



Guide sur l'analyse d'impact relative à la protection des données personnelles (Guide AIPD)

30 novembre 2023 (État au 1^{er} janvier 2026)

Table des matières

1	Destinataires du guide	2
2	Démarches en vue de réaliser une AIPD	2
2.1	Qui doit réaliser une AIPD ?	2
2.2	Quand faut-il réaliser une AIPD ?	3
2.3	Quand faut-il consulter le PFPDT ?	4
2.4	Sous quelle forme et pendant combien de temps l'AIPD doit-elle être conservée ?	5
2.5	Faut-il publier l'AIPD ?	5
3	Contenu de l'AIPD	5
3.1	Remarques liminaires : fondements de l'AIPD et méthodologie	5
3.2	Indications générales	6
3.3	Description du traitement envisagé de données personnelles	7
3.4	Évaluation des risques pour les droits fondamentaux de la personne concernée	8
3.5	Identification des mesures prévues pour protéger les droits fondamentaux de la personne concernée	13
3.6	Évaluation des effets des mesures prévues afin de déterminer s'il existe un risque résiduel élevé	14
3.7	Consultation du PFPDT en cas de risque résiduel élevé	15
3.8	Synthèse et résultats de l'AIPD	16
	Annexe : check-list du contenu de l'AIPD	17
	Première partie : indications générales	17
	Deuxième partie : description du traitement envisagé de données personnelles	17
	Troisième partie : évaluation du risque pour les droits fondamentaux de la personne concernée	18
	Quatrième partie : identification des mesures prévues pour protéger les droits fondamentaux de la personne concernée	18
	Cinquième partie : évaluation des effets des mesures prévues afin de déterminer s'il reste un risque résiduel élevé	19
	Sixième partie : synthèse et résultats de l'AIPD	19

1 Destinataires du guide

Le guide AIPD s'adresse avant tout aux unités de l'administration fédérale centrale¹ qui sont tenues de réaliser une analyse d'impact relative à la protection des données personnelles (AIPD) au sens de l'art. 22 de la loi fédérale du 25 septembre 2020 sur la protection des données (LPD)² et des Directives du Conseil fédéral concernant l'examen préalable des risques et l'analyse d'impact relative à la protection des données personnelles en cas de traitement de données personnelles par l'administration fédérale (Directives AIPD)³.

Les unités de l'administration fédérale décentralisée⁴, au même titre que les personnes chargées d'une tâche publique de la Confédération, bien que non soumises aux Directives AIPD, sont tout de même tenues de respecter la loi sur la protection des données, dans la mesure où elles sont considérées comme des organes fédéraux⁵. Ces différentes entités doivent donc procéder à une analyse d'impact relative à la protection des données personnelles (AIPD) lorsque les conditions de l'art. 22 LPD sont remplies. Dans cette optique, elles sont libres de recourir aux prescriptions des Directives AIPD, ainsi qu'aux instruments d'accompagnement, tels que le présent guide.

L'AIPD permet aussi de démontrer que le traitement de données personnelles envisagé est conçu dans le respect du droit de la protection des données (*privacy by design*)⁶. En outre, elle permet aux responsables du traitement de vérifier si les données qu'ils traitent le sont de manière conforme aux exigences en matière de protection des données.

Délimitation par rapport à l'aide-mémoire concernant l'analyse d'impact relative à la protection des données personnelles (AIPD) selon les art. 22 et 23 LPD du Préposé fédéral à la protection des données et à la transparence (PFPDT) : le guide de l'OFJ porte uniquement sur la réalisation de l'AIPD par l'administration fédérale centrale. L'[aide-mémoire du PFPDT](#) en revanche s'adresse en premier lieu aux responsables du traitement des données privés, mais peut également servir d'aide à l'interprétation pour les organes fédéraux.

2 Démarches en vue de réaliser une AIPD

2.1 Qui doit réaliser une AIPD ?

La loi se limite à dire que le responsable du traitement procède à une AIPD. En vertu de l'art. 5, let. j, LPD, l'unité administrative responsable est l'entité qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données. Cette unité doit veiller à ce que l'AIPD soit réalisée, mais elle n'est pas tenue d'y procéder elle-même.

¹ Au sens de l'art. 7 de l'Ordonnance sur l'organisation du gouvernement et de l'administration (OLOGA, RS 172.010.1). Dans le contexte du droit de la protection des données, ces unités sont considérées comme des organes fédéraux (voir l'art. 5, let. i LPD qui définit l'organe fédéral comme étant « l'autorité fédérale, le service fédéral ou la personne chargée d'une tâche publique de la Confédération », RS 235.1).

² RS 235.1.

³ FF 2023 1882.

⁴ Au sens de l'art. 7a OLOGA.

⁵ Voir l'art. 5, let. i, LPD.

⁶ Art. 7, al. 1 et 2 LPD.

Il est important de préciser que la réalisation d'une AIPD nécessite des connaissances spécifiques dans différents domaines (droit, informatique, etc.). Par conséquent, une AIPD devrait idéalement être réalisée par une équipe interdisciplinaire ayant des compétences dans le domaine de la protection des données, de l'identification des risques et des processus et systèmes informatiques.

En outre, le conseiller ou la conseillère à la protection des données de l'unité administrative conseille le responsable du traitement et vérifie l'exécution de l'AIPD⁷. Pour une meilleure prise en compte du droit de la protection des données, il est important de l'inclure tout au long du processus. Notons encore qu'il ou elle doit pouvoir exercer sa fonction de manière indépendante par rapport à l'unité de l'administration fédérale responsable et sans recevoir d'instruction de sa part⁸.

Même si un responsable du traitement envisage par la suite de confier le traitement des données personnelles à un sous-traitant, il reste responsable de réaliser l'AIPD.

A préciser qu'une AIPD doit être effectuée même si, par exemple, un projet législatif règle le traitement de données par un tiers : il est notamment fait référence au traitement des données par des entreprises proches de la Confédération dans le cadre d'une concession (par exemple La Poste, les CFF, Swisscom, Skyguide). Dans ce contexte, plus concrètement, il appartient à l'unité administrative compétente de demander au tiers de réaliser une AIPD. L'unité administrative responsable veille ainsi à la mise en œuvre de l'AIPD et joint ses résultats aux documents de la consultation des offices.

