Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

Office fédéral des assurances sociales OFAS

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

1. Quand procède-t-on à une AIPD ?

Une AIPD doit être réalisée lorsque le traitement de données décrit représente ou est susceptible de représenter un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (traitement de données sensibles ou surveillance systématique de grandes parties du domaine public ; cf. art. 22, al. 1 à 3, LPD). Le traitement de données sensibles à une échelle particulièrement vaste et l'usage de nouvelles technologies constituent à cet égard des éléments décisifs.

L'AIPD contient au minimum une description du traitement de données 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.

2. Projet / traitement des données

Il s'agit d'abord de décrire le traitement de données envisagé (art. 22, al. 3, LPD). Il faut également indiquer les bases juridiques existantes ou prévues sur lesquelles le traitement se fonde. Cela implique non seulement d'analyser les bases juridiques existantes, mais également celles qui devraient être créées ou adaptées. Le cas échéant, les bases juridiques existantes sont comparées aux bases juridiques prévues (comparaison entre ce qui est et ce qui devrait être).

3. Description du traitement de données envisagés

Ce chapitre aborde la manière, l'ampleur et le but du traitement des données personnelles ainsi que les circonstances de ce traitement (art. 22, al. 2, LPD). Par but, on entend l'objectif de la collecte et du traitement des données personnelles. La manière de traiter les données correspond aux types de traitement envisagés : collecte, enregistrement, conservation, utilisation, modification, communication, archivage, suppression et élimination des données.

Concernant la catégorie de données, il faut notamment indiquer si et dans quelle mesure les données traitées sont personnelles ou sensibles. Dans ce cadre, il faut également indiquer sous quelle forme les données sont disponibles (par ex. support écrit, audio ou vidéo). Il faut également décrire les catégories des personnes concernées (par ex. employés, assurés).

Les indications concernant l'ampleur du traitement permettent de juger si une grande quantité de données doit être traitée, si un grand nombre de personnes sont concernées et s'il s'agit d'un traitement d'une grande étendue temporelle ou géographique. Concernant l'étendue temporelle, il faut notamment indiquer sur quelle durée les données personnelles seront traitées et conservées.

4. Analyse des risques et mesures prévues

Identification et évaluation des risques pour les droits fondamentaux des personnes concernées

Par risque, on entend des effets non souhaités, potentiellement négatifs, qui ont ou pourraient avoir un impact sur les droits fondamentaux de la personne concernée.

Exemples (non exhaustifs) de risques : perte de données, données erronées, collecte excessive de données, consultation par des personnes non autorisées, mise en relation non autorisée de données ou profilage, conservation excessivement longue des données, transmission de données dans des États tiers, forte limitation de la liberté de la personne concernée de disposer de ses données, traitement d'une grande quantité de données, accès aux données accordé à un grand nombre de personnes.

Il s'agit d'abord d'identifier les risques du traitement de données personnelles envisagé.

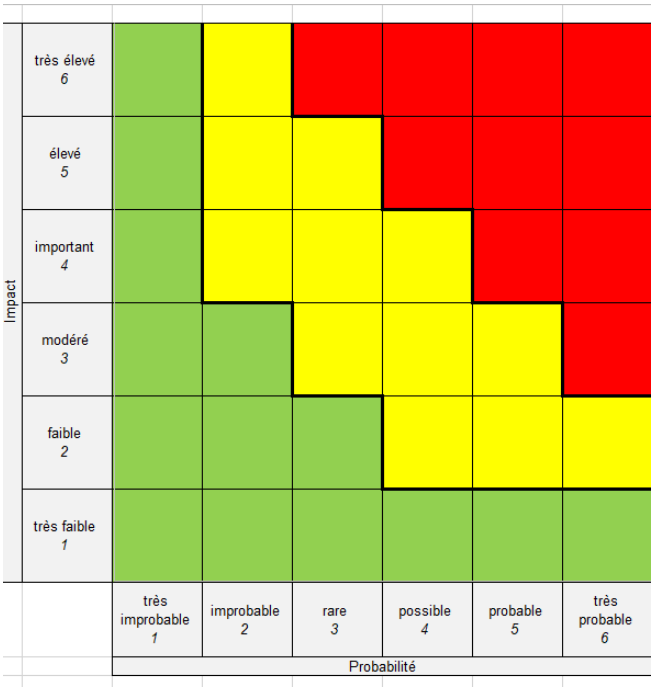
Différents types de risques existent. Les risques relatifs à la sécurité de l'information sont directement liés à la sécurité des données. Exemples : atteinte à l'intégrité des données personnelles (par ex. par manipulation ou erreur dans le système), violation de la confidentialité (par ex. en raison de failles dans le système, d'une utilisation abusive des informations ou d'une attaque contre le système), atteinte à la disponibilité (par ex. en cas de panne des systèmes, de perte d'informations ou de *ransomware*), atteinte à la traçabilité (par ex. par la falsification ou la perte des protocoles).

