PROTECTION DES DONNÉES : COMMENT RÉALISER UNE ANALYSE D'IMPACT ?

JUDITH DUCHÊNE
Conseillère

Pour chaque traitement de données susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées, une analyse d'impact relative à la protection des données doit être menée avant le début du traitement. Si les DPD connaissent bien ces principes, ils ont peu l'occasion de partager des exemples concrets auxquels ceux-ci pourraient s'appliquer en CPAS. Lors de la Plateforme des DPD de CPAS du 9 novembre 2021, deux DPD de CPAS[1] sont venus présenter deux analyses d'impact qu'ils avaient eu l'occasion de réaliser. Nous reprenons, dans cet article, les principaux enseignements de leurs présentations complétés par des ressources méthodologiques issues de différents documents émanant de l'Autorité de Protection des Données et de la CNIL[2].

Qu'est-ce qu'une analyse d'impact ?

L'article 35, § 1, du RGPD indique que « *Lorsqu'un type de traitement* […] *est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue,* ***avant le traitement****, une analyse de l'impact des opérations de traitement envisagées* […] ».

L'analyse d'impact relative à la protection des données (AIPD) est donc un outil qui vise à responsabiliser les responsables de traitement avant de réaliser un traitement de données.

Reste à savoir comment déterminer le périmètre de son champ d'application. Comment apprécier cette notion de « risque élevé » qui n'est pas définie dans le RGPD lui-même ?

Le « risque » peut être ici compris comme la possibilité qu'une conséquence négative pour les droits et libertés des personnes physiques survienne, à la suite d'un traitement de données à caractère personnel.

Source : CNIL[3]

Définir son champ d'application

Il n'est pas requis que le responsable du traitement procède à une AIPD pour chaque traitement de données à caractère personnel.

L'article 35, § 3, du RGPD indique qu'une analyse d'impact relative à la protection des données est **toujours requise** dans les cas suivants :

- l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé ;
- le traitement à grande échelle de données sensibles[4] ;
- la surveillance systématique à grande échelle d'une zone accessible au public.

Il s'agit de traitements qui sont, par nature, susceptibles d'engendrer un risque élevé[5].

Neuf critères ont été définis par le Groupe 29 pour déterminer s'il est ou non probable qu'un traitement de données envisagé donne lieu à un risque élevé[6].

1. Évaluation ou notation, y compris les activités de profilage et de prédiction.
2. Prise de décision automatisée avec effet juridique ou effet similaire significatif.
3. Surveillance systématique.
4. Données sensibles ou données à caractère hautement personnel.
5. Traitement de données à caractère personnel à grande échelle.
6. Croisement ou combinaison d'ensembles de données.
7. Données concernant des personnes vulnérables (enfants, travailleurs, personnes souffrant de maladie mentale, demandeurs d'asile, personnes âgées, patients…).
8. Utilisation ou application innovante de nouvelles solutions technologiques ou organisationnelles.
9. Lorsque, du fait du traitement lui-même, les personnes concernées ne peuvent pas exercer un droit ou bénéficier d'un service ou d'un contrat.

Dans la plupart des cas, il peut être considéré qu'une analyse d'impact doit être réalisée lorsqu'un traitement répond à **deux** de ces critères et que le risque croit à mesure qu'un même traitement répond à un nombre de plus en plus élevé de critères.

L'Autorité de Protection des Données (APD) a, conformément à l'article 35, § 4, du RGPD, publié une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

---

1 Sorin Lazarescu, DPD mutualisé, et Ludivine Carels, ancienne DPD mutualisée.

2 Commission nationale de l'Informatique et des Libertés de France.

3 CNIL, *Analyse d'impact relative à la protection des données*, 2.2018, p. 3. V. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf.

4 Telles que définies dans l'art.9, § 1 du RGPD.

5 APD, Recommandation n° 1/2018 du 28.2.2018, p. 7. V. https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2018.pdf

6 *Ibid.*, pp. 9-11.

Suivant cette liste, outre les cas prévus à l'article 35, § 3, que nous venons de mentionner, une AIPD est requise lorsque[7] :

