Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé federal à la protection des données et à la transparence
PFPDT

Aide-mémoire

concernant l'analyse d'impact relative à la protection des données personnelles (AIPD) au sens des art. 22 et 23 LPD

État : août 2023

Bibliographie

- Message du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF **2017** 6565 (message)

- Lobsiger Adrian, *Hohes Risiko – kein Killerargument gegen Vorhaben der digitalen Transformation*, Revue suisse de jurisprudence RSJ 6/119

Table des matières

1 But et champ d'application de l'aide-mémoire sur l'AIPD 4
2 Objet et finalités de l'AIPD 4
3 Objets de la protection de l'AIPD 4
4 Qualification du « risque élevé » 5
4.1 Définition générale du risque élevé (art. 22, al. 2, 1re partie, LPD) 6
4.2 Critères absolus visés à l'art. 22, al. 2, let. a et b, LPD 6
5 Examen préalable des risques selon l'art. 22, al. 1 et 2, LPD 6
6 Obligation de procéder à une AIPD (art. 22, al. 3, LPD) 7
6.1 Contenu et étape de l'AIPD 7
6.2 Description du traitement envisagé 7
6.3 Description et évaluation des risques initiaux potentiellement élevés 7
6.4 Mesures prévues pour réduire les risques initiaux potentiellement élevés 8
6.5 Risques résiduels 8
7 Procédure à suivre après la réalisation de l'AIPD 8
7.1 Absence de risque résiduel élevé 8
7.2 Risque résiduel élevé 9
8 Procédure applicable en cas de traitement comportant un risque élevé et donnant lieu à une violation de la sécurité des données 9
9 Prise de position du PFPDT sur l'AIPD 9
10 Mesures pouvant être ordonnées par le PFPDT en vertu du droit de la surveillance 10
Annexe 1 11
Annexe 2 13

1 But et champ d'application de l'aide-mémoire sur l'AIPD

L'aide-mémoire du PFPDT s'adresse en premier lieu aux responsables privés du traitement des données, bien qu'il puisse également être utilisé comme aide à l'interprétation par les organes fédéraux. Pour les unités administratives de l'administration fédérale centrale, l'Office fédéral de la justice a publié sur son site Internet les directives du Conseil fédéral concernant l'évaluation préliminaire des risques et l'analyse d'impact relative à la protection des données lors de traitements de données effectués par l'administration fédérale (directives DSFA), un instrument pour l'évaluation préliminaire des risques ainsi qu'un guide pour la DSFA. Les responsables privés peuvent également s'inspirer de ces instruments.

2 Objet et finalités de l'AIPD

À compter du 1er septembre 2023, tout traitement de données entraînant à un risque élevé devra, en vertu des art. 22 et 23 de la loi sur la protection des données révisée (LPD), faire l'objet d'une **analyse d'impact relative à la protection des données personnelles (AIPD)**. Selon l'art. 22, al. 1, LPD, le responsable du traitement devra procéder à cette analyse lorsque le traitement envisagé sera susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

En tant qu'instrument de travail du droit moderne de la protection des données, l'AIPD vise à préserver les droits des personnes concernées dans la réalité sociale de l'ère du numérique. Comme le souligne les art. 22, al. 1, et 23, al. 1, LPD, l'AIPD concerne les **traitements de données personnelles envisagés**. Le législateur a pensé en premier lieu aux grands projets de transformation numérique, mais il ne doit pas nécessairement s'agir de **nouveaux traitements de données personnelles**. Le développement et l'extension d'un **traitement préexistant** peuvent aussi faire l'objet d'une AIPD.

L'AIPD vise à **identifier à un stade préalable les risques élevés associés à un projet**, qui se caractérisent par leur **probabilité de survenance** et, du fait du qualificatif « élevés », par la **gravité** de leurs conséquences.

