1 Méthode « GRC » pour réaliser une AIPD avec MONARC

1.1 Généralités

Une AIPD est un processus itératif permettant de vérifier la maîtrise permanente des impacts relatifs aux droits et libertés des personnes concernées lors d'un traitement de données à caractère personnel.

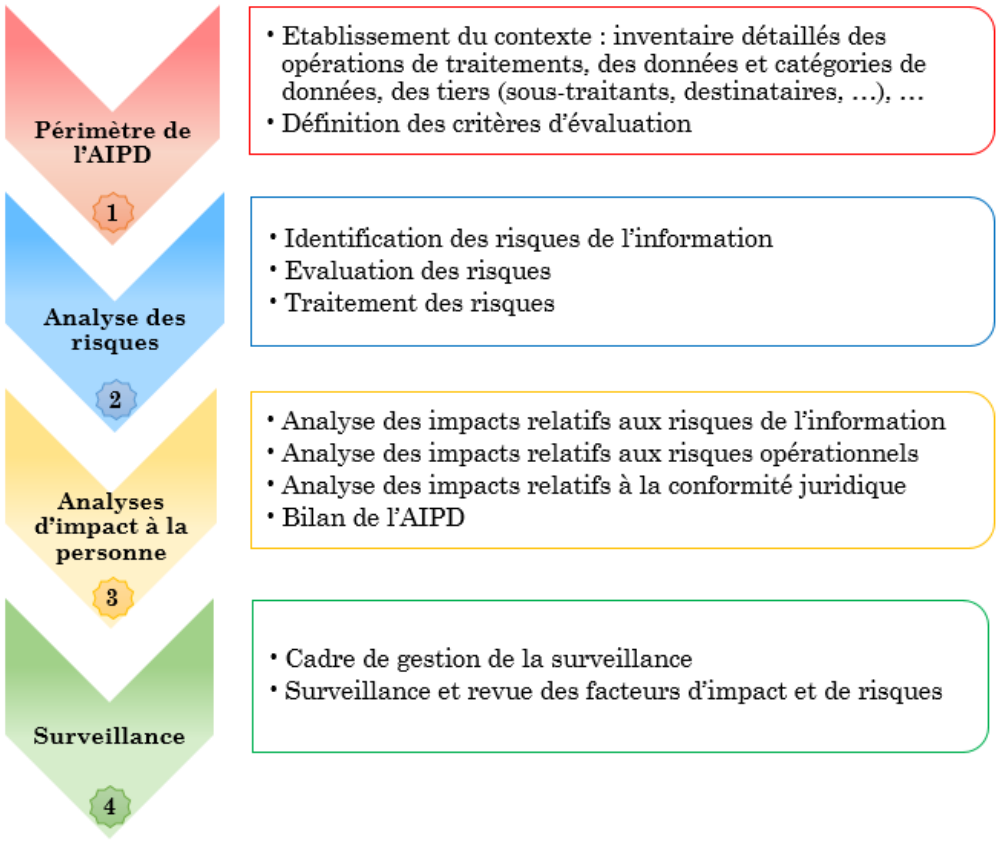
L'AIPD englobe des processus qui sont eux-mêmes itératifs comme la gestion des risques (ISO/IEC 27005). Il faut donc mettre en place un cadre de gestion cohérent qui prend en compte la mise à jour périodique de l'AIPD.

La cible de l'AIPD peut porter sur un traitement ou un ensemble d'opérations de traitement en fonction du contexte. Un responsable du traitement peut également avoir recours à plusieurs AIPD pour couvrir l'ensemble des traitements sur lesquels il juge qu'une AIPD est nécessaire ou obligatoire.

La base de l'AIPD est le registre des traitements du responsable du traitement, de préférence [1]déjà conforme.

1.2 Présentation de la méthodologie

La méthode d'AIPD de GRC Luxembourg se repose sur la méthodologie d'analyse des risques de l'information MONARC et son outil associé. Chaque étape de l'analyse est décomposée en 4 phases, décrites ci-dessous :



[1] L'AIPD ne démontre pas à elle seule la conformité des opérations de traitement au GDPR. Par contre son absence, si elle était requise remettrait en cause la conformité.