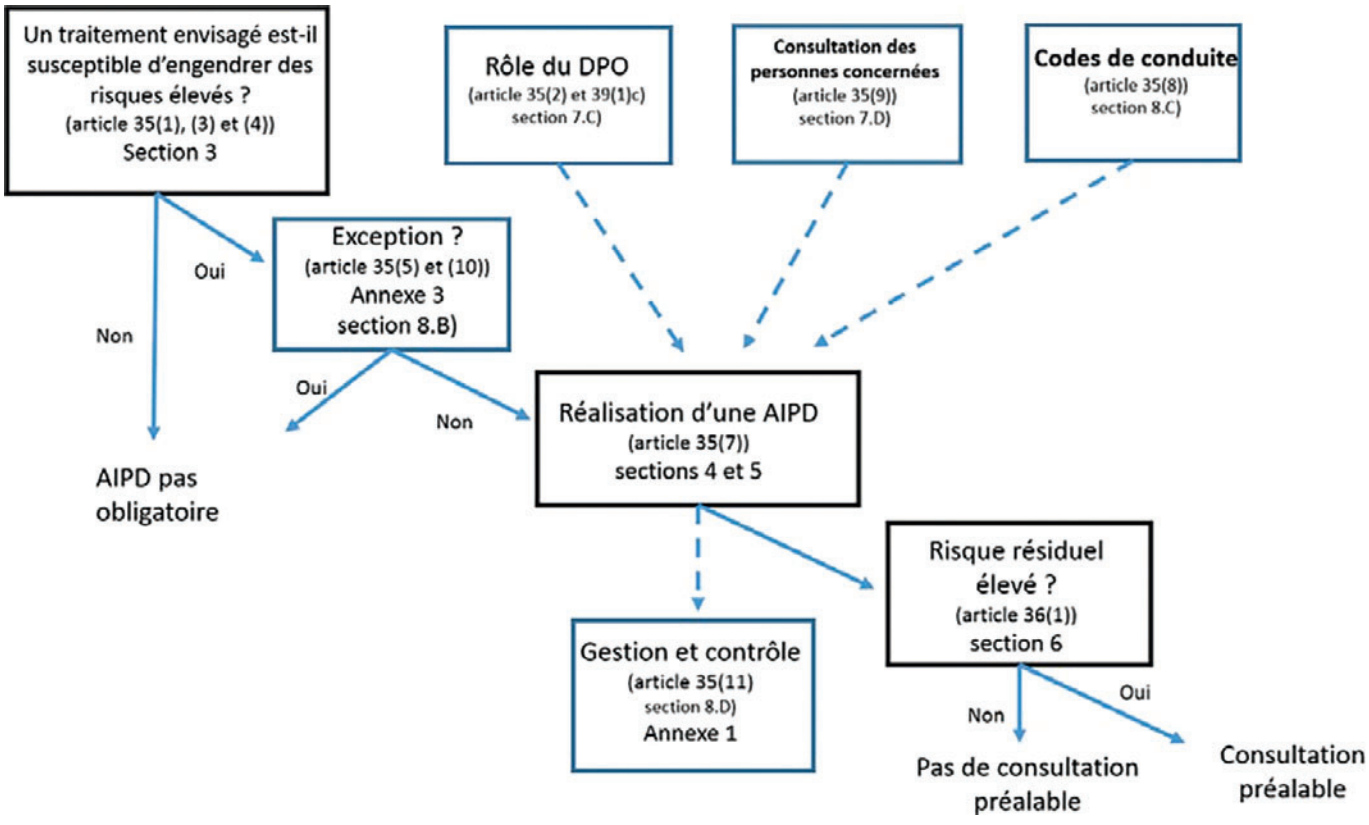
- le traitement utilise des données biométriques en vue de l'identification unique des personnes concernées se trouvant dans un lieu public ou dans un lieu privé accessible au public ;
- des données à caractère personnel sont collectées auprès de tiers afin d'être prises ensuite en considération dans le cadre de la décision de refuser ou de cesser un contrat de service déterminé avec une personne physique ;
- des données de santé d'une personne concernée sont collectées par voie automatisée à l'aide d'un dispositif médical implantable actif ;
- des données sont collectées à grande échelle auprès de tiers afin d'analyser ou de prédire la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements de personnes physique ;
- des données sensibles ou des données de nature très personnelle (données sur la pauvreté, le chômage, l'implication de l'aide à la jeunesse ou le travail social, données sur les activités domestiques et privées, données de localisation) sont échangées systématiquement entre plusieurs responsables du traitement ;
- il y a traitement à grande échelle de données générées au moyen d'appareils dotés de capteurs qui envoient des données via internet ou via un autre moyen (télévisions intelligentes, appareils ménagers intelligents, jouets connectés, « smart cities », compteurs d'énergie intelligent...) servant à analyser ou prédire la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements de personnes physiques ;
- il y a traitement à grande échelle et/ou systématique de données de téléphonie, d'internet ou d'autres données de communication, de métadonnées ou de données de localisation de personnes physiques ou permettant de mener à des personnes physiques lorsque le traitement n'est pas strictement nécessaire pour un service demandé par la personne concernée ;
- il y a traitement de données à caractère personnel à grande échelle où le comportement de personnes physiques est observé, collecté, établi ou influencé, y compris à des fins publicitaires, et ce de manière systématique via un traitement automatisé.