2.2 Quand faut-il réaliser une AIPD ?

Une AIPD doit être réalisée en cas de risque élevé pour les droits fondamentaux d'une personne concernée. Pour déterminer s'il existe un risque élevé, il convient de recourir à l'[instrument d'examen préalable des risques](#), élaboré par l'Office fédéral de la justice (OFJ) et qui présente les principaux facteurs de risques.

L'art. 22 LPD prévoit des exceptions à la réalisation d'une AIPD pour les responsables privés, mais pas pour les unités administratives. Si l'instrument d'examen préalable des risques indique qu'il existe un risque élevé pour les droits fondamentaux des personnes concernées, une AIPD est obligatoire. L'art. 22, al. 1, LPD prévoit la possibilité d'établir une AIPD commune lorsque plusieurs opérations de traitement semblables sont envisagées.

Cette disposition exige que l'AIPD soit réalisée « au préalable », c'est-à-dire que le risque et son impact soient évalués avant d'entamer le traitement de données personnelles. Idéalement, l'AIPD sera établie le plus tôt possible, même si tous les paramètres du traitement ne sont pas encore connus.

L'AIPD devrait être réalisée dès que l'unité de l'administration fédérale responsable envisage un nouveau traitement de données. Un projet de traitement de données personnelles peut soit être nouveau, soit être une adaptation d'un traitement en cours. Pour les traitements en cours avant l'entrée en vigueur de la nouvelle LPD, l'art. 69 LPD prévoit une réglementation précise : une AIPD

⁷ Art. 26, al. 2, let. a, ch. 2 de l'ordonnance du 31 août 2022 sur la protection des données (OPDo), RS 235.11.

⁸ Art. 26, al. 1, let. b, OPDo.

ne doit être établie que si les finalités du traitement en question changent ou si de nouvelles catégories de données sont collectées.

La réalisation de l'AIPD s'inscrit ainsi dans un processus itératif. En effet, l'analyse doit être effectuée en parallèle avec la conception des bases légales prévoyant le traitement de données et elle doit être adaptée au fur et à mesure que le projet de traitement se précise (par exemple au moment de l'élaboration d'une ordonnance ou de la mise en place des systèmes ou des registres de données). Conformément à la procédure en vigueur, une première version initiale est jointe aux documents de la consultation des offices, et, selon le contexte, est présentée au PFPDT. Toutefois, par la suite, l'AIPD doit être mise à jour de manière régulière en complétant la version précédente (en précisant à chaque fois la date de la nouvelle version) lorsque des éléments nouveaux apparaissent.

Coordination avec la procédure normative (ch. 4 Directives AIPD) : si le traitement des données nécessite une nouvelle base légale ou l'adaptation d'une base légale existante, l'AIPD doit être réalisée avant l'élaboration ou la modification de la base légale, puisque les résultats de l'AIPD doivent être joints au dossier de consultation des offices. Si la nécessité de procéder à une AIPD ou de l'adapter n'est apparue qu'après l'ouverture de la consultation des offices, les résultats de l'AIPD sont joints au dossier de la consultation des offices suivante ou de la procédure de co-rapport.

Coordination avec la méthode de gestion de projet HERMES⁹ (ch. 5 Directives AIPD) : si le traitement des données intervient dans le cadre d'un projet HERMES, la réalisation de l'AIPD commence lors de la phase de création de la solution. Le terme « création de la solution » se rapporte à l'utilisation soit d'une méthode classique soit de la méthode agile. HERMES admet le recours à d'autres méthodes, mais il en définit toujours le cadre. Dans la méthode classique, la phase de la création de la solution correspond à l'étape de la conception. Dans la méthode agile, l'AIPD doit se faire au fur et à mesure. Idéalement, l'AIPD sera dans ce cas établie en même temps que le concept SIPD.

2.3 Quand faut-il consulter le PFPDT ?

Si l'AIPD révèle que le traitement envisagé, malgré les mesures envisagées par l'unité administrative responsable, comporte toujours un risque élevé (pour la définition d'un risque résiduel élevé, voir chapitres 3.4.2 et 3.6) pour les droits fondamentaux de la personne concernée, celle-ci doit consulter le PFPDT avant de procéder au traitement.

Il convient de mentionner que cette consultation peut prendre du temps. Par conséquent, la transmission d'un dossier complet contribue à optimiser l'efficacité du processus. Le guide traite plus précisément de ces questions dans le cadre du chapitre 3.7.

En cas de coordination avec la procédure normative, le PFPDT doit être consulté avant la consultation des offices (voir encadré ci-dessus).

⁹ www.hermes.admin.ch

2.4 Sous quelle forme et pendant combien de temps l'AIPD doit-elle être conservée ?

La LPD et l'ordonnance du 31 août 2022 sur la protection des données (OPDo)¹⁰ ne contiennent aucune prescription concernant la forme de l'AIPD. Comme pour d'autres instruments de la LPD et de l'OPDo, il appartient à l'unité administrative compétente de définir sous quelle forme elle conserve l'AIPD. Il est cependant essentiel que l'unité puisse prouver qu'elle a procédé à l'analyse et elle doit être en mesure de remettre le document au PFPDT et de joindre les résultats pour les besoins de la consultation des offices. En d'autres termes, l'AIPD et ses résultats doivent être lisibles dans un format usuel.

S'agissant de la conservation de l'AIPD, l'art. 14 OPDo prescrit que l'unité administrative responsable doit l'assurer pendant deux ans au moins à compter de la fin du traitement des données.

2.5 Faut-il publier l'AIPD ?

La LPD et l'OPDo ne prévoient aucune obligation de publier l'AIPD, car elle peut contenir des informations délicates. Une publication peut toutefois être considérée, dans la perspective d'un renforcement de la protection des droits fondamentaux des personnes concernées, laquelle constitue précisément le but d'une AIPD. Elle assure une meilleure transparence au sujet du traitement de données personnelles. De plus, la relation de confiance entre la personne concernée et le responsable du traitement s'en trouve consolidée. Il appartient à l'unité administrative responsable de décider de l'opportunité d'une publication.