Elle ne se résume pas à la **prévisibilité et à l'évaluation des risques « élevés »**. Son intérêt pratique réside aussi et surtout dans le fait qu'elle permet, d'une part, de **documenter** de façon claire l'origine et l'analyse des risques systémiques et relevant des techniques de sécurité et, d'autre part, de réduire les risques à un niveau acceptable du point de vue du droit de la protection des données par des **mesures** appropriées.

3 Objets de la protection de l'AIPD

Les art. 22, al. 1, et 23, al. 1, LPD précisent que les « risques élevés » visés par la loi doivent menacer la personnalité ou les droits fondamentaux de la personne concernée. Le législateur a ainsi érigé la protection de la personnalité comme objet de protection fondamental de la protection des données, dont découlent la **sphère privée et l'autodétermination informationnelle** en tant qu'**objets primaires de la protection** de l'AIPD, qui englobent aussi bien l'autonomie de l'individu que sa dignité et son identité. S'agissant de l'autodétermination informationnelle, le message précise qu'on peut admettre l'existence d'un risque élevé lorsqu'il apparaît que les propriétés du traitement envisagé ont – ou pourraient avoir – pour effet de restreindre dans une large mesure la liberté de la personne de disposer de ses données.

Lorsque des données personnelles font l'objet d'un traitement illicite, il peut en résulter des **violations subséquentes** physiques et financières qui portent atteinte à d'autres biens juridiques ou droits fondamentaux que les objets primaires de la protection des données, tels que le droit à la vie, à l'intégrité physique ou à la propriété. Ces violations peuvent toucher les personnes concernées par le traitement mais aussi, dans la suite du processus causal, les responsables du traitement.

Exemple fictif pour mieux comprendre : une association humanitaire mène un projet numérique à visée statistique qui consiste à traiter des données de migrants faisant l'objet de poursuites politiques. Une première appréciation des risques lui livre les résultats suivants :

- *le traitement envisagé comporte le risque potentiellement élevé pour la sphère privée et pour l'autodétermination informationnelle des migrants concernés de rendre leurs coordonnées personnelles accessibles, y compris à des personnes mal intentionnées (risque primaire pour les personnes concernées) ;*
- *la réalisation de ce risque primaire peut entraîner pour les personnes concernées un risque d'être poursuivies illégalement pouvant aller jusqu'à l'assassinat (risque subséquent pour les personnes concernées) ;*
- *la réalisation de ce risque subséquent pour les personnes concernées peut à son tour entraîner le risque, pour le responsable du traitement, de voir sa réputation entachée et de devoir verser une compensation financière aux personnes concernées (risque subséquent pour le responsable du traitement).*

S'agissant de la distinction faite dans notre exemple entre **risques primaires et risques subséquents**, le PFPDT recommande aux responsables du traitement, lorsqu'ils évaluent le « risque élevé », d'exposer :

- dans un premier temps, les risques qui pèsent sur les objets primaires de la protection que sont la sphère privée et l'autodétermination informationnelle des personnes concernées, et
- dans un second temps, les risques subséquents qui pèsent sur les autres biens juridiques et droits fondamentaux.

Si les risques subséquents **concernent les responsables du traitement eux-mêmes**, ils ne relèvent pas du droit de la surveillance puisque la LPD vise, conformément à ses art. 1 et 22, al. 1, à protéger non pas les responsables du traitement mais la personnalité et les droits fondamentaux des personnes physiques dont les données personnelles font l'objet d'un traitement. La situation est différente lorsque la réalisation de ces risques subséquents risque en outre d'aggraver les dommages subis par les personnes concernées. Par exemple, lorsqu'un responsable du traitement est empêché, par son insolvabilité, de consacrer les moyens nécessaires à la maintenance de l'infrastructure afin d'assurer la protection technique des données personnelles qu'il traite.

4 Qualification du « risque élevé »

En dehors des dispositions des art. 22 et 23 relatives à l'AIPD, la LPD évoque les traitements de données personnelles présentant un « risque élevé » à propos :

- du « profilage à risque élevé » visé à l'art. 5, let. g ;
- de l'obligation de désigner un représentant en Suisse (art. 14, al. 1, let. d) ;
- de l'annonce des violations de la sécurité des données visée à l'art. 24, et
- du traitement de données personnelles dans le but d'évaluer la solvabilité (art. 31, al. 2, let. c, ch. 1).