Au contraire, l'article 35, § 10, du RGPD prévoit deux circonstances dans lesquelles l'obligation de procéder à une AIPD n'est potentiellement pas d'application[8] :

- lorsque le traitement envisagé est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- lorsque le traitement envisagé est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

De même, l'APD a publié une liste des types d'opérations de traitement pour lesquelles aucune AIPD n'est requise[9]. Nous ne la détaillerons pas ici par souci de concision.

Les modalités que nous venons de détailler peuvent être schématisées comme suit[10] :



7 *Ibid.*, p. 43.

8 *Ibid.*, p. 33.

9 *Ibid.*, p. 45.

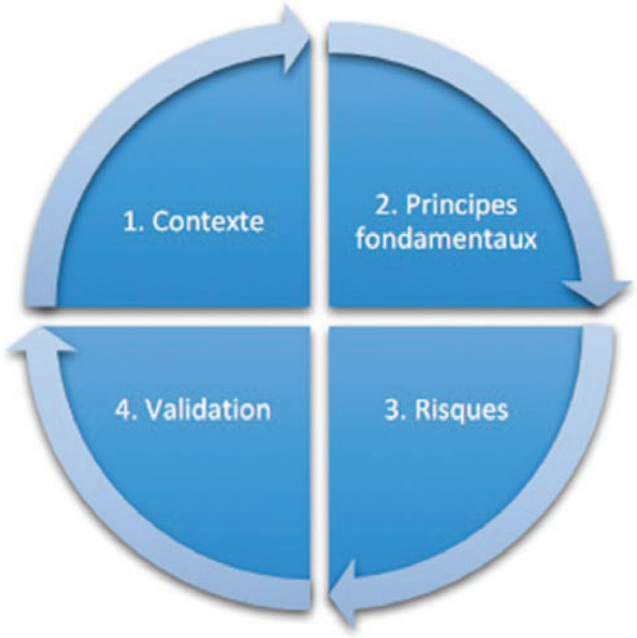
10 *Ibid.*, p. 5.

Quels sont les intervenants pour la réalisation d'une AIPD ?

L'obligation de procéder à une AIPD incombe en premier lieu au responsable du traitement qui endosse la responsabilité finale et est responsable si l'AIPD n'est pas (ou pas correctement) réalisée[11].

Le responsable de traitement doit veiller à ce que les bonnes personnes au sein de la structure soient impliquées, en temps opportun, dans l'évaluation des risques : le délégué à la protection des données évidemment mais aussi, le personnel du service informatique, les juristes, les personnes qui prennent les décisions stratégiques, les personnes faisant partie du service concerné par le traitement de données, les sous-traitants impactés par le projet…

Étapes à suivre pour la réalisation d'une AIPD[12]



Source : CNIL[13]

1. Étudier le contexte

Il s'agit, lors de cette étape, de disposer d'une vision claire des traitements de données personnelles considérés ; de délimiter et décrire leur contexte.

- Quel est le traitement considéré, sa nature, sa portée, son contexte, ses finalités, ses enjeux ?
- Qui est le responsable de traitement ? Quels sont les éventuels sous-traitants ?
- Quels sont les référentiels applicables au traitement (codes de conduite, certification, politique de sécurité, normes juridiques sectorielles…) ?
- Quelles sont les données concernées, les destinataires, les durées de conservation ?
- Quels sont les processus et les supports utilisés de la collecte à l'effacement des données ?

2. Étudier les principes fondamentaux

Il s'agit de bâtir un dispositif de conformité en adéquation avec les principes de protection de la vie privée.

- Évaluer les mesures garantissant la proportionnalité et la nécessité du traitement :
  - expliciter et justifier les choix effectués pour respecter les exigences relatives à la finalité du traitement, à son fondement, à la minimisation des données, leur qualité et la limitation de la durée de conservation ;
  - vérifier qu'il n'est pas utile/pas possible d'améliorer chacun des points ;
  - si c'est le cas, revoir la description/proposer des mesures complémentaires.
- Évaluer les mesures protectrices des droits des personnes concernées :
  - déterminer et décrire les mesures pour respecter les exigences relatives à l'information des personnes concernées, le recueil du consentement, l'exercice des droits des personnes (accès, portabilité, rectification, effacement, limitation, opposition), la sous-traitance, les transferts de données ;
  - vérifier qu'il n'est pas utile/pas possible d'améliorer chacun des points ;
  - si c'est le cas, revoir la description/proposer des mesures complémentaires.

3. Étudier les risques liés à la sécurité des données

Il s'agit d'apprécier les risques sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités.

