RGPD Niveau II

L'ANALYSE D'IMPACT

GRAND PARIS SEINE OUEST

BOULOGNE-BILLANCOURT
CHAVILLE
ISSY-LES-MOULINEAUX
MARNES-LA-COQUETTE
MEUDON
SÈVRES
VANVES
VILLE-D'AVRAY

Direction des Affaires Institutionnelles - Mars 2024

Sommaire

GRAND PARIS SEINE OUEST

Qu'est-ce que l'AIPD ?

*** Version Française :** **AIPD = Analyse d'impact relative à la protection des données**

*** Version Anglaise :** **PIA = Privacy Impact Assessment (évaluation de l'impact sur les données personnelles).**

L'article 35 du RGPD impose qu'une AIPD soit effectuée en amont de la mise en place d'un traitement.

1. L'AIPD = outil essentiel de conformité au **Règlement général sur la protection des données (RGPD)**.
2. Démarche qui vise à construire un traitement **respectueux de la vie privée**.
3. L'AIPD s'applique aux traitements de données personnelles susceptibles d'engendrer un **risque élevé** pour les droits et libertés des personnes concernées.
4. L'AIPD est **obligatoire** lorsque le traitement présente des **risques élevés**. Elle permet d'évaluer les risques et de mettre en place les mesures nécessaires pour atténuer ceux-ci.

France : Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Art. 62 *Modifié par l'ordonnance n° 2018-1125 du 12 décembre 2018*

« *Le responsable du traitement effectue préalablement à la mise en œuvre du traitement une analyse d'impact des opérations de traitement envisagées sur la protection des données à caractère personnel dans les conditions prévues à l'article 35 du règlement (UE) 2016/679 du 27 avril 2016.* »

Les objectifs assignés à l'AIPD

Différent d'une analyse de conformité classique (respect des obligations du RGPD)

On ne parle pas du risque pour l'organisme mais bien du **risque pour les droits et libertés des personnes.**

Schéma organisationnel à partir du besoin

Exemples de risques :

=> Fuite du fichier des signalements à la Direction des Ressources Humaines

- Risque de disparition des preuves et enquête compromise
- Risque de représailles physiques ou morales sur la personne auteur du signalement
- Risque de représailles physiques ou morales sur la victime si personne différente
- Atteinte à la vie professionnelle (et privée) de la victime (santé)
- Violation de la présomption d'innocence
- Atteinte à la réputation de la personne visée par le signalement

Comment déterminer la nécessité d'une analyse d'impact ?

En cas de doute :
Faire une AIPD

Mon traitement est-il sur la liste des cas pour lesquels une AIPD **n'est pas obligatoire ?**

NON il n'est pas sur la liste

OUI il est sur la liste

Mon traitement est-il sur la liste des cas pour lesquels une AIPD **est obligatoire ?**

Oui il est sur la liste

NON il n'est pas sur la liste

Combien des 9 critères sont remplis ?

Evaluation ou notation	Prise de décision automatique avec effet juridique ou effet similaire significatif	Surveillance systématique
Données sensibles ou données à caractère hautement personnel	Collecte de données à grande échelle	Croisement ou combinaison d'ensembles de données
Données concernant des personnes vulnérables	Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles	Traitements en eux-mêmes qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat

Au moins 2 critères ou bien je considère que mon traitement comporte un risque élevé

Aucun critère ou un seul critère est rempli

AIPD REQUISE

AIPD NON REQUISE

Les traitements pour lesquels une AIPD n'est pas requise doivent tout de même respecter les autres principes du RGPD

GRAND PARIS SEINE OUEST

Direction des Affaires Institutionnelles - Mars 2024

Liste des types d'opérations de traitement pour lesquelles une AIPD n'est pas requise 1/2