Parce qu'elle est sujette à interprétation, la notion juridique indéterminée de « risque élevé » utilisée dans la loi ouvre aux responsables du traitement et à la surveillance de la protection des données assurée par l'autorité fédérale de surveillance un vaste champ d'application. Le législateur s'étant aussi abstenu de la préciser dans l'ordonnance, sa définition se précisera au fil de la pratique et de la jurisprudence.

4.1 Définition générale du risque élevé (art. 22, al. 2, 1re partie, LPD)

Le législateur fournit des aides à l'interprétation à l'art. 22, al. 2, LPD. Selon cette disposition, l'existence d'un « risque élevé » dépend :

- de la nature ;
- de l'étendue ;
- des circonstances, et
- de la finalité

du traitement, ce qui laisse une vaste marge d'appréciation dans l'application du droit. Par **nature** d'un traitement susceptible d'entraîner un risque élevé, on entend par exemple le profilage au sens de l'art. 5, let. g, LPD qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique, ou d'autres formes de traitement automatique telles que la décision individuelle automatisée visée à l'art. 21 LPD. Au rang des **circonstances** d'un traitement figurent par exemple les rapports de subordination entre le responsable du traitement et les personnes concernées.

4.2 Critères absolus visés à l'art. 22, al. 2, let. a et b, LPD

L'art. 22, al. 2, let. a et b, LPD indique, sans prétendre à l'exhaustivité, deux critères absolus de l'existence d'un « risque élevé » aux yeux de la loi :

- le traitement de données sensibles à grande échelle, et
- la surveillance systématique de grandes parties du domaine public.

5 Examen préalable des risques selon l'art. 22, al. 1 et 2, LPD

Si un traitement envisagé est susceptible d'entraîner des risques potentiellement élevés, le responsable du traitement doit effectuer un examen préalable (sommaire) des risques liés au projet. Cet examen préalable doit respecter les critères énoncés au ch. 3, qui s'appliquent à l'AIPD elle-même.

L'examen préalable doit être effectué le plus tôt possible, c'est-à-dire dès le stade de la **planification du projet**, même si les détails du traitement n'ont pas encore été arrêtés. Il peut par conséquent être judicieux de prévoir plusieurs variantes.

Il est recommandé d'établir un registre des activités de traitement et une description systématique des procédures et des finalités du traitement envisagé, y compris les modèles d'affaires et les autres intentions et centres d'intérêts des responsables du projet. S'il est prévu d'étendre et de développer des **applications préexistantes**, il faut **comparer** le traitement existant et le traitement prévu.

Le responsable du traitement doit **documenter** le résultat de l'examen préalable et ses conclusions. Si le résultat manque de clarté, il est recommandé d'effectuer une AIPD.

Le déroulement et les autres critères de l'examen préalable sont exposés sous forme de schéma à l'annexe 1.

Des outils élaborés par l'Office fédéral de la justice pour l'examen préalable des risques liés au traitement de données personnelles par les organes fédéraux, dont les responsables privés pourront aussi s'inspirer, seront présentés ultérieurement.

6 Obligation de procéder à une AIPD (art. 22, al. 3, LPD)

Si l'examen préalable révèle qu'un traitement envisagé est susceptible d'entraîner un risque potentiellement élevé, une AIPD s'impose. Conformément aux prescriptions de l'art. 7 LPD (protection des données dès la conception et par défaut), elle doit être réalisée le plus tôt possible, tout comme l'examen préalable. Étant donné qu'il reste alors, la plupart du temps, de nombreux détails à régler, il peut être judicieux de prévoir, comme pour l'examen préalable, plusieurs variantes qui seront adaptées et triées au fur et à mesure.