Pour le reste, les dispositions de la loi du 17 décembre 2004 sur la transparence¹¹ s'appliquent également à l'AIPD.

Coordination avec la procédure normative (ch. 4 Directives AIPD) : lorsque la réalisation de l'AIPD intervient dans le cadre d'une procédure normative, les résultats¹² de l'AIPD doivent être joints au dossier de la consultation des offices. Par ailleurs, l'unité administrative responsable (Département ou ChF) informe des résultats de l'AIPD notamment dans la proposition au Conseil fédéral, le rapport explicatif, le message et la brochure des Explications du Conseil fédéral.

3 Contenu de l'AIPD

3.1 Remarques liminaires : fondements de l'AIPD et méthodologie

Selon l'art. 22, al. 3, LPD, « l'analyse d'impact contient une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, ainsi que les mesures prévues pour protéger sa personnalité et ses droits fondamentaux ».

Le ch. 3, al. 1, des Directives AIPD précise par ailleurs que « l'AIPD comprend les étapes suivantes :

- a. description du traitement envisagé ;

¹⁰ RS 235.11.

¹¹ RS 152.3.

¹² Voir chapitre 3.8 ci-dessous concernant les résultats de l'AIPD.

- b. évaluation des risques pour les droits fondamentaux de la personne concernée ;
- c. identification des mesures prévues pour protéger les droits fondamentaux ;
- d. évaluation des effets des mesures prévues pour déterminer s'il existe un risque résiduel élevé. »

L'AIPD réalisée par l'unité administrative responsable doit au moins porter sur les quatre points mentionnés ci-dessus.

Coordination avec la méthode de gestion de projet HERMES (ch. 5 Directives AIPD) : lorsque la méthode de gestion de projet HERMES est appliquée, certaines parties de l'AIPD se déroulent dans ce cadre : ainsi, l'analyse des bases légales et les instruments qui sont établis en cas de besoin de protection accru¹³ font partie intégrante de l'AIPD.

3.2 Indications générales

La partie de l'AIPD relative aux indications générales porte essentiellement sur les mêmes éléments que ceux figurant dans la première partie de l'[instrument d'examen préalable des risques](#).

Elle doit notamment contenir des informations sur l'unité administrative responsable, ainsi que sur la personne de contact au sein de cette unité.

Les indications générales doivent également présenter les bases légales existantes ou prévues pour le traitement envisagé. Cette analyse révèle s'il existe des bases légales et, le cas échéant, lesquelles, s'il faut en créer ou en adapter¹⁴. L'unité de l'administration fédérale responsable doit par conséquent comparer les bases légales existantes à celles qui sont prévues.

Coordination avec la méthode de gestion de projet HERMES (ch. 5 Directives AIPD) : si la méthode de gestion de projet HERMES est appliquée, il est possible de reprendre les explications concernant les bases légales existantes ou à créer de l'analyse des bases légales effectuée dans le cadre d'HERMES pour autant que celle-ci soit encore actuelle.

Cette partie indiquera aussi l'identité du conseiller ou de la conseillère à la protection des données de l'unité de l'administration fédérale responsable et précisera si cette personne a été consultée dans le cadre de l'AIPD.

Coordination avec la procédure normative (ch. 4 Directives AIPD) : dans les indications générales, l'unité administrative doit préciser si l'AIPD a lieu dans le cadre d'une procédure normative, en particulier de la révision d'une loi ou d'une ordonnance. Lors de la coordination avec la procédure normative, il faut tenir compte des exigences des Directives AIPD.

Coordination avec la méthode de gestion de projet HERMES (ch. 5 Directives AIPD) : il faut également mentionner dans les indications générales si l'AIPD a été ou non réalisée dans le cadre d'HERMES. La coordination avec HERMES est réglée dans les Directives AIPD.

¹³ www.ncsc.admin.ch > Documentation > Directives de sécurité informatique > Procédure de sécurité > Protection élevée.

¹⁴ L'analyse peut être réalisée dans le cadre d'HERMES : <https://www.hermes.admin.ch/fr/>.

Aperçu des indications générales

Unité(s) administrative(s) responsable(s)	
Personne de contact (nom, prénom, tél., courriel)	
Bases légales existantes ou prévues	
Conseiller ou conseillère à la protection des données (nom, prénom, tél., courriel)	
Coordination avec la procédure normative	Oui <input type="checkbox"/> Non <input type="checkbox"/>
Application d'HERMES	Oui <input type="checkbox"/> Non <input type="checkbox"/>

3.3 Description du traitement envisagé de données personnelles

Il faut commencer par décrire le traitement envisagé (art. 22, al. 3, LPD). D'une manière générale, la partie de l'AIPD relative à la description du traitement envisagé de données personnelles porte sur les mêmes éléments que ceux figurant dans la deuxième partie de l'[instrument d'examen préalable des risques](#) (intitulé « indications sur le traitement »).

Cette description englobe la nature, l'étendue et les finalités du traitement ainsi que les conditions dans lesquelles il se déroulera (art. 22, al. 2, LPD). L'unité administrative responsable indique qui traitera quelles données, dans quel but et comment. Lors de l'extension et du développement d'applications et de systèmes existants, la description du traitement envisagé doit également comprendre une comparaison avec le traitement actuel.

La description détaillée du traitement envisagé fonde l'évaluation des risques consécutive (voir chapitre 3.4). Lorsque survient un risque pour la sécurité de l'information, le traitement envisagé peut avoir un impact plus grave sur la personne concernée s'il s'agit de données personnelles sensibles.

L'unité administrative responsable doit préciser qui traitera les données. Il faut notamment indiquer s'il y a plusieurs responsables du traitement¹⁵ ou s'il est prévu de confier des tâches à un sous-traitant¹⁶.

