l'organe d'exécution (protection de base et, le cas échéant, documentation élargie de la SIPD).
2.15.2	Il faut s'assurer que les principes de l'administration fédérale relatifs aux services de *cloud* sont respectés[7] :		

[7]Voir le site de l' administration fédérale sur l'informatique en nuage

	1. Traitement de données dans des clouds publics standard (niveau I) : traitement de données non critiques, anonymes ou publiques. 2. Traitement de données dans des clouds publics+ (niveau II) : uniquement pour les informations jusqu'à la classification « INTERNE » ou les données personnelles non sensibles. En cas d'exigences plus élevées, par exemple pour les données personnelles sensibles, une analyse des besoins de protection, une analyse des risques, un contrôle de la conformité au droit et une analyse d'impact relative à la protection des données personnelles sont nécessaires. En outre, des mesures de protection techniques et organisationnelles (par ex. cryptage) s'imposent. 3. Traitement de données dans un cloud privé standard (niveau III) : des exigences accrues en matière de protection des données peuvent être garanties. Traitement de données classifiées « CONFIDENTIEL » et de données personnelles sensibles, et respect d'exigences fixées dans des lois spéciales. 4. Traitement de données dans un cloud privé+ (niveau IV) : répondre à des exigences de sécurité très spécifiques.		
2.16	**2.16 Gestion des incidents relatifs à la sécurité de l'information** Le préposé à la sécurité de l'information des organes d'exécution s'assure que les notifications concernant des incidents de sécurité en lien avec les systèmes d'information sont adéquatement traitées, documentées et évaluées, afin 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 de garantir que les personnes compétentes prennent les mesures appropriées (cf. exemple à l'annexe 2).	A.5.24 - A.5.28, A.6.8	
2.17	**2.17 Maintien de la sécurité de l'information (gestion de la continuité des activités)** Les organes d'exécution disposent - conformément au besoin des objets du SI à protéger (cf. ch. 2.8.2 et 2.8.3) - de procédures de redémarrage testées pour maintenir et restaurer l'exploitation des systèmes TIC critiques à protéger en cas de perturbations, d'urgences et de catastrophes.	A.5.29, A.8.14	
2.18	**2.18 Conformité aux directives** Les organes d'exécution veillent à ce que les lacunes liées aux systèmes d'information identifiées grâce à leur système de contrôle interne, à leur gestion de la qualité ou à leur gestion du risque (cf. aussi ch. 2.3) soient comblées, indépendamment du fait qu'elles aient déjà été découvertes lors d'une révision prévue par le droit de la surveillance.	A.5.31-A.5.34, A.5.35, A.5.36, A.8.8	

Annexes

Annexe 1 : Références juridiques sur le thème de la sécurité de l'information

1. Sources juridiques nationales

Les bases légales relatives à la sécurité de l'information (ainsi qu'à la protection et à la sécurité des données) se trouvent dans différentes sources.

A. Au niveau fédéral

1. L'art. 13, al. 2, Cst. protège toute personne contre l'emploi abusif des données qui la concernent ; l'art. 35 Cst. oblige les organes d'exécution à contribuer à la réalisation de ce droit fondamental.
2. La **loi fédérale sur la protection des données** (LPD ; RS *235.1*) et son ordonnance (OPDo ; RS *235.11*)
   - règlent les aspects formels (définition des données personnelles, des données sensibles, du profilage, etc.) ;
   - fixent les limites du traitement et de la communication des données personnelles (conformité au droit, proportionnalité, finalité, exactitude, etc.) ;
   - garantissent certains droits individuels liés aux données (droit d'accès) ;
   - imposent l'utilisation de moyens « techniques et organisationnels » garantissant la sécurité des données (confidentialité, intégrité, disponibilité).
3. La **législation spéciale du droit des assurances sociales**
   - contient des normes d'autorisation (liée à la LPD) permettant aux assurances sociales de traiter des données sensibles (et d'établir un profilage) et de communiquer les données nécessaires aux systèmes d'information ;
   - définit les présentes exigences techniques et organisationnelles applicables aux systèmes d'information ;
   - garantit (en lien avec la PA [RS 172.021]) certains droits d'information individuels et liés à la procédure (par ex., consultation des pièces).
4. De nombreuses autres prescriptions (LOGA, RS *172.010* ; OTNI, RS *172.010.58* ; ordonnance sur la sécurité de l'information et autres directives du Centre national pour la cybersécurité [NCSC][2]) s'appliquent aux systèmes d'information des autorités fédérales et de l'armée (par ex., CdC), auxquelles il faut ajouter la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[8].

B. Au niveau cantonal

Les législations cantonales entrent également en ligne de compte, qu'il s'agisse de la sécurité de l'information ou de la protection des données.

[8] FF **2020** 9665

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

S'agissant du champ d'application, les organes d'exécution

- doivent appliquer l'ensemble des normes relevant de la législation spéciale des assurances sociales. En effet, la LPD s'applique non seulement aux organes d'exécution faisant partie de l'administration fédérale, mais aussi aux organes d'exécution organisés par des associations, qu'elle assimile aux organes fédéraux ;
- sont soumis, en tant qu'organismes cantonaux, à la loi sur la protection des données de leur canton.

2. Les normes ISO et leur importance

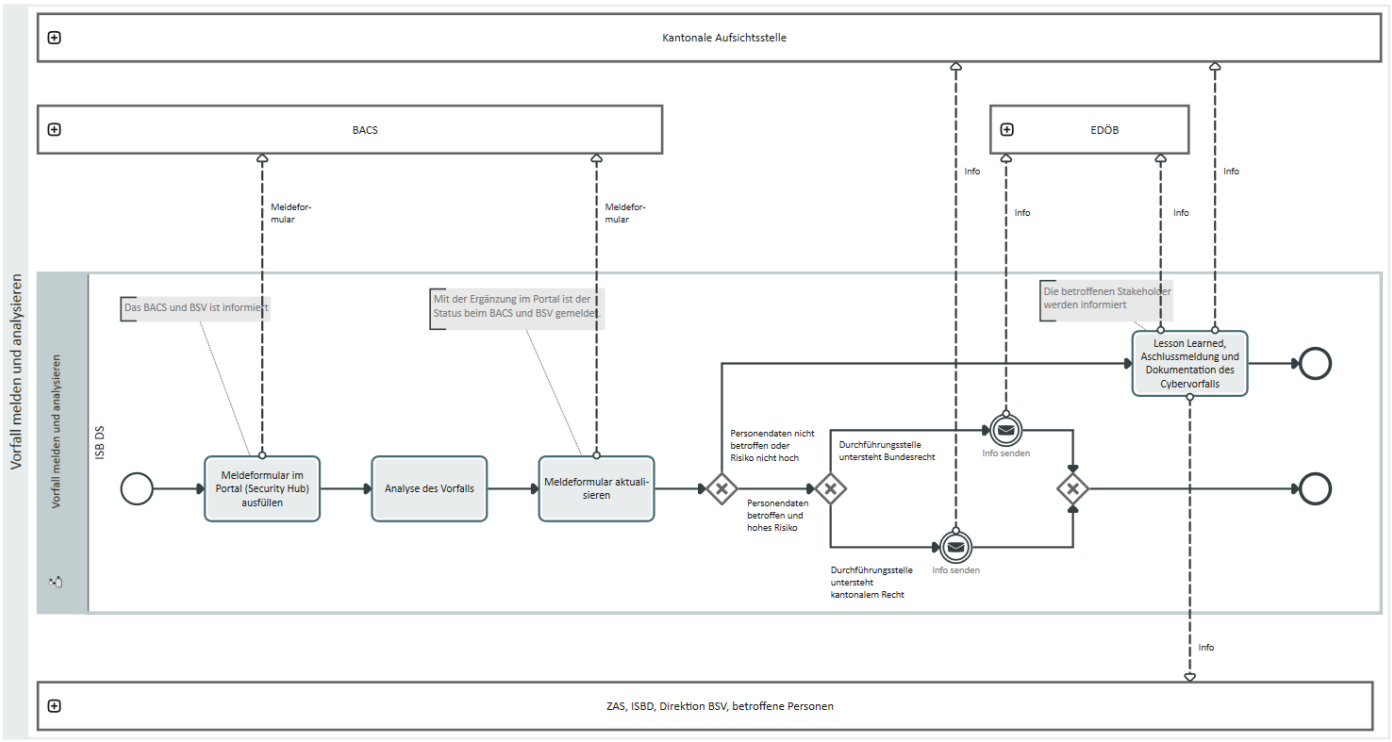
L'Organisation internationale de normalisation (ISO) est composée de représentants d'organisations nationales de normalisation et élabore des normes internationales. Les normes ISO 27001 et 27002 concernent l'informatique, et plus précisément les procédures de sécurité de l'information. Elles mettent l'accent sur la gestion de cette sécurité et définissent notamment les exigences applicables à ce type de systèmes. Ces exigences prennent toujours la forme d'objectifs et de mesures numérotés de manière continue, qui constituent un système de numéros de référence. Comme les questions relevant de l'informatique et de la sécurité informatique se posent dans le monde entier, de nombreuses entreprises, organisations étatiques et ONG utilisent ces normes. En Suisse, elles sont intégrées aux lois et ordonnances.

Par exemple,

5. les directives sur la protection informatique de base dans l'administration fédérale se réfèrent aux normes ISO ;
6. la certification visée à l'art. 13 LPD (obligatoire, par ex., pour le service de réception des données des assureurs-maladie visé à l'art. 59a, al. 6, OAMal[9]) dépend notamment du respect de la norme ISO 27001 (cf. ch. 4 des directives du 19 mars 2014 sur les exigences minimales qu'un système de gestion de la protection des données doit remplir). Les directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir et leurs annexes font le lien entre la législation nationale sur la protection des données (LPD et OLPD), dont la teneur reflète les normes ISO, et la numérotation de ces normes, puisqu'elles reposent sur cette dernière (cf. notamment ch. 4 des directives et let. g de l'annexe sur le thème de la sécurité des données au sens de l'art. 8 LPD). Les mesures supplémentaires, qui reposent sur la législation nationale, sont explicitement structurées sur le modèle de la norme ISO 27002.