Article 35 § 10 du RGPD

Lien ICI

- Traitements, mis en œuvre uniquement à des fins de **ressources humaines** et dans les conditions prévues par les textes applicables, pour la seule gestion du personnel des organismes **qui emploient** moins de 250 personnes, à l'exception du recours au profilage
- Traitements de gestion de la relation **fournisseurs**.
- Traitements mis en œuvre dans les conditions prévues par les textes relatifs à la gestion du **fichier électoral** des communes.
- Traitements mis en œuvre aux seules fins de gestion des **contrôles d'accès physiques et des horaires** pour le calcul du temps de travail, en dehors de tout dispositif biométrique et A l'exclusion des traitements des données qui révèlent des données sensibles ou à caractère hautement personnel.
- Traitements mis en œuvre par une association, une fondation ou toute autre institution sans but lucratif pour la gestion de ses membres et de ses donateurs dans le cadre de ses activités habituelles dès lors que les données ne sont pas sensibles.
- Traitements de données de **santé** nécessaires à la prise en charge d'un patient par un professionnel de santé exerçant à titre individuel au sein d'un cabinet médical, d'une officine de pharmacie ou d'un laboratoire de biologie médicale.
- Traitements mis en œuvre par les **notaires** aux fins d'exercice de leur activité notariale et de rédaction des documents des offices notariaux.
- Traitements mis en œuvre par les **avocats** dans le cadre de l'exercice de leur profession à titre individuel.
- Traitements destinés à la gestion des activités des **comités d'entreprise et d'établissement**.

Liste des types d'opérations de traitement pour lesquelles une AIPD n'est pas requise 2/2

Article 35 § 10 du RGPD

- Traitements relatifs aux **éthylotests**, strictement encadrés par un texte et mis en œuvre dans le cadre d'activités de transport aux seules fins d'empêcher les conducteurs de conduire un véhicule sous l'influence de l'alcool ou de stupéfiants.
- Traitements mis en œuvre par les **greffiers des tribunaux de commerce** aux fins d'exercice de leur activité.
- Traitements mis en œuvre par les collectivités territoriales et les personnes morales de droit public et de droit privé aux fins de gérer les services en matière **d'affaires scolaires, périscolaires et de la petite enfance.**

- Cette exonération s'applique aux traitements relatifs à :
  - la préinscription, l'inscription, le suivi et la facturation des services en matière d'affaires scolaires, périscolaires, extrascolaires et de petite enfance (la scolarisation en école maternelle et élémentaire) ;
  - le recensement des enfants soumis à l'obligation scolaire ;
  - la restauration scolaire et extrascolaire ;
  - les transports scolaires ;
  - les accueils et activités périscolaires et extrascolaires ;
  - les accueils collectifs de mineurs ;
  - la participation à l'organisation matérielle et financière des sorties scolaires, les séjours scolaires courts et classes de découvertes dans le premier degré ;
  - l'accueil de la petite enfance au sein des établissements et services d'accueil des enfants de moins de six ans

Liste des types d'opérations de traitement pour lesquelles une AIPD est quoi qu'il en soit requise1/2

Article 35 § 3 du RGPD

Lien ICI

- Traitements de données de localisation à large échelle
  - Collecte de données sensibles
  - Données traitées à grande échelle
  - Surveillance systématique
  - Personnes dites « vulnérables »
  - Usage innovant ou application de nouvelles solutions technologiques
    - - Application mobile permettant de collecter les données de géolocalisation des utilisateurs ;
    - - fourniture d'un service de géolocalisation de mobilité urbaine utilisé par un grand nombre de personnes ;
    - - base de données « clients » des opérateurs de communication électronique ;
    - - mise en œuvre d'un système de billettique par des opérateurs de transport.
- Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médicosociaux pour la prise en charge des personnes.
- Traitements portant sur des données génétiques de personnes dites « vulnérables » (patients, employés, enfants, etc.).
- Traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines (par exemple par algorithme)
- Traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés

Liste des types d'opérations de traitement pour lesquelles une AIPD est, quoi qu'il en soit, requise 2/2

Article 35 § 3 du RGPD

- Traitements ayant pour finalité la gestion des alertes et des signalements en matière sociale et sanitaire
- Traitements ayant pour finalité la gestion des alertes et des signalements en matière professionnelle
- Traitements des données de santé nécessaires à la constitution d'un entrepôt de données ou d'un registre
- Traitements impliquant le profilage des personnes pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci
- Traitements mutualisés de manquements contractuels constatés, susceptibles d'aboutir à une décision d'exclusion ou de suspension du bénéfice d'un contrat
- Traitements de profilage faisant appel à des données provenant de sources externes
- Traitements de données biométriques aux fins d'identifier une personne physique de manière unique parmi lesquelles figurent des personnes dites « vulnérables » (élèves, personnes âgées, patients, demandeurs d'asile, etc.)
- Instruction des demandes et gestion des logements sociaux
- Traitements ayant pour finalité l'accompagnement social ou médico-social des personnes

Les 9 critères du Comité Européen de la Protection des données

- Le comité européen de la protection des données (ou CEPD), pour aider les organismes à déterminer si leur traitement est à risque ou non, s'appuie sur une liste de 9 critères.
- Si 2 des 9 critères sont remplis, le traitement doit faire l'objet d'une analyse d'impact.
- Chaque fois que l'on a un nouveau traitement qui est mis en œuvre, il faut passer au crible les 9 critères pour voir si on doit ou pas faire une analyse.
- Dans les lignes directrices du comité européen de protection des données, on a des orientations mais rien n'est défini de manière claire.

- => Dans certains cas, le responsable de traitement peut considérer que même si le traitement ne remplit aucun ou un seul de ces critères, une AIPD s'impose, dans la mesure où pour lui, ce traitement fait courir un risque élevé pour les personnes concernées par le traitement des données personnelles.

Les 9 critères du CEPD

Evaluation ou notation (Scoring y compris le profilage)	Prise de décision automatique avec effet juridique ou effet similaire significatif	Surveillance systématique
Données sensibles ou données à caractère hautement personnel	Collecte de données à grande échelle	Croisement ou combinaison d'ensembles de données
Données concernant des personnes vulnérables	Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles	Traitements en eux-mêmes qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat

Critère 1 : Evaluation / Scoring (y compris profilage)

EXEMPLE

- Attribution d'une subvention = évaluation, notation, qui ont des conséquences juridiques puisque amène à l'arbitrage de la décision d'attribution, le traitement peut empêcher la personne concernée d'exercer un droit ou de bénéficier d'un service ou d'un contrat donc AI.
- Les critères de notation ne doivent pas être complètement hors contexte par rapport à l'objectif final, ni un critère de notation utilisé d'une manière différente pour une personne plutôt qu'une autre). Recours possibles.
- Si on perd des données, la subvention ne sera peut-être pas attribuée, donc recours possibles.

EXEMPLE

Cibler des personnes de « tel âge » pour leur proposer de pouvoir bénéficier de telles préventions et de tels rendez-vous prévention…

- Attribution d'un marché public
- Evaluation d'une capacité de paiement

Critère 2 : Décision automatique avec effet légal ou similaire

- Le traitement conduit à une décision **automatisée, sans intervention humaine** avec effet légal sur la personne.
- Ou bien le traitement a pour objet d'aider à la décision de façon automatisée ayant un effet légal sur une personne ou qui l'affecte de manière significative.
- Par exemple, le traitement conduit à une discrimination ou à l'exclusion.

- Exemple : formulaire de recrutement avec « cases à cocher » sans validation par intervention humaine, qui conditionne le recrutement.