Il faut en outre préciser le type de données qui seront traitées. Pour les catégories de données, il convient en particulier de spécifier si et dans quelle mesure le traitement englobe des données personnelles¹⁷ et spécialement des données personnelles sensibles¹⁸. Il faut en outre indiquer la forme des données visées (p. ex. texte, son, image). Les catégories de personnes concernées (p. ex. employés, assurés) doivent également être décrites. Si le traitement inclut des données portant sur des personnes vulnérables (p. ex. atteintes d'un handicap physique ou psychique, mineurs, seniors) il faut en tenir compte et il convient d'examiner s'il peut en résulter un besoin de protection particulier.

¹⁵ L'art. 5, let. j, LPD définit le terme « responsable du traitement ».

¹⁶ L'art. 5, let. k, LPD définit le terme « sous-traitant ».

¹⁷ L'art. 5, let. a, LPD définit le terme « données personnelles ».

¹⁸ L'art. 5, let. c, LPD contient une liste exhaustive des données personnelles sensibles (données sensibles). Pour les exemples, voir l'[instrument d'examen préalable des risques](#).

Les indications comprennent également une description de la nature de traitement. L'unité administrative responsable doit expliquer quel(s) type(s) de traitement(s) elle envisage et comment celui-ci (ceux-ci) va (vont) se dérouler. Ces informations portent notamment sur les types de traitements suivants : collecte, enregistrement, conservation, utilisation, modification, communication, archivage, effacement ou destruction de données¹⁹. Il faut ainsi spécifier si les données personnelles sont collectées secrètement (c.-à-d. à l'insu de la personne concernée)²⁰, si elles résultent d'une interconnexion ou d'un appariement avec d'autres bases de données²¹, si et comment elles sont communiquées à des tiers (p. ex. par un accès en ligne²² ou communiquées à l'étranger²³). Il doit ressortir de la description si un profilage ou un profilage à risque élevé²⁴ est prévu ou si des décisions individuelles automatisées²⁵ seront prises. L'unité administrative responsable doit indiquer si le traitement comprend une surveillance de personnes²⁶.

Il faut également préciser au moyen de quelles technologies se fera le traitement des données, et comment il sera mis en œuvre sur le plan technique (p. ex. logiciel, réseau). En l'occurrence, il faut prendre en compte le mode de traitement des données et déterminer s'il se fonde ou recourt à de nouvelles technologies ou à des technologies qui, sans être nouvelles, comportent des risques pour les droits fondamentaux de la personne concernée ou dont l'impact sur les droits fondamentaux de la personne concernée ne peut pas être évalué ; on songe ici à l'intelligence artificielle par exemple²⁷.

L'étendue du traitement des données doit être déterminée avec précision. Les informations fournies doivent révéler si le traitement portera sur un important volume de données, si un grand nombre de personnes sera touché et si le traitement sera de grande envergure sur le plan temporel ou géographique²⁸. Pour la dimension temporelle, il faut indiquer la durée pendant laquelle des données personnelles seront traitées et conservées. Pour savoir s'il s'agit d'un traitement à grande échelle, on peut se demander si le traitement de données personnelles constitue l'activité principale de l'unité administrative responsable. Ce critère n'est toutefois pas déterminant à lui seul pour estimer l'étendue du traitement ; il doit être considéré en relation avec d'autres critères²⁹.

La description doit indiquer également les finalités du traitement, plus précisément à quelles fins les données personnelles sont collectées et traitées.

3.4 Évaluation des risques pour les droits fondamentaux de la personne concernée

D'une manière générale, la partie de l'AIPD relative à l'évaluation des risques pour les droits fondamentaux de la personne concernée est liée à ce qui figure dans la troisième partie de

¹⁹ Art. 5, let. d, LPD.

²⁰ Pour les exemples, voir l'[instrument d'examen préalable des risques](#).

²¹ Pour les exemples, voir l'[instrument d'examen préalable des risques](#).

²² L'accès en ligne constitue une forme de communication spécifique. Le destinataire peut accéder lui-même aux données personnelles, sans que le responsable n'intervienne (principe du self-service).

²³ Art. 16 ss LPD.

²⁴ Le profilage et le profilage à risque élevé sont définis à l'art. 5, let. f et g, LPD. Pour les exemples, voir l'[instrument d'examen préalable des risques](#).

²⁵ L'art. 21, al. 1, LPD définit le terme « décision individuelle automatisée ». Pour les exemples, voir l'[instrument d'examen préalable des risques](#).

²⁶ Pour les exemples, voir l'[instrument d'examen préalable des risques](#).

²⁷ Pour d'autres exemples, voir l'[instrument d'examen préalable des risques](#).

²⁸ Pour les exemples, voir l'[instrument d'examen préalable des risques](#).

²⁹ Pour les exemples, voir l'[instrument d'examen préalable des risques](#).

l'[instrument d'examen préalable des risques](#) (intitulée « évaluation globale du risque élevé »). Si ces indications peuvent être utiles, elles ne suffisent cependant pas. Dans l'AIPD, il faut identifier les risques et pour chaque risque, il convient encore de déterminer la probabilité d'occurrence du risque, ainsi que l'impact du risque sur les droits fondamentaux de la personne concernée. Pour la gravité, respectivement l'impact du risque sur les droits fondamentaux de la personne concernée, les facteurs de risques identifiés dans l'instrument d'examen préalable des risques peuvent constituer un indice.

3.4.1 Identification des risques

La notion de risque se rapporte à un événement potentiel qui a ou pourrait avoir un impact sur les droits fondamentaux de la personne concernée. L'évaluation des risques vise à déterminer la probabilité et l'impact que les risques ont ou pourraient avoir sur les personnes concernées. Il faut commencer par identifier les risques d'un traitement.

Il existe différents types de risques. Les **risques liés à la sécurité de l'information** sont en relation avec la sécurité des données.

Exemples (voir aussi la liste des risques dans l'analyse détaillée de risque du concept SIPD³⁰) :

- Violation de l'intégrité des données personnelles, par exemple par une manipulation ou par des erreurs du système ;
- Violation de la confidentialité, par exemple en raison de failles du système, d'une utilisation abusive des informations ou d'une attaque contre le système ;
- Violation de la disponibilité, par exemple suite à une panne du système, d'une perte d'information ou d'un ransomware ;
- Violation de la traçabilité, due par exemple à une falsification ou à la perte des procès-verbaux de journalisation.

Les **risques de protection des données** se rapportent aux différents types de traitement des données. Ils dépassent le cadre de la sécurité des données.

Exemples :

- Collecte et traitement illicites de données personnelles ;
- Utilisation de données personnelles à des fins autres que celles qui étaient envisagées ;
- Traitement de données incorrectes ;
- Accès non autorisé à des données personnelles ;
- Conservation de données personnelles pendant une durée trop longue ;
- Négation des droits des personnes concernées.

L'identification des risques dépend des circonstances, c'est-à-dire de chaque traitement envisagé. Les responsables doivent décrire les scénarios envisageables pour chaque type de risque. Ainsi, pour le risque d'accès non autorisé à des données personnelles, il se pourrait que des collaborateurs internes accèdent à de telles données, alors qu'ils n'en ont pas besoin pour l'accomplissement de leurs tâches. Il est envisageable également que des personnes externes

³⁰ Le modèle pour l'analyse de risque du concept SIPD peut être téléchargé à l'adresse suivante : www.ncsc.admin.ch > Documentation > Directives de sécurité informatique > Procédure de sécurité > Protection élevée.

accèdent illicitement à des données personnelles (p. ex. attaque pirate) (voir tableau des exemples au chapitre 3.4.2).

Lors de l'identification des risques, il est important de veiller à ce que leur définition soit pertinente eu égard à la protection des données personnelles. Il faut éviter de retenir des risques abstraits qui n'ont qu'un effet indirect sur la protection des données personnelles (p. ex. tremblements de terre).

En outre, les mesures à prévoir ne jouent aucun rôle au stade de l'évaluation des risques. La réglementation des autorisations d'accès par exemple ne doit pas être établie à ce stade ; elle n'interviendra que si l'évaluation des risques conclut qu'il faut prévoir des mesures afin d'empêcher des accès non autorisés.

Coordination avec la méthode de gestion de projet HERMES (ch. 5 Directives AIPD) : si l'analyse des besoins de protection indique un besoin élevé, il convient de procéder à une analyse détaillée des risques dans le cadre du concept SIPD. Cette analyse a pour but de repérer et d'évaluer les risques pour la sécurité de l'information. Le concept SIPD fait partie intégrante de l'AIPD. Les risques pour la protection des données doivent être évalués séparément ou dans le cadre du concept SIPD.

3.4.2 Évaluation des risques

L'évaluation des risques vise notamment à déterminer la probabilité d'occurrence des risques identifiés et l'impact qu'ils auraient (ou pourraient avoir) sur les droits fondamentaux des personnes concernées.

Elle peut être réalisée à l'aide de la matrice des risques « 6 x 6 », qui est également utilisée pour l'analyse détaillée dans le cadre concept SIPD³¹.

Impact	très élevé 6						
	élevé 5						
	important 4						
	modéré 3						
	faible 2						
	très faible 1						
		très improbable 1	improbable 2	rare 3	possible 4	probable 5	très probable 6
		Probabilité					

³¹ Le modèle pour l'analyse de risque du concept SIPD peut être téléchargé à l'adresse suivante : www.ncsc.admin.ch > Documentation > Directives de sécurité informatique > Procédure de sécurité > Protection élevée.

Pour ce qui est de l'impact, il peut être d'ordre physique (p. ex. un traitement médical erroné en raison de données inexactes), matériel (p. ex. perte d'emploi, utilisation abusive de la carte de crédit, perception de taxes injustifiées) ou immatériel (p. ex. discriminations, notamment racisme, sexisme, désavantages sociaux, stigmatisation en raison d'une maladie). L'impact sur les droits fondamentaux de la personne concernée ou la gravité du risque peuvent être classés en six niveaux : très faible, faible, modéré, important, élevé, très élevé. Ces niveaux peuvent être décrits comme suit :

- Très faible : pas d'impact sur les droits fondamentaux ; pas de préjudices moraux ou sociaux notables ; pas de dommage financier ayant un lien de causalité adéquate. Exemples : léger dépassement de la durée de conservation admise pour les données personnelles ; appels téléphoniques ou messages indésirables sans conséquence directe ou indirecte.
- Faible : impact négligeable sur les droits fondamentaux ; préjudices moraux ou sociaux à peine perceptibles ; éventuel dommage financier minimal ayant un lien de causalité adéquate. Exemple : nécessité de modifier ses identifiants, adresse électronique ou numéro de téléphone.
- Modéré : impact sur les droits fondamentaux faible sur le long terme ou grave à court terme ; faibles préjudices psychiques, moraux ou sociaux ; éventuel dommage financier ayant un lien de causalité adéquate. Exemple : influence cachée et non autorisée sur le comportement d'achat.
- Important ou élevé³² : impact sur les droits fondamentaux grave sur le long terme ; préjudices physiques, psychiques, moraux ou sociaux de gravité moyenne ; dommage financier substantiel ayant un lien de causalité adéquate. Exemples : refus/résiliation d'un contrat ; dégâts de réputation.
- Très élevé : impact fatal sur les droits fondamentaux ; préjudices graves sur le plan physique, psychique, moral ou social ; dommage financier ayant un lien de causalité adéquate dont la gravité menace l'existence. Exemple : mauvais traitement médical ayant des conséquences graves, en raison d'une identification erronée du patient ou d'informations erronées à son sujet ; risques de répression transnationale en raison de données personnelles des requérants d'asile qui parviendraient à l'État d'origine avec des risques pour la personne concernée ou sa famille (intégrité physique, vie, etc.).

La probabilité d'occurrence est une estimation de la probabilité qu'un événement spécifique survienne dans un intervalle de temps donné. Elle peut également être définie par six niveaux : très improbable, improbable, rare, possible, probable, très probable. Pour l'évaluation de la probabilité, il est possible de s'appuyer sur la légende figurant dans le concept SIPD utilisé pour l'analyse de risque détaillée³³. La probabilité est évaluée comme suit :

- Très improbable : moins d'une fois tous les 10 ans
- Improbable : tous les 5 à 10 ans
- Rare : tous les 3 à 5 ans
- Possible : tous les 2 à 3 ans
- Probable : tous les 1 à 2 ans
- Très probable : plusieurs fois par année

³² La nuance entre ces deux catégories est difficile à établir et dépend du cas d'espèce.