Un risque est « *un scénario hypothétique qui décrit un événement redouté et toutes les menaces qui permettraient qu'il survienne. Plus précisément, il décrit :*

- comment des sources de risques (ex. : un salarié soudoyé par un concurrent)
- pourraient exploiter les vulnérabilités des supports de données (ex. : le système de gestion des fichiers, qui permet de manipuler les données)
- dans le cadre de menaces (ex. : détournement par envoi de courriers électroniques)
- et permettre à des événements redoutés de survenir (ex. : accès illégitime à des données)
- sur les données à caractère personnel (ex. : fichier des clients)
- *et ainsi provoquer des impacts sur la vie privée des personnes concernées (ex. : sollicitations non désirées, sentiment d'atteinte à la vie privée, ennuis personnels ou professionnels)* »[14].

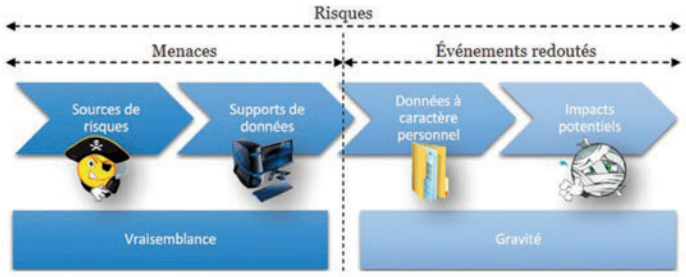
Le niveau de risque doit être évalué au regard des impacts potentiels qu'un risque peut avoir (gravité) et de la vraisemblance qu'il se produise.

[11] *Ibid.*, p. 27.

[12] CNIL, *Analyse d'impact relative à la protection des données*, 2.2018. V. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf

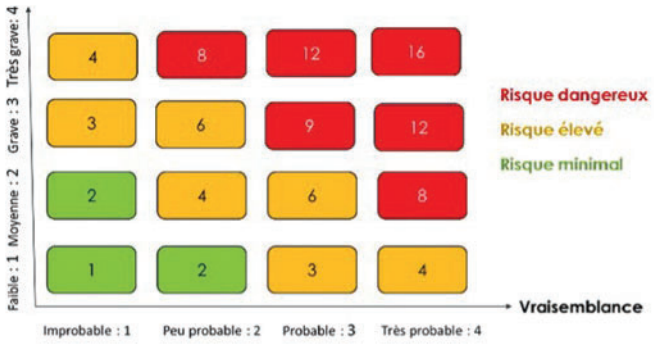
[13] *Ibid.*, p. 3.

[14] *Ibid.*, p.6.



Source : CNIL[15]

- Évaluer les mesures existantes ou prévues et contribuant à la sécurité :
  - identifier ou déterminer les mesures existantes ou prévues (déjà engagées) qui portent sur les données du traitement (chiffrement, anonymisation, cloisonnement, contrôle d'accès, traçabilité…), sur la sécurité du système dans lequel le traitement est mis en œuvre (sécurité de l'exploitation, sauvegardes, sécurité des matériels…), sur les mesures organisationnelles (politique, gestion des projets, gestion des personnels, gestion des incidents et violations, relations avec les tiers…) ;
  - vérifier qu'il n'est pas utile/pas possible d'améliorer chacun des points ;
  - si c'est le cas, revoir la description/proposer des mesures complémentaires.
- Apprécier les causes et conséquences des risques et les atteintes potentielles à la vie privée (accès illégitime aux données, modification non désirée de données, disparition de données) :
  - déterminer les impacts potentiels sur la vie privée des personnes s'ils survenaient ;
  - estimer la gravité (par exemple, une matrice de risques peut être utilisée : faible = 1 ; moyenne = 2 ; grave = 3 ; très grave = 4) ;
  - identifier les menaces sur les supports des données et les sources de risques ;
  - estimer la vraisemblance des risques (par exemple, dans la matrice de risque ci-dessous : improbable = 1 ; peu probable (rare) = 2 ; probable (possible) = 3 ; très probable (fréquente) = 4) ;



  - estimer si les risques sont acceptables ou, si ce n'est pas le cas, proposer des mesures de sécurité complémentaires.

[15] *Ibid.*, p. 6.

4. Validation

Au regard des résultats de l'analyse, l'AIPD doit être validée ou pas.

- Préparer les éléments utiles à la validation :
  - consolider et mettre en forme les résultats de l'analyse ;
  - formaliser la prise en compte des parties prenantes.
- Valider formellement l'analyse :
  - décider de l'acceptabilité des mesures choisies, des risques résiduels et du plan d'action, de manière argumentée, au regard des enjeux préalablement identifiés et de l'avis des parties prenantes → l'analyse peut être validée, à améliorer (expliquer sur quels aspects), refusée (ainsi que le traitement considéré) ;
  - si c'est indiqué, revoir les étapes précédentes pour que l'analyse puisse être validée.

Un outil qui peut vous aider

La CNIL met gratuitement à disposition sur son site un logiciel open source appelé PIA qui permet de faciliter la conduite et la formalisation d'analyses d'impact[16]. ■

[16] https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil