CNIL.

Fiche n° 5 - Quelles démarches accomplir préalablement à la mise en œuvre d'un traitement ?

Un responsable de traitement doit pouvoir démontrer, grâce à une documentation adaptée, le respect des principes « Informatique et Libertés » pour tous les traitements mis en œuvre dans son organisme, notamment au moyen du registre des activités de traitement et des analyses d'impact relatives à la protection des données.

Règles de droit

Le RGPD a établi une logique de responsabilisation des acteurs : les formalités préalables ont ainsi été remplacées par une obligation de démontrer le respect des principes « informatique et libertés ». Ils doivent, à cet égard, mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles dès le départ.

Une structure doit donc adopter **une démarche continue de conformité** au travers notamment de l'élaboration d'une documentation et de procédures permettant de prouver le respect des règles relatives à la protection des données.

Pour cela, elle doit notamment :

- tenir un **registre des traitements de données** mis en place ;
- mener des **analyses d'impact relatives à la protection des données** (« **AIPD** ») pour les traitements susceptibles de présenter « **un risque élevé** » pour les personnes ;
- formaliser **les rôles et responsabilités des différents acteurs** qui interviennent dans les traitements mis en place (p.ex. : contrat de sous-traitance établi avec un prestataire) ;
- documenter **les mesures prises pour garantir la sécurité** des données personnelles ;
- désigner un référent ou un **délégué à la protection des données** (DPD ou DPO pour *Data Protection Officer*).

En pratique

Une structure dispose de plusieurs outils pour documenter la conformité de ses traitements.

1. Le registre des traitements

Il s'agit d'un **outil de pilotage** permettant de recenser tous les traitements de données personnelles que l'organisme met en œuvre afin de disposer d'un panorama complet des traitements mis en œuvre.

Chaque fiche composant ce guide présente les caractéristiques d'un traitement :

- les **parties prenantes** (notamment les sous-traitants et responsable(s) des traitements) qui interviennent dans le traitement des données personnelles collectées ;
- les **catégories de données personnelles** collectées ;
- **à quoi servent** les données collectées (le ou les objectifs poursuivis par le traitement), **qui peut y accéder** et **à qui elles sont communiquées** (les destinataires) ;
- **combien de temps les données personnelles sont conservées** ;
- si des **transferts d'informations vers des pays tiers** sont prévus et dans ce cas, les garanties associées à ces transferts ;
- comment ces informations sont **sécurisées**.

Focus

Bien qu'elle ne soit pas dans l'obligation de le formaliser par écrit, une structure doit être en mesure de **justifier ses choix**, c'est-à-dire qu'elle doit pouvoir **démontrer en quoi les caractéristiques du traitement** (durées de conservation, données collectées, destinataires des données, conditions de sécurité, etc.) **sont appropriées à ses besoins**.

Afin d'avoir une documentation la plus complète possible, **divers documents sont susceptibles d'être annexés au registre** : audit de sécurité, contrat de sous-traitance, etc.

Cette documentation, particulièrement le registre, doit être régulièrement mise à jour lorsqu'une modification est opérée sur le traitement (nouvelles données collectées, allongement de la durée de conservation, etc.).

Le registre **est un document interne que l'organisme doit conserver**. Il ne doit pas être envoyé à la CNIL, sauf si elle le demande.

2. L'analyse d'impact relative à la protection des données (AIPD)

Un organisme doit réaliser une AIPD pour chaque traitement susceptible de présenter un risque élevé pour les droits et les libertés des personnes concernées.

Tel est le cas lorsque le traitement remplit **au moins deux critères sont remplis parmi les neuf critères suivants** :

- évaluation ou notation d'une personne ;
- prise de décision automatisée ;
- surveillance systématique ;
- traitement de données sensibles ou à caractère hautement personnel (notamment données de santé, revenus, données bancaires) ;
- traitement à grande échelle ;
- croisement ou combinaison d'ensembles de données personnelles ;
- données concernant des personnes vulnérables ;
- utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles ;
- traitement qui empêche les personnes d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

Certains traitements doivent obligatoirement faire l'objet d'une AIPD : c'est notamment le cas des traitements relatifs à l'instruction des demandes de logement social et d'accession à la propriété ainsi que la gestion des logements sociaux. Ces derniers figurent en effet sur la liste des traitements devant obligatoirement faire l'objet d'une AIPD.