[9] Ordonnance du 27 juin 1995 sur l'assurance-maladie ; RS *832.102*

Annexe 2 : Processus d'annonce



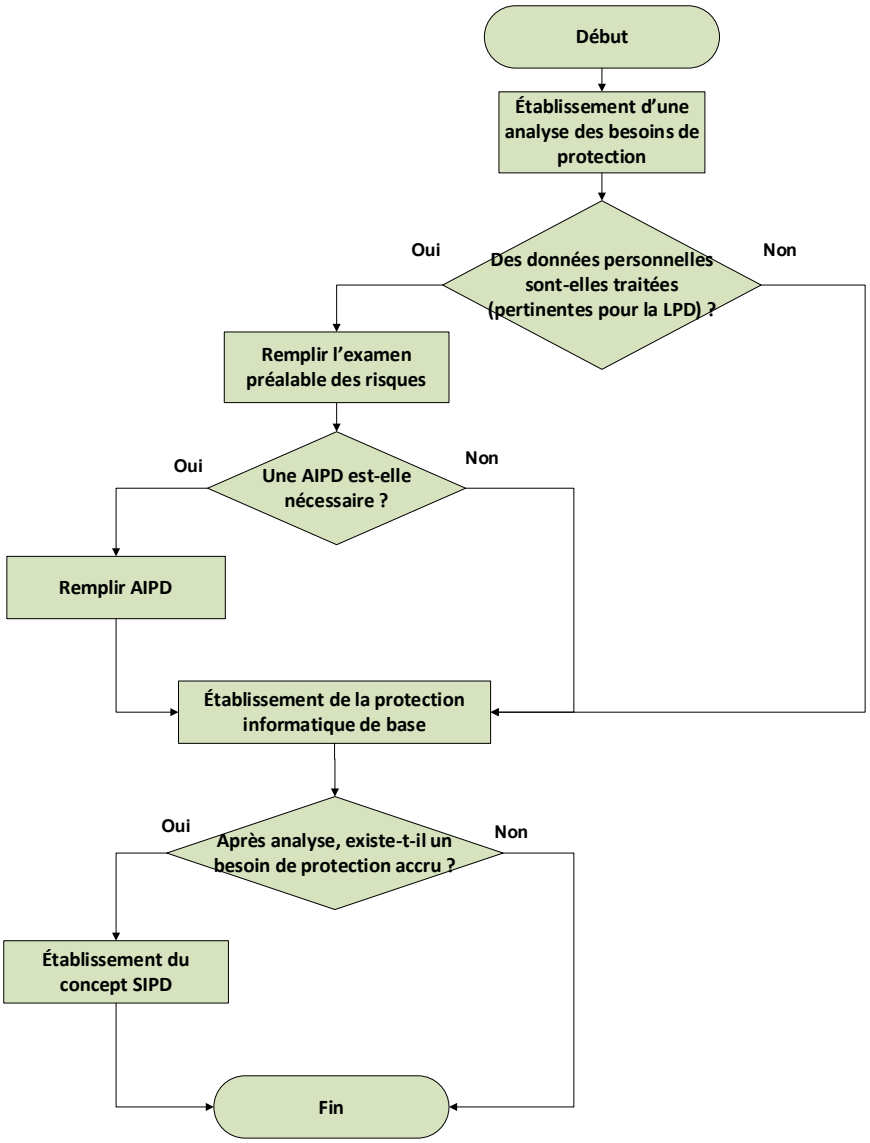
Annexe 3 Documentation de base de la SIPD

Pour chaque objet de protection, il faut au moins remplir l'analyse d'impact relative à la protection des données personnelles, l'analyse des besoins de protection et de protection IT de base et, le cas échéant, l'examen préalable des risques.

Liens vers les modèles des documentations à établir voir Annexe 6

- Examen préalable des risques
- Analyse d'impact relative à la protection des données personnelles
- Analyse des besoins de protection

Le résultat de l'analyse des besoins de protection est une évaluation de la classification de l'objet de protection informatique ou du projet. Si un besoin de protection accru est constaté, un concept SIPD doit être établi en plus de l'analyse des besoins de protection et de la protection IT de base. Le diagramme suivant explique cette réglementation :



A. Guide de définition du cadre légal au sens du ch. 2.8.2, let. a

Remarques générales / explication

Chaque organe d'exécution dépend d'une assurance sociale régie par le droit fédéral et, à ce titre, est habilité et tenu d'accomplir les tâches définies par la loi (principe de légalité). Ses activités se fondent sur une loi spéciale (LAVS, LAI, etc.). Si, pour accomplir ses tâches, il utilise des systèmes d'information, il doit en plus respecter d'autres bases légales. D'une part, il est soumis à la LPGA pour l'assistance administrative (art. 32), l'obligation de garder le secret (art. 33) et l'échange électronique des données (art. 76*a*). D'autre part, il est tenu d'appliquer les dispositions de la LPD, de l'OPDo et des législations cantonales relatives à la sécurité de l'information et à la protection des données. Ces dispositions déploient souvent leurs effets sur le traitement des données et leur sécurité :

- Les organes fédéraux du 1er pilier (par ex., la Caisse fédérale de compensation ou la Caisse suisse de compensation de l'AVS) ainsi que les organes d'exécution assimilés à des organes fédéraux par la LPD (soit tous les organismes qui ne sont pas cantonaux) doivent, par exemple, respecter les prescriptions relatives au registre des activités de traitement (art. 12 LPD), à l'analyse d'impact relative à la protection des données personnelles (art. 22 LPD), à l'annonce des violations de la sécurité des données (art. 25 LPD), à la désignation d'un conseiller à la protection des données (art. 25 OPDo) et à la journalisation des données personnelles (art. 4 OPDo).
- Lorsque les législations cantonales contiennent des dispositions similaires, les organes d'exécution cantonaux sont tenus de contrôler quelles obligations en découlent.

Guide relatif au cadre légal et permettant d'établir la conformité au droit du traitement des données

#	Question/thème	Base légale	Conséquence, exemple
1	Conformité aux principes de la loi sur la protection des données : • légalité du traitement au sens de l'art. 6, al. 1, LPD ; • proportionnalité et finalité de la collecte et du traitement des données dans le respect du principe de bonne foi et de l'art. 6, al. 2 et 3, LPD.	L'art. 49*b* LAVS ou le nouvel art. 49*f* LAVS autorisent les organes d'exécution à traiter les données personnelles, y compris les données sensibles et les profils de personnalité, pour autant que l'accomplissement de leurs tâches légales l'exige. Cette autorisation s'applique également à tous les autres organes d'exécution (art. 66a LAI ou les nouveaux art. 66 P-LAI, art. 25 LAFam, art. 25, al. 2, LFA, art. 29 LAPG et art. 26 LPC). Dans le domaine d'activité des organes d'exécution, la base légale ordinaire suffit en général (art. 34 ss LPD).	Contrôler dans la documentation de base de la SIPD si le système d'information est réellement utilisé et convient pour l'accomplissement d'une tâche légale. **Légalité :** indications sur les bases légales du traitement des données (par ex. art. 49*b* LAVS) **Finalité :** quelle tâche légale est visée (loi ou ordonnance) ? **Proportionnalité :** à qualité égale, le même but peut-il être atteint avec un traitement des données moins poussé ? **Bonne foi :** il y a violation du principe de bonne foi si une personne ne peut en aucun cas s'attendre à ce que ses données soient traitées dans ce cas précis. **Exemple : classement d'une application de courrier électronique d'une caisse de compensation**