Les risques relatifs à la protection des données se rapportent aux différentes opérations de traitement des données. Ils dépassent la simple sécurité des données. Exemples : collecte et traitement illicites de données personnelles, utilisation de données personnelles à des fins non prévues, traitement de données incorrectes, accès non autorisé à des données personnelles, conservation excessivement longue de données personnelles, déni des droits des personnes concernées.

Probabilité de survenance

Une fois les risques potentiels identifiés, il s'agit de procéder pour chaque risque à une évaluation de la probabilité de survenance du risque et de son impact sur les droits fondamentaux de la personne concernée.

On procède à l'évaluation du risque à l'aide de la matrice de risques 6 x 6, également appliquée dans le cadre de l'analyse de risque détaillée prévue par le concept SIPD[1]. Les risques qui apparaissent en jaune ou en rouge dans la matrice de risques doivent être considérés comme des risques élevés. Des mesures doivent être prises pour les réduire.



[1] Le modèle d'analyse détaillée des risques du concept SIPD peut être consulté sur la page suivante : https://www.ncsc.admin.ch/ncsc/fr/home.html > Documentation > Directives de sécurité informatique > Procédure de sécurité > Protection élevée.

Les répercussions peuvent être d'ordre physique (par ex. un traitement médical incorrect en raison de données erronées), matériel (par ex. la perte d'un emploi, l'utilisation abusive de la carte de crédit, le prélèvement de taxes injustifiées) ou immatériel (discrimination, entre autres : racisme, sexisme, désavantages sociaux, stigmatisation en raison d'une maladie). L'impact sur les droits fondamentaux de la personne concernée ou le degré de gravité des risques peuvent être répartis en six échelons : très faible, faible, modéré, important, élevé, très élevé. Ces échelons peuvent être définis de la manière suivante.

Très faible : aucune répercussion sur les droits fondamentaux ; pas d'atteintes notables à l'intégrité sur le plan moral ou social ; pas de préjudice financier présentant un lien de causalité adéquat avec l'atteinte subie (ex. : léger dépassement de la durée de conservation autorisée des données personnelles ; appels téléphoniques ou messages non sollicités sans conséquences directes ou indirectes).

Faible : répercussions négligeables sur les droits fondamentaux ; atteintes à peine perceptibles à l'intégrité sur le plan moral ou social ; éventuellement, préjudice financier négligeable présentant un lien de causalité adéquat avec l'atteinte subie (ex. : nécessité de changer de compte Internet, d'adresse électronique ou de numéro de téléphone).

Modéré : répercussions mineures à long terme ou majeures à court terme sur les droits fondamentaux ; atteintes peu graves à l'intégrité sur le plan physique, psychique, moral ou social ; éventuellement préjudice financier présentant un lien de causalité adéquat avec l'atteinte subie (ex. : fait d'influencer de manière indue et non transparente le comportement d'achat).

Important/Élevé : longues et sévères répercussions sur les droits fondamentaux ; atteintes moyennement graves à l'intégrité sur les plans physique, psychique, moral ou social ; préjudice financier substantiel présentant un lien de causalité adéquat avec l'atteinte subie (ex. : refus opposé à une relation contractuelle, résiliation d'une relation contractuelle ; atteinte à la réputation).

Très élevé : répercussions fatales sur les droits fondamentaux ; graves atteintes à l'intégrité sur les plans physique, psychique, moral ou social ; préjudice financier menaçant l'existence de l'entité concernée et présentant un lien de causalité adéquat avec l'atteinte subie (ex. : traitement médical erroné lourd de conséquences, dû à l'inexactitude des informations sur le patient ou à la mauvaise identification du patient) ; menace de poursuites pénales transfrontalières résultant de données personnelles divulguées dans le pays d'origine d'un requérant d'asile, avec des risques pour la personne concernée ou sa famille (intégrité physique, vie, etc.).

La probabilité de survenance consiste en une estimation de la probabilité que surviennent certains événements à l'avenir sur une période donnée. Elle est également répartie en six échelons : très improbable, improbable, rare, possible, probable, très probable. La légende appliquée dans le cadre de l'analyse de risque détaillée du concept SIPD peut être utilisée pour évaluer la probabilité. D'après cette légende, la probabilité doit être évaluée d'après l'échelle suivante :

très improbable	plus de 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 an

Mesures envisagées

Les mesures possibles pour la protection des personnes concernées peuvent comprendre des mesures organisationnelles aussi bien que techniques.

Exemples (non exhaustifs) de mesures organisationnelles : mise en place de formations, directives, guides d'utilisation, stratégies de droits d'accès, obligations de confidentialité, SMSI, processus pour les droits d'accès, processus pour les demandes de suppression et contrôle de conformité.

Exemples (non exhaustifs) de mesures techniques : contrôles d'accès, contrôles d'utilisation, accès limités dans le temps, codages, anonymisation et minimisation des données.

5. Consultation du conseiller à la protection des données et du PFPDT

Si l'AIPD révèle que, malgré les mesures prises ou prévues, le traitement des données présente un risque élevé pour les personnes concernées, le responsable du traitement est tenu de consulter le conseiller à la protection des données, puis le PFPDT (voir art. 10 et 23 LPD).