Si le PFPDT, apprenant qu'un traitement est envisagé, estime que le responsable doit effectuer un examen préalable puis une AIPD, il peut, en cas de refus du responsable, prendre des mesures de surveillance pour empêcher la réalisation du traitement (cf. ch. 8).

6.1 Contenu et étape de l'AIPD

L'art. 22, al. 3, précise qu'une AIPD doit contenir :

- une **description du traitement envisagé** ;
- une **évaluation des risques** pour la personnalité ou les droits fondamentaux de la personne concernée, et
- les **mesures** prévues pour protéger la personnalité et les droits fondamentaux de la personne concernée,

c'est-à-dire les objets primaires et les objets secondaires de la protection (cf. ch. 2). Nous proposons un exemple de structure de l'AIPD à l'annexe 2.

6.2 Description du traitement envisagé

Il faut d'abord mettre à jour les descriptions et les comparaisons établies lors de l'examen préalable (cf. ch. 4) puis les approfondir dans le cadre de l'AIPD. Pour plus de précisions, nous renvoyons à l'annexe 2.

6.3 Description et évaluation des risques initiaux potentiellement élevés

Nous avons donné aux ch. 1 à 3 la description des risques primaires et secondaires potentiellement élevés susceptibles de se réaliser lors d'un traitement et leur évaluation en fonction de leur probabilité de survenance et de leur gravité.

Lorsque des données personnelles sont transférées à l'étranger, le transfert lui-même doit être examiné dans le cadre de l'AIPD. C'est surtout quand le pays destinataire n'offre pas un niveau de protection des données approprié que peuvent se produire des risques potentiellement élevés sur lesquels le responsable du traitement **n'a pas les moyens** matériels ni juridiques **d'agir**, ce qui fait que l'AIPD conclura à un risque résiduel élevé. Tel est par exemple le cas lorsque les autorités étrangères risquent, en vertu des pouvoirs que leur confère leur droit national, de porter atteinte à la personnalité ou aux droits fondamentaux des personnes concernées et que le responsable du traitement n'a aucun moyen d'y remédier, ni sur une base autonome privée en agissant sur la forme du contrat ni par la voie d'un recours, ce qui l'empêche par conséquent de fournir une évaluation fiable de la probabilité de survenance et de la gravité du risque, même compte tenu des mesures prévues dans l'AIPD.

Par mesure de transparence, l'AIPD doit, le cas échéant, préciser qu'il est impossible de fournir une appréciation fiable de ces risques. Cette exigence peut notamment se révéler

pertinente, selon l'efficacité des mesures techniques, juridiques et organisationnelles prises, lorsqu'il est question d'externaliser des données personnelles dans des centres de calcul dont l'exploitant appartient à un groupe qui a son siège dans un État dont le droit n'offre pas un niveau de protection des données comparable à celui de la Suisse.

6.4 Mesures prévues pour réduire les risques initiaux potentiellement élevés

Les mesures de protection de la personnalité et des droits fondamentaux des personnes concernées visées à l'art. 22, al. 3, LPD ont pour but de réduire à un niveau approprié les risques initiaux élevés liés à la réalisation du traitement envisagé afin qu'ils puissent être qualifiés de « réduits » ou de « moins élevés ». Les mesures envisagées peuvent comprendre une pesée des intérêts entre ceux de la personne concernée et ceux du responsable du traitement. Celle-ci doit être mentionnée et dûment motivée dans l'AIPD.

Pour plus de détails sur la description des mesures de protection envisagées, nous renvoyons à l'annexe 2.

6.5 Risques résiduels

L'art. 23, al. 1, LPD prévoit expressément qu'un traitement de données potentiellement dangereux peut, selon les circonstances, continuer de présenter un « risque élevé », malgré les mesures de protection considérées comme appropriées et raisonnables par le responsable du traitement. La LPD n'exige donc pas du responsable du traitement ni du PFPDT qu'ils réduisent les risques potentiellement élevés à un niveau clairement défini, et encore moins qu'ils les éliminent.

Le responsable du traitement doit toutefois exposer de façon claire, nette et précise les risques finaux résultant de l'AIPD et veiller à ce que ceux qui restent « élevés » soient compatibles avec les prescriptions de la législation sur la protection des données. À cette condition seulement, le traitement en question sera considéré comme supportable pour les personnes concernées et donc acceptable, tant par l'étendue que par l'intensité prévues.

Pour plus de détails sur la description et l'appréciation des risques résiduels, nous renvoyons à l'annexe 2.

7 Procédure à suivre après la réalisation de l'AIPD

Le responsable du traitement devra suivre des procédures différentes selon l'évaluation du risque résiduel indiqué.

7.1 Absence de risque résiduel élevé

a) Même si le risque résiduel est jugé inférieur à « élevé », le responsable du traitement devra vérifier si le traitement envisagé respecte bien toutes les prescriptions de la législation sur la protection des données. Il ne pourra procéder au traitement que si cette condition fondamentale est remplie.

b) Le responsable du traitement n'est pas tenu de soumettre l'AIPD au PFPDT.

S'il le fait à titre volontaire, le PFPDT ne sera pas obligé d'en tenir compte ni de donner son avis mais il pourra, à titre exceptionnel, se prononcer sur des risques résiduels inférieurs à « élevés » dans le cadre de son activité de conseil, pour laquelle il doit percevoir des émoluments (cf. art. 59, al. 1, let. e, LPD).

7.2 Risque résiduel élevé

a) Lorsque le traitement est maintenu malgré des risques résiduels élevés, ce qui est en principe admissible, ces risques doivent être exposés clairement aux personnes concernées, même s'ils sont impossibles à influencer et à évaluer de façon fiable. Les responsables du traitement privés doivent tenir compte du fait que le consentement des risques résiduels élevés n'est juridiquement valable que si elle a été formulée en connaissance de cause, c'est-à.dire en connaissance des risques résiduels mentionnés dans l'AIPD.

b) Conformément à l'art. 23, al. 1, LPD, le responsable du traitement doit soumettre l'AIPD au PFPDT pour prise de position. Cette prise de position est soumise à émoluments (art. 59, let. c, LPD).

   En vertu de l'al. 4, le responsable du traitement privé peut renoncer à consulter le PFPDT s'il a consulté son propre conseiller à la protection des données. Dans ce cas, il peut soumettre l'AIPD au PFPDT à titre volontaire. Si le PFPDT y donne suite, sa prise de position sera soumise à émoluments conformément à l'art. 59, al. 1, let. c, LPD.

8 Procédure applicable en cas de traitement comportant un risque élevé et donnant lieu à une violation de la sécurité des données

S'il existe des indices suffisants qu'il a pu se produire des circonstances dans lesquelles un traitement existant ou développé est susceptible d'entraîner des risques supplémentaires considérés globalement comme élevés, le responsable du traitement doit, selon la situation, effectuer une AIPD ou, s'il en a déjà effectué une, actualiser celle-ci. Cette action peut avoir pour déclencheur un rapport d'experts, la plainte d'une personne concernée, un article de presse, une cyberattaque repoussée ou commise sans intention de nuire, ou toute autre violation de la sécurité des données. Si l'AIPD nouvelle ou actualisée révèle un risque résiduel élevé, le responsable du traitement doit la soumettre au PFPDT pour prise de position, en comparant la manière dont le traitement a été appliqué et la manière dont il devrait être appliqué.

Si le traitement de données personnelles a causé une violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personne concernée au sens de l'art. 24 LPD et dont l'annonce au PFPDT est obligatoire, le responsable du traitement doit prendre à temps les mesures nécessaires pour rétablir une situation conforme au droit, cas échéant informer les personnes concernées des atteintes à leur personnalité ou à leurs droits fondamentaux qui se sont produites ou qui menacent de se produire. S'il apparaît que les risques resteront élevés dans la suite du traitement, le PFPDT peut demander au responsable du traitement d'effectuer une AIPD.