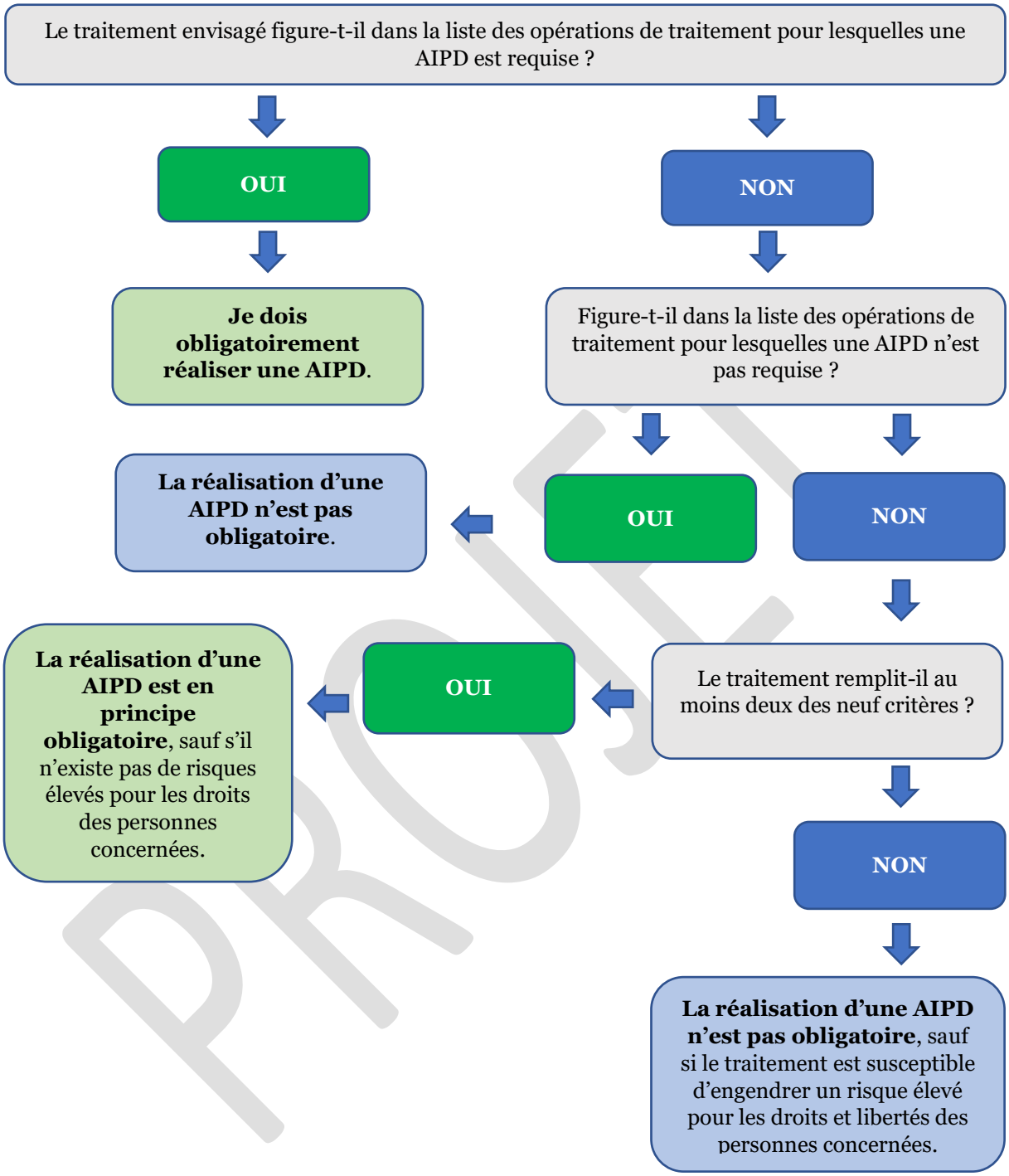
À l'inverse, les bailleurs sont dispensés d'élaborer une AIPD pour les traitements figurant sur cette liste.