NB : Dès lors qu'il y a une décision prise à échelle humaine en bout de chaine, on ne parle pas de décision automatisée

Critère 3 : Surveillance systématique

- Ce n'est pas tant la nature de la collecte que son caractère **systématique** qui est visé ;
- « Surveillance systématique » = toute forme de suivi ou d'observation récurrente ou continue d'une personne ou d'un groupe de personnes. Exemple : géolocalisation, contrôle d'accès ou biométrie.
- Pour savoir si un traitement implique une surveillance « systématique », il faut prendre en compte plusieurs facteurs, tels que :
  - la fréquence, la durée ou la permanence de la surveillance ;
  - le nombre ou la catégorie de personnes concernées ;
  - la sensibilité ou la nature des données collectées ;
  - l'impact ou les conséquences potentielles de la surveillance pour les personnes concernées ;
  - l'utilisation de technologies innovantes ou intrusives ;
  - le croisement ou la combinaison de données provenant de sources diverses.

Critère 4 : Collecte de données à grande (ou large) échelle

- Il n'existe pas de définition de ce qu'est la « grande échelle ».

- Pour déterminer si le traitement est effectué à grande échelle, doivent être pris en compte les facteurs suivants :
  - **le nombre de personnes concernées,**
  - **le volume de données et/ou l'éventail des différents éléments de données traitées,**
  - **la durée ou la permanence de l'activité de traitement de données**
  - **et l'étendue géographique de l'activité de traitement ;**

- **ATTENTION** : Si le traitement implique une surveillance systématique « **à grande échelle** » d'une zone accessible au public, il faut obligatoirement réaliser une AIPD sans attendre les 2 critères.

Critère 5 : Croisement ou combinaison d'ensembles de données

- Ce critère s'applique lorsque le traitement implique le croisement, le recoupement, la combinaison de plusieurs jeux de données provenant de différentes sources, bases de données, ou traitements qui ne sont pas liés entre eux ou qui n'ont pas été initialement collectés à des fins compatibles.

= sources de données qui sont distinctes que l'on associe pour dégager une autre donnée.

- **EXEMPLE :** utiliser le traitement d'une autre direction pour élaborer un autre traitement pour ma direction. Ou bien 2 traitements différents pour en faire un 3ème.

Critère 6 :Traitement ayant comme cible des « personnes vulnérables »

- « personne vulnérable » = **par rapport aux responsables de traitement** (exemple : un patient par rapport au médecin), les mineurs, les personnes âgées, les personnes en situation de handicap où les personnes sous tutelle.
- Il s'agit des personnes vulnérables « **par nature** » (personnes âgées, enfants…) ou en fonction de leur **situation** (agents sous subordination, patients …)

- La personne n'est pas forcément en capacité ou n'a pas autorité pour donner son **consentement** sur les décisions qui peuvent être prises ou sur le traitement de ses données (déséquilibre dans la relation). Pas de capacité ou de maturité suffisante pour prendre une décision = posture d'infériorité ou pourront difficilement agir.
- **EXEMPLE :** personnes qui sont en situation sociale délicate pour un CCAS, les mineurs, dans les conservatoires etc…

=> La question : la personne cible est-elle en capacité de se protéger ?

Critère 7 : Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles

- Le RGPD indique clairement que l'utilisation d'une nouvelle technologie, définie en « conformité avec l'état des connaissances technologiques » peut déclencher la nécessité d'une AIPD.

- Pourquoi ?

=> l'utilisation de la technologie en question peut impliquer de nouvelles formes de collecte et d'utilisation des données, présentant potentiellement un risque élevé pour les droits et libertés des personnes ;

Critère 8 : Traitements qui en eux-mêmes, empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat

- Notamment les opérations visant à **autoriser**, **modifier** ou **refuser** l'accès à un droit, à service ou la conclusion d'un contrat

- EXEMPLE : Tout ce qui est subventions

Critère 9 : Données sensibles ou données à caractère hautement personnel

- Eléments de patrimoine, éléments de santé, salaire / traitement, données relatives aux mineurs…

- Le traitement des données à caractère personnel de l'article 9 du RGPD qui révèle :
  - l'origine raciale ou ethnique,
  - les opinions politiques,
  - les convictions religieuses ou philosophiques ou l'appartenance syndicale,
  - le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique,
  - des données concernant la santé,
  - des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Rappel sur les données sensibles ou données à caractère hautement personnel