9 Prise de position du PFPDT sur l'AIPD

Le PFPDT vérifie si l'AIPD qui lui est soumise expose de façon claire, nette et précise les risques résiduels élevés identifiés. Il vérifie aussi si le traitement envisagé, compte tenu des risques exposés, est compatible avec les prescriptions de la législation sur la protection des données et s'il paraît supportable pour les personnes concernées et donc acceptable, tant par l'étendue que par l'intensité prévues.

Le PFPDT communique au responsable du traitement ses objections dans le délai de 2 mois prévu à l'art. 23, al. 2, LPD. Sa prise de position est soumise à émoluments (art. 59 LPD). Il peut porter sur le traitement prévu ou sur la structure de l'AIPD, par exemple si le responsable du traitement n'a pas évalué ni exposé correctement les risques imminents.

L’avis du PFPDT a valeur de recommandation et ne constitue en rien une approbation ni une autorisation du traitement prévu.

Si le PFPDT a des objections concernant le traitement envisagé, il propose au responsable du traitement des mesures appropriées, pour autant qu'elles permettent de réduire les risques constatés (art. 23, al. 3, LPD).

10 Mesures de surveillance du PFPDT

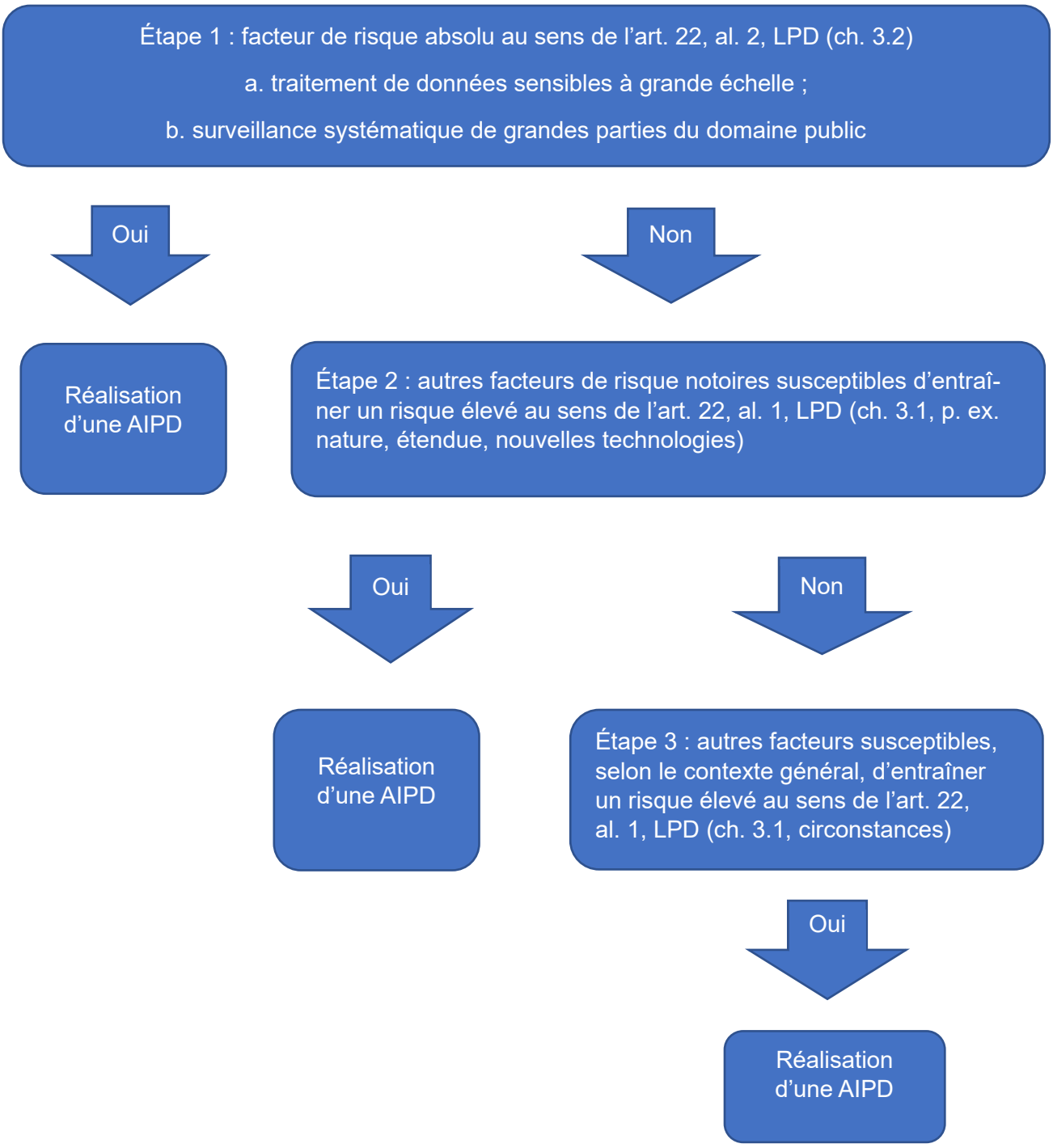
Si un responsable du traitement refuse de se plier à des objections et à des propositions importantes du PFPDT, celui-ci peut ouvrir une enquête et ordonner formellement les modifications proposées en temps utile, lesquelles peuvent aller jusqu’à l’interdiction du traitement. Toutefois, le PFPDT respecte la marge d’appréciation qui revient aux responsables du traitement, spécialistes de leur domaine, dans l’évaluation des risques de traitement.

L’intervention formelle du PFPDT est indiquée notamment lorsqu’un risque ne peut raisonnablement être admis en raison de la probabilité de sa survenance et de la gravité des atteintes à la personnalité qu’il représente, ce qui rend le traitement envisagé illicite du point de vue du droit de la protection des données. Tel est par exemple le cas si la réalisation d’un traitement à risque résiduel élevé est susceptible de violer les principes du droit de la protection des données visés à l’art. 6 LPD comme le principe de la proportionnalité, ou les exigences en matière de sécurité des données visées à l’art. 8 LPD. Quant à la question de savoir si et dans quelle mesure le responsable du traitement peut faire supporter aux personnes concernées des risques résiduels élevés qui ne peuvent pas être évalués de manière fiable selon l’AIPD, ne peuvent pas être résolus à partir des dispositions relatives à l’AIPD mais au moyen de la législation sur la protection des données dans son ensemble.

Annexe 1

Schéma de la procédure d'examen préalable visant à déterminer la pertinence de procéder à une AIPD

L'examen préalable visé à l'art. 22, al. 1, LPD peut suivre le schéma ci-dessous. L'instrument d'évaluation préliminaire des risques de l'Office fédéral de la justice est obligatoire pour les unités de l'administration fédérale centrale.



Commentaire du schéma

Les étapes ci-après permettent de déterminer si une AIPD est nécessaire.

Étape 1 :

La présence d'au moins un des facteurs de risque absolus rend nécessaire une AIPD.

À défaut, passer à l'étape 2.

Étape 2 :

Vérifier la présence de facteurs de risque notoires (un ou plusieurs, cf. aussi la liste non exhaustive ci-après).

- Y a-t-il un profilage à risque élevé ?
- Y a-t-il une décision individuelle automatisée ?
- Des nouvelles technologies (intelligence artificielle comprise) sont-elles employées ?
- Les données personnelles sont-elles recueillies secrètement (à l'insu de la personne concernée) ?
- Le traitement porte-t-il sur un volume important de données ou sur un nombre important de personnes ?
- Le traitement est-il important du point de vue de la durée ou de la couverture géographique ?
- Y a-t-il une interconnexion ou une comparaison de différentes bases de données ?
- Les données personnelles sont-elles communiquées à des tiers ?
- Le traitement de données personnelles implique-t-il la surveillance des personnes concernées ?
- Les personnes concernées sont-elles empêchées d'exercer un de leurs droits, d'utiliser un service ou d'exécuter un contrat ?