#	Question/thème	Base légale	Conséquence, exemple
			AVS privée dans la documentation de base de la SIPD : Les assurés utilisent régulièrement les courriers électroniques pour obtenir des renseignements ou des conseils au sens de l'art. 27 LPGA. Or, les données utilisées peuvent être sensibles. Il convient d'en tenir compte, sur le plan technique, lors de la classification (cf. Modèle, let. C et D). En vertu de l'art. 49*a* (nouvel art. 49*f* LAVS), le traitement de données personnelles est **légal**. Lorsque les courriels ne contiennent que des données pertinentes pour le cas traité, **les principes de finalité, de proportionnalité et de bonne foi sont respectés.**
2	Entrée (collecte) et sortie (communication) de données et obligation de garder le secret	La loi encadre la collecte et la communication de données ; de plus, par la force des choses, toute donnée collectée l'est par le biais d'une communication. Sur le plan formel, la communication de données fait partie du traitement (art. 5, let. d, LPD). La LPD encadre cette collecte (art. 6, al. 3, art. 19), mais des exceptions sont prévues (en particulier par l'art. 20 LPD). Cependant, dans le cadre de l'obligation de collaboration et d'annonce, les lois sur les assurances sociales règlent souvent une partie de l'entrée de données. À cela il faut ajouter l'envoi automatisé de notifications en raison de réglementations relatives à certains systèmes d'information (par ex. notification d'état civil à l'AVS). Enfin, dans certains cas, la LPGA garantit l'assistance administrative. L'art. 36, al. 1, LPD dispose qu'il faut également prévoir une base légale pour la communication de données (comme pour le traitement des données). Les différentes lois régissant les assurances sociales règlent en détail la communication de données dans leurs propres catalogues, en distinguant notamment les sorties de données au cas par cas des pro-	Il convient de vérifier dans la documentation de base de la SIPD si l'entrée et la sortie de données sont juridiquement admissibles. Pour les systèmes d'information qui prévoient une entrée ou une sortie automatique de données, il est nécessaire de déterminer et de documenter la base légale. **Exemple : classement d'une application de courrier électronique d'une caisse de compensation AVS privée dans la documentation de base de la SIPD :** Les courriers électroniques servent exclusivement au transfert de données au cas par cas. L'utilisateur formé concerné doit vérifier la validité juridique de l'entrée et de la sortie de données. Il faut veiller à ce que les utilisateurs soient formés et en mesure de déterminer l'identité du destinataire des données avec l'aide éventuelle de mesures techniques et organisationnelles.

#	Question/thème	Base légale	Conséquence, exemple
		cessus de masse. Ce faisant, elles dérogent à l'obligation générale de garder le secret visée à l'art. 33 LPGA.	
3	Exactitude et rectification des données (art. 6, al. 5, et 41, al. 2, LPD)	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 de la SIPD quelles sont les garanties de l'exactitude des données, quelles sont les possibilités de confirmer la plausibilité, quelles méthodes de vérification sont utilisées et comment sont faites les corrections nécessaires. Il convient d'établir des processus à cet effet. **Exemple : classement d'une application de courrier électronique d'une caisse de compensation AVS privée dans la documentation de base de la SIPD :** Les données utilisées dans les courriers électroniques sont liées à un cas particulier et il n'est pas possible de les vérifier systématiquement. Il appartient à l'utilisateur, si nécessaire, de vérifier leur plausibilité par les méthodes appropriées. Il faut veiller à ce que les utilisateurs soient formés et utilisent les données correctes avec l'aide éventuelle de mesures techniques et organisationnelles.
4	Droit d'accès (art. 25 LPD et art. 16 OPDo)	L'art. 25 LPD 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 LPD. La personne peut en outre demander la remise de données, encore une fois sous certaines conditions (art. 28 et 29 LPD). Lorsque plusieurs responsables traitent conjointement les données personnelles, la personne concernée peut faire valoir son droit d'accès auprès de chacun.	Il convient d'analyser dans la documentation de base de la 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 de la 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, LPD). **Exemple : classement d'une application de courrier électronique d'une caisse de compensation**

#	Question/thème	Base légale	Conséquence, exemple
			AVS privée dans la documentation de base de la SIPD : Il faut s'assurer, dans le cadre de la documentation de base de la SIPD, qu'il est possible d'accéder aux courriers électroniques d'une personne déterminée. On peut également s'en assurer en définissant un processus pour un autre système d'information tel qu'une gestion électronique des affaires. Il faut y faire référence dans la documentation de base la 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 organes fédéraux du 1e pilier (par ex. la Caisse fédérale de compensation ou la Caisse suisse de compensation) ainsi que les organes d'exécution assimilés à des organes fédéraux par la LPD (soit tous les organes d'exécution qui ne sont pas cantonaux) doivent respecter les dispositions relatives au registre de leurs activités de traitement et déclarer leurs registres au PFPDT (art. 12 LPD).	
6	Conseiller à la protection des données	Les organes d'exécution désignent un conseiller à la protection des données, qui assiste le responsable du traitement lors de l'établissement de l'analyse d'impact relative à la protection des données et vérifie son exécution (art. 25 et 26, al. 2, let. a, ch. 2, OPDo). Le conseiller à la protection des données peut formuler des critiques dans le cadre de l'analyse d'impact. Ces critiques font partie intégrante de l'analyse. Le responsable du traitement met les ressources nécessaires à la disposition du conseiller à la protection des données et lui donne accès à tous les renseignements, les documents, les registres des activités de traitement et à toutes les données personnelles dont il a besoin pour l'accomplissement de ses tâches (art. 23, let. a et b, OPDo). Plusieurs organes fédéraux peuvent désigner le même conseiller. Les petits organes fédéraux ou les départements dont l'organisation est centralisée peuvent	

