Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Annexes Complementaire

vers les directives 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)

État au 20 Avril 2026

Suivi des modifications

VERSION	DATE	AUTEUR	REMARQUES
1.0	23.01.2026	Markus Burri (OFAS) Markus Moog (OFAS)	Annexes reprises du D-SIPD 2.3

Objet et délimitation

Le document présent contient des documents et des annexes relatifs au D-SIPD qui ne font pas partie intégrante des directives et n'ont pas de caractère normatif. Son contenu sert à des fins d'information, d'explication et d'assistance technique et n'a aucune valeur juridique contraignante. Il ne fonde notamment aucun droit ni aucune obligation.

Seules les directives D-SIPD et les annexes qui y sont expressément mentionnées comme pertinentes pour les directives sont déterminantes pour l'exécution.

Table des matières

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)[1].

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.

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.

[1] FF **2020** 9665

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[2]) 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.

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

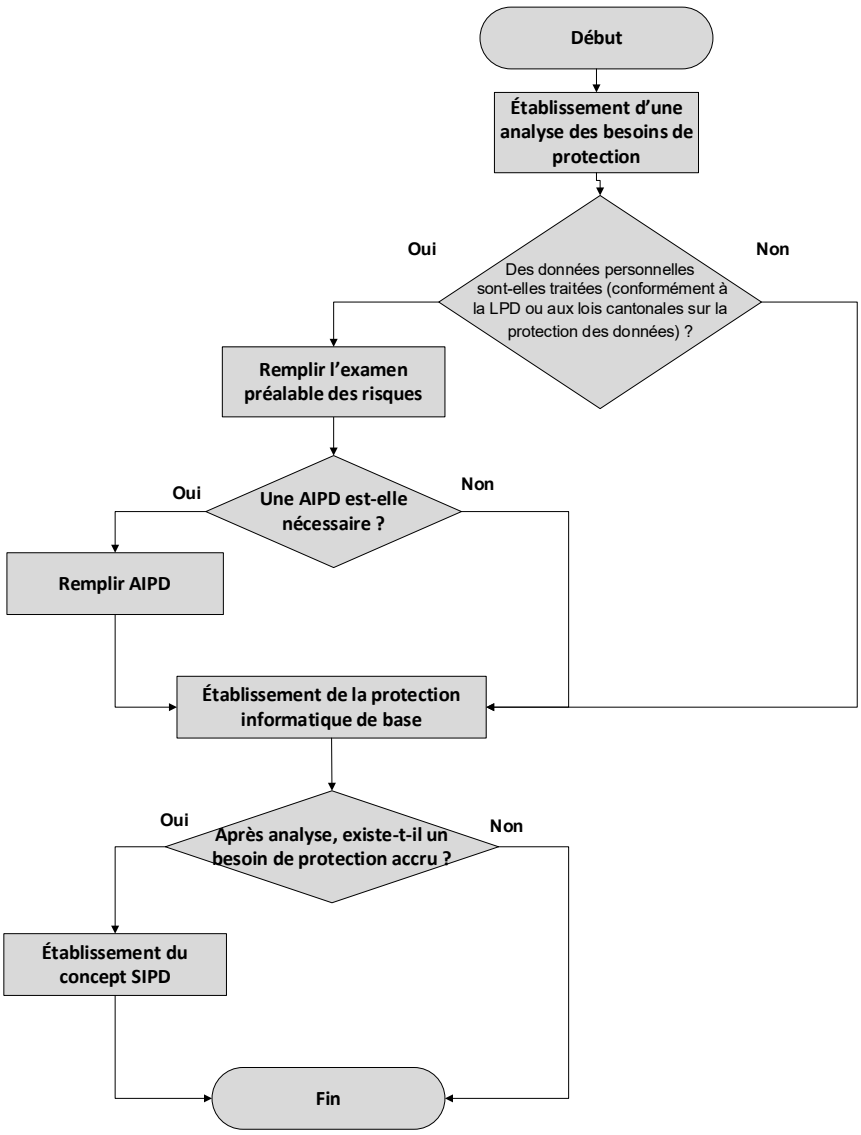
Annexe 2 : Documentation de base de la SIPD

Pour chaque objet de protection, il faut au moins remplir l'analyse des besoins de protection ainsi que la protection IT de base. Si nécessaire, il convient en outre de procéder à l'examen préalable des risques et, le cas échéant, à une analyse d'impact relative à la protection des données.
Liens vers les modèles des documentations à établir voir Annexe . Des modèles cantonaux ou internes peuvent également être utilisés.

- 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 :

Organigramme Analyse des besoins de protection



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). Les organes cantonaux sont soumis aux obligations d'enregistrement/de déclaration de leur canton.	
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).	

#	Question/thème	Base légale	Conséquence, exemple
		Plusieurs organes fédéraux peuvent désigner le même conseiller. Les petits organes fédéraux ou les départements dont l'organisation est centralisée peuvent 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.	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
		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 personnes chargées 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. Modèle pour la classification des exigences de disponibilité

#	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) ?[3] 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.

[3] 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. »

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 ?	Critères de classification
Intégrité normale	Pour les domaines des technologies de l'information et de la communication (TIC) classés au niveau « intégrité nomale », on peut renoncer à des mesures particulières pour conserver l'intégrité.	Les mesures générales pour les appareils et les équipements (ch. 2.11.2 et 2.12.2) doivent garantir l'« intégrité normale ».	Non	Aucun processus critique pour l'activité, aucun impact sur la sécurité en cas de modifications non détectées, aucune exigence en matière de journalisation ou de conformité aux audits
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.	Analyse des conséquences de modifications erronées (changement de version, erreurs de configuration, etc.) ; en cas de conséquences critiques, des tests, une documentation et une mise en œuvre conformément aux exigences du système de gestion de la qualité sont nécessaires. (ch. 2.5, 2.14)	Oui	Les modifications apportées aux données pourraient avoir des répercussions négatives sur l'accomplissement des tâches, la réputation de l'organisation ou les finances. Il existe des exigences en matière de validation, d'assurance qualité et de contrôle des modifications. Aucune traçabilité systématique n'est requise.
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.	Des mécanismes d'enregistrement et de surveillance appropriés (p. ex. journaux d'audit, valeurs de hachage, suivi des modifications) doivent être mis en place afin de pouvoir détecter et documenter les violations de l'intégrité. Ces mesures doivent garantir non seulement que les modifications non autorisées soient empêchées, mais aussi qu'elles puissent être retracées et analysées a posteriori.	Oui	Le traitement concerne des données à caractère personnel ou des données pertinentes pour l'activité, pour lesquelles la traçabilité est exigée par la loi ou l'organisation. L'enregistrement des accès aux données et des modifications apportées à celles-ci est impératif.
Intégrité signée	Pour les domaines des TIC classés au niveau « intégrité signée », on mettra en place en plus des signatures numériques.	Les signatures numériques (par exemple, qualifiées selon VZertES), des mécanismes de contrôle cryptographiques équivalents (par exemple, HMAC) ou des vérifications d'intégrité doivent être utilisés afin de garantir de manière vérifiable l'authenticité et l'inaltérabilité des données. La vérificationd'intégrité doit être effectuée régulièrement au moyen de procédures de vérification automatisées ou manuelles. Cette exigence s'applique uniquement lorsque la version numérique d'un document a valeur probante ou est utilisée comme version de référence.	Oui	Les données ou documents (p. ex. décisions de prestations, notifications) ont une grande valeur probante. Leur caractère contraignant, leur authenticité et leur intégrité doivent pouvoir être démontrées de manière incontestable.

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)

Important: les exemples ci-dessous ne doivent pas être confondus avec les niveaux de classification selon les articles 18 à 20 de l'Ordonnance sur la sécurité de l'information dans l'administration fédérale et l'armée (OSI). La désignation des groupes de protection peut être effectuée à la discrétion de chacun.

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**[4]	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**[5]	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

L'administration fédérale a défini les classifications suivantes dans l'ordonnance sur la sécurité de l'information[6] (OSI) :

- Interne
- Confidentiel
- Secret

Dans le domaine du cloud computing en particulier (qui inclut l'utilisation de M365), il existe des restrictions pour le stockage et le traitement des données de niveau «confidentiel» et «secret».