1.2.1 Phase 1 : Périmètre de l'AIPD

La phase 1 permet de détailler le ou les traitement(s) sur lequel(s) le processus d'AIPD va se dérouler.

Il s'agit de définir ce qui est inclus dans l'analyse et de collecter l'information suffisante pour appréhender les risques et impacts générés par le traitement.

À ce stade, il est nécessaire d'inclure les processus internes, mais aussi les interfaces avec les parties prenantes comme les sous-traitants, les destinataires, tiers, etc.

Les critères d'impacts à la personne doivent être personnalisés en fonction des catégories de données traitées et du contexte. Les critères d'évaluation et d'acceptation des risques et les risques bruts (inhérents) doivent être également définis.

1.2.2 Phase 2 : Analyse des risques de l'information

MONARC propose une démarche complètement standard et met en œuvre la norme internationale du domaine, à citer ISO/IEC 27005.

Le contexte est déjà défini en phase 1, les processus ISO/IEC 27005 à dérouler sont :

- L'identification des risques.
- L'évaluation des risques.
- Le traitement des risques.

Cette phase peut directement intégrer ou non l'impact à la personne en fonction de l'itération d'analyse en cours (1ère ou suivantes).

1.2.3 Phase 3 : Analyses d'impacts à la personne et bilan de l'AIPD

La phase 3 est composée de 3 analyses d'impact distinctes en fonction des 3 typologies de risques :

1 Risques de l'information : Les critères challengés sont la confidentialité, l'intégrité et la disponibilité de l'information. Pour chacun de ces critères, des scénarios de risques sont proposés à partir de bases de connaissances du domaine de la sécurité de l'information fournies par MONARC.
Les impacts sont définis au niveau des processus et sous-processus en fonction des conséquences que pourraient avoir sur les personnes concernées, une perte de confidentialité, d'intégrité ou de disponibilité des données et des processus.
Dans le but de réduire l'impact à la personne, les mesures de sécurité proposées sont issues du référentiel de bonnes pratiques ISO/IEC 27002.

2 Risques opérationnels : Ce sont les risques liés aux activités métiers ou non qui réalisent les traitements. Ils proviennent de processus internes inadéquats ou défaillants, de personnes et systèmes ou d'évènements externes. Parfois proches des risques de l'information, les risques opérationnels pourraient se définir dans l'une ou l'autre des typologies. Dans le cadre des risques opérationnels, les critères challengés sont habituellement le ROLF : « Réputation », « Opération », « Légal » et « Financier » de l'organisme traitant les données. Pour l'AIPD, il faut se focaliser sur le 5ème critère qui est « P : l'impact à la personne ». Dans MONARC, la terminologie utilisée est « ROLFP » qui réunit tous ces critères cités ci-dessus.

3 Risques dus au traitement ou à des non-conformités au RGPD : Il s'agit des risques à la personne qui pourraient être générés par le traitement lui-même ou par le non-respect d'exigences formulées par le RGPD. Par exemple, l'absence de procédure de traitement des violations qui ne permettrait pas d'informer les personnes concernées d'une violation de leurs données à temps.

La plupart des articles du RGPD sont concernés, sauf l'article 32 qui est traité principalement traité dans la partie risques de l'information.

Dès lors où les 3 analyses d'impacts sont achevées, les risques relatifs aux droits et libertés générés par le traitement sont pour la plupart connus et évalués. Un plan d'action de réduction des risques peut-être éventuellement dressé, ainsi que le bilan de l'AIPD. Toutes les conclusions concernant le futur traitement ou le traitement en cours sont formulées en connaissance de cause.

1.2.4 Phase 4 : Surveillance

La phase 4 permet de s'assurer qu'un cadre de gestion est présent. Il a pour objectif de vérifier qu'il n'y a pas de dégradation de la situation de risques dans le temps. Des processus doivent être déclenchés pour contrôler périodiquement les changements internes (modification des traitements, des catégories de données manipulées, changements de technologies, etc.) ou externes (changement de sous-traitant, évolution des menaces, etc.).