#	Question/thème	Base légale	Conséquence, exemple
		ainsi réaliser des économies en utilisant les synergies.	
7	Journalisation	Lors du traitement automatisé de données personnelles, l'organe fédéral responsable et son sous-traitant journalisent au moins l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données. La journalisation doit fournir des informations sur l'identité de la personne qui a effectué le traitement, sur la nature, la date et l'heure du traitement et, cas échéant, sur l'identité du destinataire des données (art. 4, al. 2 et 4, OPDo). Conformément à l'article 4 de l'OLPD, le processus de « lecture » dans les systèmes de traitement des données doit également être consigné afin de garantir la traçabilité du traitement des données personnelles. L'obligation légale de journaliser les accès en lecture existe indépendamment de l'utilité (perçue) et de l'éventuelle perte de performance causée par la journalisation. Des dispositions transitoires s'appliquent dans ce contexte. Tant que le système de traitement des données est exploité sans extension de l'étendue des fonctions et continue à fonctionner comme lors de l'entrée en vigueur de l'OLPD (1.9.2023), l'art. 4 al. 2 OLPD ne s'applique pas encore. Les simples mises à jour de sécurité n'y changent rien non plus. Dès que des extensions fonctionnelles ayant des conséquences sur le traitement des données personnelles (comme le remplacement de modules) sont effectuées, il ne tombe pas sous le coup de la disposition transitoire et une journalisation doit être effectuée conformément à l'art. 4, al. 2, RGPD. Les procès-verbaux de journalisation sont conservés durant au moins un an, séparément du système dans lequel les données personnelles sont traitées. Ils sont accessibles uniquement aux organes et aux	Sur le plan de la sécurité des données, l'exploitation des données de journalisation garantit le respect des principes de confidentialité, d'intégrité et de disponibilité. Elle permet de relever toute utilisation inhabituelle, les incidents de sécurité potentiels (par ex. emploi abusif d'un système) ainsi que les attaques ciblées.

#	Question/thème	Base légale	Conséquence, exemple
		personnes chargés de vérifier l'application des dispositions relatives à la protection des données personnelles ou de préserver ou restaurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, et ne peuvent être utilisés qu'à cette fin (art. 4, al. 5, OPDo).	

B. Muster zur Klassifizierung der Verfügbarkeitsanforderungen (nach Rz 2.8.2, Bst. b)

#	Question ou exigence	Critères	Besoin de protection accru ? > documentation élargie de la SIPD visée au ch. 2.8.3 nécessaire ? *(à la place de la documentation, analyses du risque et exigences de sécurité, notamment)*
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 ? (cf. ch. 2.8.2, point 2, let. b) : faut-il prendre des mesures de prévention contre les catastrophes pour l'objet à protéger	Mesures de prévention nécessaires	**oui**
		Pas de mesures de prévention nécessaires	**non**

C. Guide pour les exigences de confidentialité (selon ch. 2.8.2, let. c)

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

Question ou exigence	Critères	Besoin de protection accru ? > documentation élargie de la SIPD visée au ch. 2.8.3 nécessaire ? *(à la place de la documentation, analyses du risque et exigences de sécurité, notamment)*	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	Description des mesures de protection de base existantes
	Données personnelles	Non	Description des mesures de protection existantes
	Données personnelles sensibles (art. 5, let. c, LPD) ? et/ou profilage (évaluation automatisée ; cf. art. 5, let. f, LPD) ?[10] Si profilage : à risque élevé (cf. art. 5, let. g, LPD) ?	Oui Oui Oui	Description des mesures de protection de base existantes
Dans quel niveau de classification se trouvent les données de l'objet à protéger ?	Public Interne Confidentiel Hautement confidentiel	Non Non Oui Oui	La classification devrait être définie dans une prochaine version.

D. Guide de classification des exigences d'intégrité et de traçabilité (selon ch. 2.8.2, let. d)

Classification	Description	Mesures	Documentation élargie de la SIPD visée au ch. 2.8.3 nécessaire ?
Intégrité normale	Pour les domaines des technologies de l'information et de la communication (TIC) classés au niveau « intégrité normale », on	Les mesures générales pour les appareils et les équipements (ch. 2.11.2 et 2.12.2) doivent garantir l'« intégrité normale ».	Non

[10] 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 *(terme qui n'est plus défini par la loi)* est le résultat d'un traitement et traduit ainsi quelque chose de statique. À l'inverse, le profilage 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 santé, son comportement, ses préférences, son lieu de résidence 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. Autrement dit, il s'agit d'une analyse automatisée de données personnelles permettant d'évaluer, d'une manière également automatisée, les caractéristiques d'une 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 de 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. »

	peut renoncer à des mesures particulières pour conserver l'intégrité.		
Intégrité sécurisée	Pour les domaines des TIC classés au niveau « intégrité sécurisée », on doit mettre en place des mesures de protection contre les modifications par des tiers non autorisés.	La documentation de base de la SIPD permet d'examiner l'importance des conséquences de modifications incorrectes apportées aux systèmes d'information (nouvelle version). Les critères d'évaluation sont, par exemple, la perturbation de l'exécution des tâches, les impacts externes négatifs ou les conséquences financières pour l'assurance.	Oui Afin de pouvoir corriger les conséquences d'éventuelles erreurs, il faut tester et documenter les modifications de manière approfondie (selon l'importance des conséquences possibles) et les effectuer de sorte qu'elles correspondent aux exigences des projets, en particulier aux critères applicables de gestion de la qualité et du risque (cf. ch. 2.5, point 1, et ch. 2.14, 3e paragraphe).
Intégrité vérifiable	Pour les domaines des TIC classés au 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 classés au niveau « intégrité signée », on mettra en place en plus des signatures numériques.		La version définitive suivra.