Hypothèses dans lesquelles le traitement figure dans la liste des opérations de traitements nécessitant une AIPD (liste non-exhaustive)	
Traitements	*Critères remplis*
Instruction des demandes de logement des candidats à la location et décision d'attribution Gestion du relogement dans le cadre des opérations de travaux et rénovation urbaine	• Données sensibles ou à caractère hautement personnel • Evaluation ou notation
Mise en place d'un suivi social personnalisé afin de permettre le maintien au sein du logement ou un aménagement adapté	• Données sensibles ou à caractère hautement personnel • Personnes dites « vulnérables »
Mutualisation de la liste des locataires en situation de fraude ou de manquement contractuel	• Croisement ou combinaison d'ensemble de données • Prise de décision automatisée avec effet juridique ou effet similaire significatif

Dans les hypothèses où le traitement ne figure sur aucune liste, une analyse devra être menée au cas par cas. Si deux critères ou plus sont remplis, une AIPD devra être réalisée.

Hypothèses pour lesquelles une AIPD devra, en principe, être réalisée car le traitement remplit plusieurs critères et est donc susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées (liste non-exhaustive)	
Traitements	*Critères remplis*
Signalement des locataires suspectés de radicalisation	• Données sensibles • Personnes dites « vulnérables »
Signalement des locataires en danger ou dangereux aux établissements sociaux, médicaux et médico-sociaux	
Liste noire des locataires ou anciens locataires mise en œuvre aux fins d'écarter les personnes d'un futur bail	• Prise de décision automatisée • Traitements qui empêchent les personnes d'exercer un droit ou de bénéficier d'un service ou d'un contrat • Données concernant des personnes vulnérables

Schéma récapitulatif



Comment réaliser une AIPD ?

L'analyse d'impact se décompose en trois parties :

- une **description détaillée du traitement** mis en place, comprenant tant les aspects techniques qu'opérationnels ;
- une **évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux** (finalité, données personnelles et durées de conservation, information et droits des personnes, etc.), qui sont fixés par la loi et doivent être respectés, quels que soient les risques ;

- une **évaluation, de nature plus technique, des risques sur la sécurité des données** (confidentialité, intégrité et disponibilité) ainsi que leur impact potentiel sur les personnes concernées s'ils se matérialisent, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données personnelles.

Le DPO devra être consulté pour l'élaboration de ces fiches. Dans le cas où l'analyse d'impact indiquerait que les mesures ne permettent pas de réduire les risques à un niveau acceptable, l'organisme doit consulter la CNIL préalablement à la mise en place du traitement.

Ce document devra également faire l'objet de mises à jour pendant toute la durée du traitement.

La CNIL propose des outils méthodologiques ainsi que des modèles pour accompagner les responsables de traitement dans la réalisation d'une AIPD et la constitution du registre des traitements mis en place.

Pour en savoir plus : Le registre des activités de traitement et l'analyse d'impact relative à la protection des données (AIPD)

Pour se mettre en conformité

- **se poser** les bonnes questions avant le traitement : l'organisme a-t-il vraiment besoin de certaines données concernant le candidat à la location/le locataire dans le cadre de son traitement ? Est-il pertinent de conserver les données aussi longtemps ? Les données sont-elles suffisamment protégées ? etc. ;
- **renseigner** et **mettre à jour** régulièrement la fiche dédiée dans le registre des traitements mis en place par la structure ;
- **vérifier** en fonction des caractéristiques du traitement si une analyse d'impact doit être réalisée et, pour ce faire, apprécier dans quelle mesure le traitement envisagé présente un risque élevé pour les personnes concernées.

Références

- Articles 30 (registre des activités de traitement) et 35 (analyse d'impact relative à la protection des données) du RGPD
- L'analyse d'impact relative à la protection des données (AIPD)
- Lignes directrices du 4 avril 2017 du CEPD concernant l'analyse relative à la protection des données et la manière de déterminer si le traitement est susceptible d'engendrer un risque élevé