Si des facteurs de risque notoires sont avérés, il convient de procéder à une AIPD en cas de doute.

À défaut, passer à l'étape 3.

Étape 3 :

Vérifier si, compte tenu de toutes les circonstances, le traitement est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées (ch. 3.1, p. ex. : les rapports de subordination).

Si oui, il convient de procéder à une AIPD.

Si non, il est possible de s'en abstenir.

Annexe 2

Structure possible

Pour élaborer une AIPD, on peut s'inspirer de la liste ci-dessous, qui est fournie à titre purement indicatif. Les unités de l'administration fédérale centrale sont soumises au guide de l'AIPD qui explique la procédure et le contenu de l'analyse d'impact relative à la protection des données personnelles par l'administration fédérale.

1. Responsable

- Responsable
- Conseiller à la protection des données
- Autres services internes impliqués
- Sous-traitant
- Responsabilité conjointe

2. Contexte du traitement

- Description de l'état actuel
- Description de l'état souhaité
- En cas d'extension d'applications préexistantes : comparaison entre l'état actuel et l'état souhaité et renvoi aux AIPD préexistantes

3. Traitement des données

- Base légale (public) / motif justificatif (privé)
- Finalité du traitement
- Personnes concernées
  - Type (employés, clients, patients, etc.)
  - Implication (consentement / refus ; traitement automatisé ; transparence)
- Nature des données :
  - Texte / images / son, etc.
- Catégories de données
  - Données personnelles / données sensibles, etc.
- Étendue du traitement / quantité de données
  - Nombre des personnes concernées
  - Volume de données par personne concernée
- Qualité des données
  - Sources / collecte
- Communication de données
- Étendue géographique
- Durée / intensité du traitement
- Délais d'effacement

- Mise en œuvre technique
  - Technologies employées
  - Processus de traitement
  - Cryptage
  - Systèmes informatiques et interfaces
  - Droits d'accès
- Respect des principes de protection des données
  - Licéité
  - Bonne foi
  - Finalité
  - Proportionnalité
  - Transparence
  - Exactitude des données
  - Sécurité des données / risques techniques : éventuellement, concept SIPD, etc.
- Mise en œuvre de la protection des données dès la conception et par défaut
- Sous-traitant

4. Risques potentiellement élevés avant les mesures (risques initiaux)

- Nature des risques
  - Risques systémiques
  - Risques juridiques
  - Risques relevant des techniques de sécurité
  - S'agit-il de risques primaires pour la sphère privée et l'autodétermination informationnelle des personnes concernées ?
  - S'agit-il de risques secondaires pour d'autres biens juridiques ou droits fondamentaux des personnes concernées ?

- Analyse et évaluation des risques initiaux potentiellement élevés
  - Personnes concernées (responsables du traitement ou personnes dont les données font l'objet du traitement)
  - Étendue
  - Probabilité de survenance

5. Mesures visant à réduire les risques initiaux potentiellement élevés

- Mesures juridiques
  - Contrats, clauses contractuelles types, etc.
- Mesures organisationnelles
  - Sélection, instruction et surveillance du personnel
  - Sensibilisation, formation
- Mesures techniques conformément à l'art. 3 OPDo, p. ex. contrôle utilisateur

6. Risques résiduels ou finaux (subsistant après les mesures prises)

- Conséquences des mesures prises sur les risques initiaux potentiellement élevés
- Les mesures du responsable du traitement peuvent influer sur les risques
- Les mesures du responsable du traitement ne peuvent influer sur les risques (accès d'autorités étrangères, p. ex.)
- Proportionnalité des mesures / pesée des intérêts

7. Résultat

- Risque résiduel élevé
- Le risque final résiduel est-il ou non acceptable du point du vue du droit de la protection des données ?
- Risque résiduel réduit

8. Consultation du PFPDT

- Risque résiduel élevé malgré les mesures prises
- Exception : consultation du conseiller interne à la protection des données