E. Conservation des 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 à protéger / du projet

- But et objet
- Processus soutenus
- Type et étendue des données
- Utilisateurs
- Quantification de l'utilisation

G. Obligation de registre / d'annonce

Selon le ch. 2.8.1, il existe en principe une obligation d'inventaire pour tous les systèmes d'information. Une obligation de tenir un registre s'applique également, conformément à l'art. 12 LPD. Cette dernière vise les organes fédéraux / organes d'exécution (soit tous les organes d'exécution qui ne sont pas 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 de la SIPD doit déterminer si et quelles obligations de registre et d'annonce s'appliquent et doit documenter la manière dont elles sont remplies.

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

Conformément à l'art. 22 LPD, l'analyse d'impact relative à la protection des données personnelles 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 en question.

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

La réglementation de la LPD (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 personnelles 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 personnelles dans la documentation de base en fonction de la législation cantonale correspondante.

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

- 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, LPD) ?
- Est-il prévu de prendre des mesures déjà connues ou à développer pour protéger la personnalité et les droits fondamentaux°?

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 visés au ch. 2.8.2, point 2.

Exemples de groupes de protection et d'attributions (liste non exhaustive)

Groupes de protection		**Description / exemple**	**Exemples d'information**
S1	**publique**	Informations et données publiques	▪ Internet ▪ Réseaux sociaux ▪ Informations de presse, communiqués de presse
S2	**interne**	Données personnelles des collaborateurs et des clients ainsi que données d'affaires et de projets internes	▪ Registre des adresses ▪ Données personnelles non sensibles sans protection particulière

S3	**confidentiel**	Données relatives à la stratégie de l'entreprise, données financières et personnelles, données des clients ou des assurés (données de base)	▪ Documents de stratégie ▪ Comptabilité financière ▪ Dossiers/documents personnels : candidatures, évaluations, contrats de travail, etc. ▪ Plans du réseau informatique
S4	**Hautement confidentiel**	Toutes les données personnelles hautement sensibles qui sont réputées sensibles selon la LPD	Les données personnelles sensibles, telles que : ▪ Données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales ▪ Données relatives à la santé ▪ Sphère intime ▪ Appartenance ethnique ou origine ▪ Données génétiques ou biométriques ▪ Données concernant des mesures d'aide sociale ▪ Procédures pénales ou disciplinaires ▪ Saisie de salaire

Annexe 4 : Documentation élargie de la SIPD

(visée au ch. 2.8.3)

Si l'analyse révèle des besoins de protection accrus de l'objet à protéger (voir la documentation du processus à l'annexe 3), un concept SIPD et une analyse des risques doivent être établis.

Liens vers les modèles des documentations à établir : voir Annexe 6

a. Résumé des résultats pertinents de la documentation de base de la SIPD

Le résumé sert de base pour le concept SIPD avec **analyse du risque** et porte sur la classification de l'objet à protéger 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 à protéger, 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 personnelles.

b. Description du système du point de vue de la sécurité

Description détaillée des éléments de sécurité issus du système, des applications, des données existantes et traitées, et des processus qui leur sont liés.

b.1 Interlocuteurs / responsabilités

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

b.2 Description de l'ensemble du système

Description des fonctions de sécurité comme la gestion de l'accès (cf. ch. 2.9), la sécurité opérationnelle (cf. ch. 2.12) et les prestations de tiers (cf. ch. 2.15). Il est également possible de renvoyer à la documentation correspondante (par ex. sécurité et documentation du réseau, cf. 2.13.3).

La description doit offrir une vue d'ensemble à une personne externe 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 légalité du traitement de données prévu conformément à l'annexe 4, let. A, en particulier :

- respect d'une éventuelle obligation d'annonce au préposé à la protection des données du canton ou au PFPDT
- élaboration d'un règlement de traitement

  Vous trouverez de l'aide dans le modèle « Règlement de traitement ainsi que dans le guide sur les mesures techniques et organisationnelles de la protection des données dans l'annexe 6.

  Le règlement de 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, il faut faire référence au document correspondant en vigueur.

c. Analyse du risque, mesures de protection et risque résiduel

Si, sur la base de l'analyse (examen préalable des risques et/ou analyse des besoins de protection), il ressort qu'un traitement de données personnelles sensibles a lieu, une analyse détaillée du risque doit être établie.

Le concept SIPD renseigne sur le risque résiduel qui subsiste après une analyse de risque au moyen du fichier Excel de l'OFCS (à télécharger sur le site de l'OFCS) et les mesures de protection prises en compte. L'analyse du risque tient compte du risque (élevé) pour la personnalité ou les droits fondamentaux des personnes concernées qui découle :

- 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.

L'analyse porte sur les facteurs de risque pertinents et leurs conséquences en matière de disponibilité, de confidentialité, d'intégrité et de traçabilité. Les résultats sont présentés sous forme d'une liste des risques évalués et de matrice du risque.

Analyse d'impact relative à la protection des données personnelles (AIPD)

L'analyse contient, conformément à la loi (art. 22, al. 3, LPD) :

- 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.

L'analyse d'impact comporte les étapes suivantes :

- description du traitement envisagé ;
- évaluation des risques pour les droits fondamentaux des personnes concernées ;
- identification des mesures de protection des droits fondamentaux ;
- évaluation de l'impact des mesures permettant de déterminer la présence d'un risque élevé.

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[11]. Il existe donc un vaste champ de possibles violations, et il faut évaluer dans quelle mesure la personne concernée pourrait subir une atteinte et quelles mesures permettraient de 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.

[11] Fey Marco, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), loi sur la protection des données (LPD), Bern 2015, Art. 1 N 16)

La protection des droits fondamentaux (droit public)

Les droits fondamentaux sont définis aux art. 7 à 35 de la Constitution fédérale. Dans le contexte des systèmes d'information, il est nécessaire d'évaluer dans quelle mesure le traitement de données peut constituer une atteinte aux droits fondamentaux et de déterminer quelles mesures pourraient y remédier.

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

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

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

Aides / informations supplémentaires

Mémento Analyse d'impact relative à la protection des données personnelles (AIPD) de l'OFAS et modèle

Matrice des risques

L'analyse détaillée des risques peut être effectuée à l'aide du fichier Excel intégré « Analyse des risques AIPD » dans le modèle AIPD de l'OFAS ou dans le fichier Excel de l'OFCS (à télécharger sur le site web de l'OFCS). L'analyse doit déboucher sur la définition de mesures de protection et la description des risques résiduels (voir modèle AIPD de l'OFAS). 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 LPD.

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

d. Rétablissement de l'activité / plan d'urgence (source : OFCS)

Il convient d'élaborer un plan d'urgence pour tout objet à protéger qui sous-tend des processus d'affaires critiques.

Le modèle sur le site de l'OFCS sert de référence.

Le plan d'urgence décrit la planification des cas d'urgence et la prévention des catastrophes pour l'objet à protéger afin de garantir le maintien et le rétablissement des activités dans les situations extraordinaires. Il 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 de gestion de la continuité des activités (cf. ch. 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 annoncées et non annoncées ainsi que pour les contrôles des activités liées à la sécurité de l'information dans le projet, puis dans l'exploitation.

Le contrôle de l'approbation du système est également décrit :

Le processus de développement doit inclure un contrôle approfondi des nouveaux systèmes et des systèmes actualisés, y compris la planification détaillée des activités, des tests et des dépenses attendues dans différentes conditions. De la même manière que pour les projets de développement internes, ces contrôles devraient être effectués dans un premier temps par les développeurs. Ils devraient être suivis par des contrôles d'approbation indépendants (pour les projets internes et externes) garantissant que le système fonctionne comme prévu (et uniquement comme prévu ; cf. ISO/IEC 27002:2022, A.5.8 et A.8.26). L'importance et la nature du système déterminent le nombre et le degré de détails des contrôles.

Résumé de l'audit (qui, quand, quoi, résultat).

f. Mise hors service

Décrit les points auxquels il faut veiller lors de la mise hors service compte tenu des prescriptions d'archivage (cf. directives DGD). La mise hors service est décrite dans la documentation élargie de la SIPD.

Annexe 5 : Exigences relatives aux rôles des organes d'exécution

#	Abréviation	Mission	Description	Chiffre
1	CD	Comité de direction	La direction adopte des lignes directrices relatives à la sécurité de l'information qui s'appuient sur la structure de base du SGSI (ch. 2.2). Elle veille à leur diffusion au sein de l'organe d'exécution et auprès des services externes impliqués, ainsi qu'à leur actualisation régulière.	2.3
2	PSI	Préposé à la sécurité de l'information	Il est entre autres l'interlocuteur de l'OFAS pour les incidents relatifs à la sécurité de l'information pour lesquels les lignes directrices édictées par l'organe d'exécution prévoient une information à l'OFAS (ch. 2.3, point 3).	2.4
3	RA	Responsable d'application	Les organes d'exécution désignent un responsable de l'application pour chaque système d'information utilisé individuellement ou en commun. Celui-ci fixe, avec le préposé à la sécurité de l'information, les exigences de sécurité pour le système d'information. Le responsable de l'application répond de la mise en œuvre des mesures de sécurité.	2.8.5
4	CDP	Chef de projet	Dirige les projets correspondants dans le domaine des systèmes d'information	2.5
5	Admin	Administrateur du réseau/système	Gère le réseau et/ou les infrastructures du serveur	2.4
6	CPD	Conseiller à la protection des données	(art. 25 et art. 26 al. 2 let. a ch. 2 OLPD) Est impliqué lors de l'établissement de la documentation élargie de la SIPD (si des données personnelles sensibles sont traitées avec l'objet protégé)	2.8.3
7	PCE	Personne de confiance	Veille à ce que les collaborateurs se voient attribuer les rôles d'autorisation corrects pour effectuer leur travail (accès aux registres). La personne de confiance est nommée par chaque organe d'exécution et est annoncé à la CdC. La CdC ne peut accorder des autorisations aux collaborateurs de l'organe d'exécution que si la personne de confiance a cosigné la demande.	Directives SAC 2111 - 2112 2311 - 2313
8	RIO	Registration Identification Officer	(art. 59, al. 1, LAVS) Le RIO est tenu de procéder à l'identification de l'utilisateur lors de chaque remise d'un moyen d'authentification (ch. 2203 SAC).	Directives SAC, 2121 - 2125 2201 - 2203 2321 - 2330

Annexe 6 : Aide et modèles

#	Document d'aide / modèle	Source	Télécharger
1	Instrument pour l'évaluation préalable des risques	OFJ	https://www.bj.admin.ch/bj/fr/home/staat/daten-schutz/info-bundesbehoerden.html
2	Mémento et modèle Analyse d'impact relative à la protection des données personnelles (AIPD)	OFAS	https://sozialversicherungen.admin.ch/fr/f/20762
3	Analyse des besoins de protection	OFAS	https://sozialversicherungen.admin.ch/fr/d/20903/download
4	Protection informatique de base	OFAS	https://sozialversicherungen.admin.ch/fr/d/20905/download
5	Concept SIPD	OFAS	https://sozialversicherungen.admin.ch/fr/d/20907/download
6	Analyse des risques	OFCS	https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/erhoehter-schutz.html
7	Règlement de traitement et guide relatif aux mesures techniques et organisationnelles de la protection des données (TOM)	PFPDT	https://www.edoeb.admin.ch/edoeb/fr/home/daten-schutz/internet_technologie/informationssicherheit.html
8	Recommandations techniques relative à la journalisation prévue à l'art. 4 OPDo	OFCS	https://www.edoeb.admin.ch/edoeb/fr/home/daten-schutz/internet_technologie/informationssicherheit.html
9	Guide Implémentation d'un SGSI selon ISO/IEC 27001:2022 (en allemand)	ISACA	https://www.isaca.de/publikationen/publikationen/leitfaeden.html

Liste des abréviations

Abréviation	Terme	Lien
Admin	Administrateur du réseau/système	
AI	Assurance-invalidité	
AIPD	Analyse d'impact relative à la protection des données personnelles	https://sozialversicherungen.admin.ch/fr/f/20762
Al.	Alinéa	
APG	Allocations pour perte de gain	
Art.	Article	
AVS	Assurance-vieillesse et survivants	
BCM	Gestion de la continuité des activités	
CA	Certificate Authority, organisme de certification	
CC	Caisse de compensation	
CdC	Centrale de compensation	
CDP	Chef de projet	
ch.	Chiffre	
CIBIL	Circulaire sur la procédure pour la fixation des prestations dans l'AVS/AI/PC	https://sozialversicherungen.admin.ch/fr/d/6399/download
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
CPD	Conseiller à la protection des données	
Cst.	Constitution fédérale de la Confédération suisse , RS *101*	https://www.admin.ch/opc/fr/classified-compilation/19995395/201801010000/101.pdf
DGD	Directives sur la gestion, la conservation, l'archivage et la destruction des documents dans les domaines AVS/AI/APG/PC/Ptra/AFamAgr/AFam	https://sozialversicherungen.admin.ch/fr/d/6921/download
DRAT	Directives sur la remise d'autres tâches aux caisses de compensation	https://sozialversicherungen.admin.ch/fr/d/6956/download
eAVS/AI	Association des organes d'exécution de l'AVS et de l'AI	https://www.eahv-iv.ch/fr/
eCH	Association de développement de normes dans la cyberadministration	https://www.ech.ch/fr
FF	Feuille fédérale	
FISA	Foreign Intelligence Surveillance Act	https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286
ISACA	Information Systems Audit and Control Association	https://www.isaca.ch/de/
ISO	Organisation internationale de normalisation	
ISO 27001	ISO/IEC 27001 Technologies de l'information – procédures de sécurité informatique – 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 27002	ISO/IEC 27002 Technologies de l'information – procédures de sécurité informatique – guide des mesures de sécurité de l'information	
LAFam	Loi fédérale sur les allocations familiales ; RS *836.2*	https://www.admin.ch/opc/fr/classified-compilation/20042372/index.html

Abréviation	Terme	Lien
Admin	Administrateur du réseau/système	
LAI	Loi fédérale sur l'assurance-invalidité ; RS *831.20*	https://www.admin.ch/opc/fr/classified-compilation/19590131/index.html
LAPG	Loi sur les allocations pour perte de gain ; RS *834.1*	https://www.fedlex.admin.ch/eli/cc/1952/1021_1046_1050/fr
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants ; RS *831.10*	https://www.admin.ch/opc/fr/classified-compilation/19460217/index.html
LFA	Loi fédérale sur les allocations familiales dans l'agriculture ; RS *836.1*	https://www.admin.ch/opc/fr/classified-compilation/19520136/index.html
LOGA	Loi sur l'organisation du gouvernement et de l'administration ; RS 172.10	https://www.admin.ch/opc/fr/classified-compilation/19970118/index.html
LPC	Loi fédérale sur les prestations complémentaires à l'assurance-vieillesse, survivants et invalidité ; RS *831.30*	https://www.admin.ch/opc/fr/classified-compilation/20051695/index.html
LPD	Loi fédérale sur la protection des données ; RS *235.1*	https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html#a5
LPGA	Loi fédérale sur la partie générale du droit des assurances sociales ; RS *830.1*	https://www.admin.ch/opc/fr/classified-compilation/20002163/index.html
LSI	Loi du 20 décembre 2020 sur la sécurité de l'information	https://www.fedlex.admin.ch/eli/fga/2020/2696/fr
O	Ordonnance	
OAFam	Ordonnance sur les allocations familiales ; RS *836.21*	https://www.admin.ch/opc/fr/classified-compilation/20072165/index.html
OAMal	Ordonnance du 27 juin 1995 sur l'assurance-maladie ; RS *832.102*	https://www.admin.ch/opc/fr/classified-compilation/19950219/index.html
OE	Organes d'exécution	
OFCS	Office fédéral de la cybersécurité	https://www.ncsc.admin.ch/ncsc/fr/home.html
OFIT	Office fédéral de l'informatique et de la télécommunication	
OPDo	Ordonnance sur la protection des données , RS *235.11*	https://www.fedlex.admin.ch/eli/cc/2022/568/fr
OTNI	Ordonnance sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale ; RS *172.010.58*	https://www.fedlex.admin.ch/eli/cc/2020/988/fr
PA	Loi sur la procédure administrative, RS 172.021	https://www.admin.ch/opc/fr/classified-compilation/19680294/index.html
PC	Prestations complémentaires	
PCE	Personne de confiance	
PFPDT	Préposé fédéral à la protection des données et à la transparence	https://www.edoeb.admin.ch/edoeb/fr/home.html
PSI	Préposé à la sécurité de l'information (au sens des présentes directives)	
RA	Responsable d'application	
RAVS	Règlement sur l'assurance-vieillesse et survivants ; RS *831.101*	https://www.admin.ch/opc/fr/classified-compilation/19470240/index.html
SAC	Directives sur la sécurité des applications communes (SAC) dans les domaines de l'AVS/AI/APG/PC/AFA/AF	https://sozialversicherungen.admin.ch/fr/d/6867/download
SAS	Service d'accréditation suisse	https://www.sas.admin.ch/sas/fr/home.html
SCI	Système de contrôle interne	

Abréviation	Terme	Lien
Admin	Administrateur du réseau/système	
SCSE	Loi sur la signature électronique ; RS 943.03	https://www.admin.ch/opc/fr/classified-compilation/20131913/index.html
SEPOS	Service spécialisé de la Confédération pour la sécurité de l'information	https://www.sepos.admin.ch/fr/securite-information
SGQ	Système de gestion de la qualité	
SGR	Système de gestion des risques	
SGSI	Système de gestion de la sécurité de l'information	
SI	Système d'information	
SIPD	Sécurité de l'information et protection des données	
TI	Technologie de l'information	