[4] Pas au sens de l'article. 18 OSI

[5] Pas au sens de l'article. 19 OSI

[6] Ordonnance sur la sécurité de l'information dans l'administration fédérale et l'armée (OSI)

Annexe 3 : 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 . Des modèles cantonaux ou internes peuvent également être utilisés.

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[7]. 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.

[7] 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, dans le fichier Excel de l'OFCS (à télécharger sur le site web de l'OFCS) ou selon les modèles internes ou cantonaux. 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 4 : Exigences relatives aux rôles des organes d'exécution

#	Abréviation	Mission	Description
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. **Fehler! Verweisquelle konnte nicht gefunden werden.**). 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	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. **Fehler! Verweisquelle konnte nicht gefunden werden.**, point 3).
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.
4	CDP	Chef de projet	Dirige les projets correspondants dans le domaine des systèmes d'information
5	ARS	Administrateur du réseau/système	Gère le réseau et/ou les infrastructures du serveur, mise en œuvre de mesures techniques de sécurité
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)

Exemple d'attribution des rôles (Responsible) pour la mise en œuvre des exigences de la D-SIPD

Cet exemple sert de guide ; la mise en œuvre concrète peut varier selon les organes d'exécution.

Chiffre	Exigences	CD	PSI	RA	CPD	CDP	ARS
2.2	Structure de base du SGSI de l'organe d'exécution		X				
2.3	Lignes directrices relatives à la sécurité de l'information	(X)	X				
2.4	Exigences relatives à l'organisation de la sécurité de l'information		X				
2.5	Exigences applicables aux projets dans le domaine des systèmes d'information					X	
2.6	Sécurité de l'information pour les appareils mobiles et le travail mobile						X
2.7.1	Sécurité du personnel		X				
2.7.2	Information et formation		X				
2.7.3	Changement de situation						X
2.8.1	inventaire de tous les systèmes d'information		X				
2.8.2	Documentation de base de la SIPD		X				
2.8.3	Documentation élargie de la SIPD		X				
2.8.4	Actualisation de la documentation de la SIPD		X				
2.8.5	Responsable de l'application			X			
2.9	Gestion de l'accès aux systèmes d'information						X
2.10.1	Cryptographie						X
2.11.1	Dispositif de sécurité pour les locaux						X
2.11.2	Mesures pour les appareils et les équipements						X
2.12	Mesures de sécurité opérationnelle						X
2.13	Documentation de l'architecture (ch. 2.13.1 - 2.13.4)						X
2.14	Modifications des systèmes d'information					X	
2.15.1	Contrats avec des tiers	X					
2.15.2	L'utilisation de M365		X		(X)		
2.16	Gestion des incidents relatifs à la sécurité de l'information		X				
2.17	Maintien de la sécurité de l'information (gestion de la continuité des activité)						X
2.18	Conformité aux directives		X				

Les combinaisons de rôles sont admises à condition que la séparation des fonctions soit respectée, . L'unité d'exécution les documente et veille à ce que les compétences et ressources nécessaires soient garanties pour chaque rôle.

Annexe 5 : 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/dow-nload
4	Protection informatique de base	OFAS	https://sozialversicherungen.admin.ch/fr/d/20905/dow-nload
5	Concept SIPD	OFAS	https://sozialversicherungen.admin.ch/fr/d/20907/dow-nload
6	Analyse des risques	OFCS	https://www.ncsc.admin.ch/ncsc/fr/home/dokumenta-tion/sicherheitsvorgaben-bund/sicherheitsverfahren/er-hoehter-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/fr/securite-de-linformation
8	Recommandations techniques relative à la journali-sation prévue à l'art. 4 OPDo	OFCS	https://www.edoeb.admin.ch/fr/securite-de-linformation
9	Guide Implémentation d'un SGSI selon ISO/IEC 27001:2022 (en allemand) (allemand)	ISACA	https://www.isaca.de/publikationen/publikationen/leitfae-den.html