³³ Le modèle pour l'analyse de risque du concept SIPD peut être téléchargé à l'adresse suivante : www.ncsc.admin.ch > Documentation > Directives de sécurité informatique > Procédure de sécurité > Protection élevée.

Lors de l'évaluation des risques, il s'avère ardu d'estimer les risques de manière fiable. D'une part, il n'est pas aisé de définir à l'avance la probabilité d'occurrence, car il est difficile de prévoir si et quand un risque se concrétisera. D'autre part, il peut s'avérer complexe d'estimer l'impact d'un risque. Si l'on considère le risque d'un accès non autorisé, il peut s'avérer délicat de prédire ce qu'il adviendra des données personnelles et quel sera l'impact sur les droits fondamentaux des personnes concernées. Malgré ces difficultés, il est tout de même essentiel d'essayer de déterminer au mieux les risques possibles afin de pouvoir, dans un second temps, envisager des mesures permettant de protéger au mieux les droits fondamentaux des personnes concernées.

La représentation graphique sous forme de matrice des risques permet à l'unité responsable du traitement de différencier les risques non élevés en vert des risques élevés qui sont en jaune ou en rouge :

- les risques en vert dans la matrice peuvent être considérés comme acceptables, c'est-à-dire que les risques résiduels sont admissibles sans que des mesures ne doivent être prises.
- les risques en jaune ou en rouge dans la matrice doivent être considérés comme élevés, c'est-à-dire que pour chaque risque identifié des mesures s'imposent afin que ces risques élevés deviennent, dans la mesure du possible, des risques en vert.

En cas d'application d'HERMES (voir encadré au chapitre 3.4.1) : vu que les risques pour la sécurité de l'information sont déjà identifiés et évalués dans le cadre de l'analyse détaillée du concept SIPD, seuls les risques pour la protection des données doivent encore être identifiés et évalués, séparément ou dans le cadre du concept SIPD. Pour ce qui est des risques pour la sécurité de l'information, il faut en outre veiller à évaluer leur impact sur les droits fondamentaux des personnes concernées.

Exemple (exemple abstrait, à préciser dans le cas concret) :

Scénario	Risque	Probabilité d'occurrence	Impact sur les personnes concernées
Accès interne : plusieurs personnes participent au traitement de données personnelles	Accès non autorisé à des données personnelles	Interne : difficile à déterminer. Un comportement conforme à la loi peut-il être présumé ? Le personnel est-il déjà sensibilisé/formé aux risques ? Il convient de tenir compte du comportement passé	Interne/externe : des données personnelles parviennent entre les mains de personnes non autorisées ; l'impact varie en fonction du type de données et de l'intérêt qu'elles suscitent (p. ex. utilisation abusive de cartes de crédit, utilisation de données telles que l'adresse électronique)
Accès externe : sécurité lacunaire du système (piratage, etc.)		Externe : dépend de l'intérêt suscité par les données personnelles concernées	

3.5 Identification des mesures prévues pour protéger les droits fondamentaux de la personne concernée

Une fois le ou les risque(s) pour les droits fondamentaux de la personne concernée identifiés, un certain nombre de mesures peuvent être envisagées pour réduire ces risques et protéger ces droits fondamentaux. Contrairement aux précédents chapitres, la partie de l'AIPD relative à l'identification des mesures prévues pour protéger les droits fondamentaux de la personne concernée n'est pas prévue par l'instrument d'examen préalable des risques ; en effet, cet instrument ne tient pas compte des mesures qui permettraient de réduire les risques.

Lors de l'identification des mesures, il s'agit en particulier de réduire les risques pour les droits fondamentaux des personnes concernées. Les mesures envisagées doivent permettre d'assurer que le risque net (évalué en tenant compte desdites mesures) soit moins élevé que le risque brut (évalué indépendamment desdites mesures). L'AIPD vise également à attester de manière transparente les risques constatés et les mesures prévues pour y remédier.

La réduction du risque peut se faire soit en agissant sur la probabilité d'occurrence de l'événement déclencheur, soit en agissant sur la gravité de l'événement déclencheur, autrement dit l'impact du risque.

Les mesures peuvent être de nature technique (en pratique cela se traduira souvent par des mesures d'ordre informatique), organisationnelle (en particulier sur le plan du personnel ; répartition des rôles et responsabilités ; instructions, surveillance, etc.) et/ou juridique (via l'adoption de bases légales, de directives, règlements, contrats, etc.).

Un certain nombre de mesures, notamment d'ordre technique et/ou organisationnel, se trouvent dans la LPD et l'OPDo. On peut par exemple citer les normes de sécurité des données, le fait d'établir un règlement de traitement et de tenir un registre des activités de traitement, la limitation de la durée de conservation, la vérification de l'exactitude des données, etc.

Il s'agit de trouver la ou les mesure(s) les plus opportunes pour le risque envisagé. Cela peut nécessiter une certaine créativité. Les mesures peuvent porter directement sur le traitement des données personnelles (chiffrement, anonymisation, pseudonymisation, contrôle d'accès, traçabilité, etc.), sur le système de traitement (sécurité du matériel, des logiciels, journalisation, sauvegardes, etc.) ou encore sur la gouvernance en matière de protection des données personnelles (règlement de traitement, gestion des projets et du personnel ou encore des violations de la protection des données).

En pratique, il convient de trouver la ou les mesure(s) pertinente(s) pour réduire les risques qui se trouvent dans les zones jaune et rouge de la matrice. Pour chaque mesure identifiée, il conviendra encore de déterminer qui est responsable de la mettre en œuvre (service ou fonction), à partir de quand et pendant combien de temps cette mesure devra être mise en œuvre et, enfin, le coût (financier/en termes de personnel) de la mesure.

Ces différentes informations peuvent par exemple être présentées dans un tableau tel que celui-ci :

Risque	Mesure(s)	Service/Fonction	Calendrier	Coûts
Risque 1	Mesure 1	xy	De... à.../dès...	...

	Mesure 2	ef	De... à.../dès...	...
	Mesure 3	xy	De... à.../dès...	...
Risque 2	Mesure 2	ef	De... à.../dès...	...
Risque 3	Mesure 1	xy	De... à.../dès...	...
	Mesure 4	ab	De... à.../dès...	...

Les mesures à prendre au titre de la protection de base doivent être mentionnées dans l'AIPD lorsqu'elles contribuent à réduire le risque pour les droits fondamentaux d'une personne. Il n'est cependant pas nécessaire d'indiquer les coûts calculés pour leur mise en œuvre.

En cas d'application d'HERMES (voir encadré plus haut, 3.4.1) : vu que les mesures contre les risques pour la sécurité de l'information sont déjà définies dans le cadre de l'analyse détaillée des risques selon le concept SIPD, il ne reste plus qu'à prévoir des mesures contre les risques pour la protection des données, soit séparément, soit dans le concept SIPD. Pour ce qui est des risques pour la sécurité de l'information, il faut en outre veiller à évaluer leur impact sur les droits fondamentaux des personnes concernées.

Exemple (exemple abstrait, à préciser dans le cas concret) :

Scénario	Risque	Probabilité d'occurrence	Impact sur les personnes concernées	Mesure
Accès interne : plusieurs personnes participent au traitement de données personnelles	Accès non autorisé à des données personnelles	Interne : difficile à déterminer. Un comportement conforme à la loi peut-il être présumé ? Le personnel est-il déjà sensibilisé/formé aux risques ? Il convient de tenir compte du comportement passé	Interne/externe : des données personnelles parviennent entre les mains de personnes non autorisées ; l'impact varie en fonction du type de données et de l'intérêt qu'elles suscitent (p. ex. utilisation abusive de cartes de crédit, utilisation de données telles que l'adresse électronique)	Réglementer les autorisations d'accès, dresser des procès-verbaux des accès, former le personnel et établir des directives à son intention, vérifier le respect des directives
Accès externe : sécurité lacunaire du système (piratage, etc.)		Externe : dépend de l'intérêt suscité par les données personnelles concernées		Améliorer la sécurité du système, avertir les personnes concernées en cas de violation de la sécurité des données

3.6 Évaluation des effets des mesures prévues afin de déterminer s'il existe un risque résiduel élevé

Une fois les mesures déterminées, l'unité de l'administration fédérale responsable devra procéder à une nouvelle évaluation de chaque risque identifié dans les zones jaune et rouge de la matrice (voir chapitre 3.4) afin de déterminer si la ou les mesure(s) prévue(s) a (ont) permis d'appréhender et

de réduire le risque et de vérifier s'il reste encore un risque résiduel élevé (risque dans les zones jaune ou rouge de la matrice). Il est essentiel de pouvoir comprendre comment les différentes mesures réduisent la probabilité d'occurrence et/ou les impacts (par exemple à l'aide de commentaires).

Il s'agira, par exemple, d'évaluer les mesures techniques et organisationnelles prévues en matière de sécurité des données, afin de déterminer la probabilité et la gravité d'une violation de la sécurité des données, malgré lesdites mesures.

Notons que certains risques ne sont pas ou peu influençables. En effet, même en prenant différentes mesures, il est possible que le risque reste le même ou presque le même.

Exemple (exemple abstrait, à préciser dans le cas concret) :

Scénario	Risque	Probabilité d'occurrence	Impact sur la personne concernée	Mesure	Effets de la mesure (risque résiduel)
Accès interne : plusieurs personnes participent au traitement de données personnelles	Accès non autorisé à des données personnelles	Interne : difficile à déterminer. Un comportement conforme à la loi peut-il être présumé ? Le personnel est-il déjà sensibilisé/formé aux risques ? Il convient de tenir compte du comportement passé	Interne/externe : des données personnelles parviennent entre les mains de personnes non autorisées ; l'impact varie en fonction du type de données et de l'intérêt qu'elles suscitent (p. ex. utilisation abusive de cartes de crédit, utilisation de données telles que l'adresse électronique s)	Réglementer les autorisations d'accès, dresser des procès-verbaux des accès, former le personnel et établir des directives à son intention, vérifier le respect des directives	Les mesures techniques et organisationnelles peuvent largement réduire la probabilité d'occurrence, elles ne peuvent que limiter l'impact en cas de survenance d'un événement.
Accès externe : sécurité lacunaire du système (piratage, etc.)		Externe : dépend de l'intérêt suscité par les données personnelles concernées		Améliorer la sécurité du système, avertir les personnes concernées en cas de violation de la sécurité des données	L'amélioration de la sécurité du système peut largement réduire la probabilité d'occurrence, elle ne peut que limiter l'impact en cas de survenance d'un événement.

3.7 Consultation du PFPDT en cas de risque résiduel élevé

Comme il a déjà été mentionné dans le chapitre 2.3, lorsqu'il est constaté que, malgré les mesures prévues, le traitement envisagé présente encore un risque élevé pour les droits fondamentaux de la personne concernée, cela implique de consulter le PFPDT³⁴. Le responsable du traitement doit procéder à cette consultation avant le début du traitement des données et devra tenir compte

³⁴ Art. 23 LPD

des éventuelles mesures appropriées proposées par le PFPDT à l'issue de son examen afin de pouvoir traiter les données en question.

Dans le cadre de cette consultation au PFPDT, différents délais clés structurent le processus :

- Dans une première étape, le PFPDT vérifie que le dossier de l'AIPD est complet et informe l'unité administrative responsable de toute lacune éventuelle dès que possible. Deux à quatre semaines sont généralement nécessaires pour cette vérification. Si le dossier transmis par l'unité administrative responsable n'est pas complet, ce délai recommence à courir à chaque nouvelle version transmise.
- Dans une seconde étape, si le PFPDT a des objections à l'égard du traitement prévu, il propose des mesures appropriées à l'unité administrative responsable dans le délai légal de deux mois³⁵. Ce délai ne commence à courir qu'à partir du moment où l'unité administrative responsable lui a transmis un dossier complet. Il peut être prolongé d'un mois s'il s'agit d'un traitement de données complexes.

Coordination avec la procédure normative (ch. 4 Directives AIPD) : les résultats de l'AIPD ainsi que, en cas de risque résiduel élevé au sens de l'art. 23 LPD, la **prise de position PFPDT** sont joints au dossier de la consultation des offices. Si la nécessité de procéder à une AIPD ou de l'adapter apparaît après la consultation des offices, les résultats de l'AIPD et, le cas échéant, la prise de position du PFPDT sont joints au dossier de la consultation des offices suivante ou de la procédure de co-rapport.

L'unité administrative responsable (Département ou ChF) informe des résultats de l'AIPD et, le cas échéant, de la **prise de position du PFPDT**, notamment dans la proposition au Conseil fédéral, le rapport explicatif, le message et la brochure des Explications du Conseil fédéral.

3.8 Synthèse et résultats de l'AIPD

La synthèse doit mentionner les principaux résultats de l'AIPD, à savoir les risques (qui se situent dans la zone jaune et rouge de la matrice), les mesures prévues pour réduire ces risques et les éventuels risques résiduels élevés.

Coordination avec la procédure normative (ch. 4 Directives AIPD) : lorsque la réalisation de l'AIPD intervient dans le cadre d'une procédure normative, les résultats de l'AIPD doivent être joints au dossier de la consultation des offices. Par ailleurs, l'unité administrative responsable (Département ou ChF) informe des résultats de l'AIPD notamment dans la proposition au Conseil fédéral, le rapport explicatif, le message et dans la brochure des Explications du Conseil fédéral.

³⁵ Art. 23, al. 2, LPD

Annexe : check-list du contenu de l'AIPD

Première partie : indications générales

La partie de l'AIPD relative aux indications générales doit contenir les éléments suivants :

- Unité de l'administration fédérale responsable.
- Bases légales existantes ou prévues du traitement envisagé de données personnelles.
- Conseiller ou conseillère à la protection des données.
- Indication précisant si le traitement envisagé s'inscrit dans le cadre d'une procédure normative.
- Indication précisant si le traitement envisagé s'inscrit dans le cadre d'un projet HERMES.

Deuxième partie : description du traitement envisagé de données personnelles

La partie de l'AIPD qui se rapporte au traitement des données personnelles doit permettre de connaître la nature, l'étendue et les finalités du traitement ainsi que les circonstances dans lesquelles il se déroule.

- Identification des personnes participant au traitement (p. ex. plusieurs responsables, sous-traitants).
- Identification et description des catégories de données personnelles (p. ex. données personnelles/données sensibles, forme des données).
- Identification et description des catégories de personnes concernées (p. ex. personnes vulnérables).
- Identification et description du traitement envisagé (p. ex. collecte, enregistrement, conservation, utilisation, modification, communication, archivage, effacement ou destruction de données).
- Identification et description de la nature de traitement (p. ex. collecte de données personnelles à l'insu de la personne concernée ; interconnexion ou appariement avec d'autres bases de données ; communication de données personnelles à des tiers ; profilage ou profilage à risque élevé ; décision individuelle automatisée ; surveillance).
- Identification et description des technologies utilisées (p. ex. logiciels, réseaux, recours à l'intelligence artificielle).
- Identification et description de l'étendue du traitement (p. ex. volume des données personnelles traitées, nombre de personnes concernées, envergure temporelle et géographique).
- Identification et description des finalités du traitement.

Troisième partie : évaluation du risque pour les droits fondamentaux de la personne concernée

La partie de l'AIPD concernant l'évaluation des risques doit inclure les aspects suivants :

- Identification et description des risques pour la sécurité de l'information et pour la protection des données.
- Évaluation de la probabilité d'occurrence des risques identifiés.
- Évaluation et description de l'impact ou de la gravité des risques identifiés pour les droits fondamentaux des personnes concernées.

Pour chaque risque identifié, il convient de déterminer :

- Si le risque est admissible (risque dans la zone verte de la matrice).
- Si le risque n'est pas admissible (risque dans la zone jaune ou rouge de la matrice) → identifier les mesures correctives possibles ; cf. point suivant).

Quatrième partie : identification des mesures prévues pour protéger les droits fondamentaux de la personne concernée

La partie de l'AIPD relative aux mesures prévues pour protéger les droits fondamentaux de la personne concernée doit permettre de déterminer quelle mesure permet de passer du risque brut ou risque net.

Pour chaque risque identifié dans les zones jaune et rouge de la matrice (cf. chapitre 3.4, ci-dessus) :

- Identification de la ou des mesure(s) pertinente(s) pour réduire le risque.

Pour chaque mesure identifiée, il convient de mentionner :

- Le service ou la personne (fonction) responsable de la mise en œuvre de la mesure.
- Le calendrier de la mise en œuvre de la mesure.
- Le coût (financier/en termes de personnel) de la mise en œuvre de la mesure.

Identification et évaluation du respect :

- Des principes régissant le droit de la protection des données.
- Des obligations du responsable du traitement.

Cinquième partie : évaluation des effets des mesures prévues afin de déterminer s'il reste un risque résiduel élevé

Cette partie a pour but de déterminer si, malgré les mesures prévues pour protéger les droits fondamentaux de la personne concernée, il reste un risque résiduel élevé.

Pour chaque mesure prévue :

- Évaluation et description des effets desdites mesures.

Pour chaque risque identifié dans les zones jaune et rouge de la matrice, il convient de déterminer :

- S'il y a un risque résiduel élevé.
- Le cas échéant consulter le PFPDT.

Sixième partie : synthèse et résultats de l'AIPD

Cette partie a pour but de présenter une synthèse des résultats.

- Description des risques identifiés (risques de la zone jaune et rouge de la matrice).
- Description des mesures prévues pour réduire ces risques.
- Description des éventuels risques résiduels élevés.