Le registre des traitements et les AIPD doivent être mis à jour périodiquement.

1.3 Utilisation de l'outil MONARC pour gérer les AIPD

Le principe est de maintenir deux analyses de risques permanentes qui sont mises à jour régulièrement :

1 « Analyse des risques de l'information ».
2 « Analyse des risques opérationnels ».

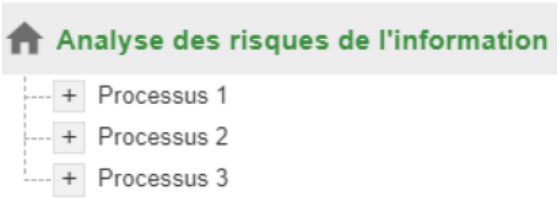
Pour générer une AIPD, il suffit de créer une analyse temporaire qui inclut les composants spécifiques de chaque analyse permanente en fonction de la cible de l'AIPD :

3 « AIPD : *Nom du traitement* ».

Le livrable final de l'AIPD est un document personnalisé décrivant l'organisation de projet, la méthode déroulée, les résultats obtenus, ainsi que toutes les informations issues automatiquement de MONARC, telles que les échelles d'évaluation et d'acceptation des risques, le plan de traitement des risques, les évaluations des 3 typologies de risques, etc.

1.3.1 Analyse : « Analyse des risques de l'information »

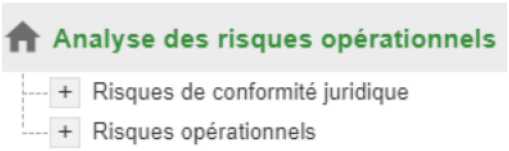
L'analyse est maintenue par le RSSI ou par une personne ayant un rôle équivalent. C'est idéalement une analyse menée sur l'ensemble de l'organisme, organisée par processus (vue transversale proche des opérations de traitement) ou par service fonctionnel.



1.3.2 Analyse : « Analyse des risques opérationnels »

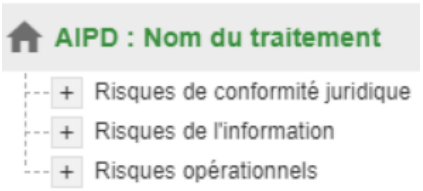
L'analyse elle est maintenue par le DPO ou par une personne ayant un rôle équivalent. Elle contient tous les risques opérationnels organisés :

1 Par « Risque de conformité juridique » : conformité au RGPD.
2 Par « Risques opérationnels » : Scénarios de risques inhérents au métier.



1.3.3 Analyse temporaire : « AIPD : *Nom du traitement* »

L'analyse contient la copie des éléments spécifiques d'une AIPD. Selon la taille de l'organisme, elle pourrait devenir l'AIPD de tous les processus de l'organisme.



1.4 Respect de l'article 35 vs méthode d'AIPD GRC Luxembourg

L'article 35 est composé de 11 alinéas :

- Article 35-1 : Réalisé dans la phase 1.
- Article 35-2 : Réalisé dans la phase 4.
- Article 35-3abc : Réalisé dans la phase 1.
- Article 35-4 : Non applicable. La CNPD n'a pas publié de liste noire. Dois être réalisé en 2019.
- Article 35-5 : Non applicable. La CNPD n'a pas publié de liste blanche. Dois être réalisé en 2019.
- Article 35-6 : Non applicable à cause des raisons citées ci-dessus (article 35-4 et 5).
- Article 35-7a : Réalisé dans la phase 1.
- Article 35-7b : Réalisé dans la phase 1. (4.1.2)
- Article 35-7c : Réalisé dans la phase 2 et la phase 3.
- Article 35-7d : Réalisé dans la phase 3, plan de traitement des risques.
- Article 35-8 : Hors compétences.
- Article 35-9 : Justification apportée dans la phase 1.
- Article 35-10 : Aucune analyse d'impact générale n'a été réalisée dans le cadre de l'adoption de la base juridique du traitement.
- Article 35-11 : Justification apportée dans la phase 4.