Pour rappel, le traitement de ces données est interdit sauf si :

- Consentement de la personne,
- Traitement obligatoire aux fins d'exécution des obligations ou l'exercice des droits propres au responsable de traitement ou à la personne concernée,
- Sauvegarde des intérêts vitaux de la personne,
- Activités légitimes et garanties ayant cette finalité,
- Données manifestement rendues publiques,
- Défense ou justice,
- Intérêt public important,
- Médecine, sanitaire et social, santé publique,
- Archives et recherche.

Risques redoutés

Disponibilité de la donnée

- Disparition des données à caractère personnel
- Dysfonctionnement de l'accès aux données
- Etc…

Ex : Site devenu non fonctionnel

Confidentialité de la donnée

- Accès illégitime aux données à caractère personnel
- Avec stockage ou non, rediffusion, corrélation, exploitation, déploiement
- Etc …

Ex : Vente pour hameçonnage

Intégrité de la donnée

- Modification non désirée des données à caractère personnel
- Avec dysfonctionnement, exploitation
- Etc …

Ex : Changements de RIB

Source du risque

Des sources humaines internes

- Agents, stagiaires …

Des sources humaines externes

- Anciens agents, destinataires des données, délinquants, sous-traitants, tiers autorisés, visiteurs, organisations criminelles, pirates informatiques, terroristes …

Des sources non humaines

- Catastrophes naturelles, épidémie, codes malveillants, Matière inflammable, corrosive ou explosive …

GRAND PARIS SEINE OUEST

= ⚠ **MENACE (s)**

ANALYSE DE LA GRAVITE DU RISQUE

1

Ici, on se pose la question de l'ampleur du risque et de la difficulté qu'aura la personne à supprimer voire amoindrir le désagrément subi.

Risque négligeable	Risque limité	Risque important	Risque maximal
Pas ou peu d'impact(s) sur les personnes	Impacts significatifs	Impacts significatifs	Conséquences significatives voire irrémédiables
Désagréments surmontables	Désagréments surmontables	Difficultés réelles pour les stopper	Ne pouvant pas être surmontées.

ANALYSE DE LA VRAISSEMBLANCE DU RISQUE

2

Ici on s'interroge sur la probabilité que le risque se réalise

Probabilité négligeable	Probabilité limitée	Probabilité importante	Probabilité maximale
Réalisation du risque semble impossible ou quasiment impossible	Réalisation du risque semble difficilement concevable	La menace de réalisation du risque existe	La réalisation du risque est quasiment inévitable

Exemples de risques sur la personne et sur les données

Accès illégitime aux données personnelles

Vol d'identité, pertes financières, atteinte à la réputation, fraude, phishing, chantage, perte d'un avantage, menace

Atteinte à l'intégrité des données (modification des données)

Vol d'identité, pertes financières, atteinte à la réputation, fraude, phishing, chantage, perte d'un avantage, menace

Disparition des données

- Perte d'un avantage
- Perte de données
- Inaccessibilité du service souscrit
- Inaccessibilité de l'application
- Atteinte à la réputation EPT
- Destruction du SI

Les acteurs de la rédaction de l'analyse d'impact

Responsable du traitement au sein de la direction opérationnelle concernée

C'est lui qui aura les connaissances techniques,

C'est aussi lui qui aura ensuite pour rôle de sensibiliser ses équipes ou directions partenaires.

Le sous-traitant

Si pour le traitement, le responsable de traitement a fait appel à un sous-traitant, celui-ci a l'obligation d'intervenir sur l'aspect technique. Il peut potentiellement être responsable si la faille vient du produit utilisé (exemple : logiciel)

A insérer dans les clauses du marché public car sinon certains sous traitants facturent ce service.

La Direction des systèmes d'information (DSI)

C'est elle qui aura les connaissances techniques relatives à la protection des risques au niveau informatique.

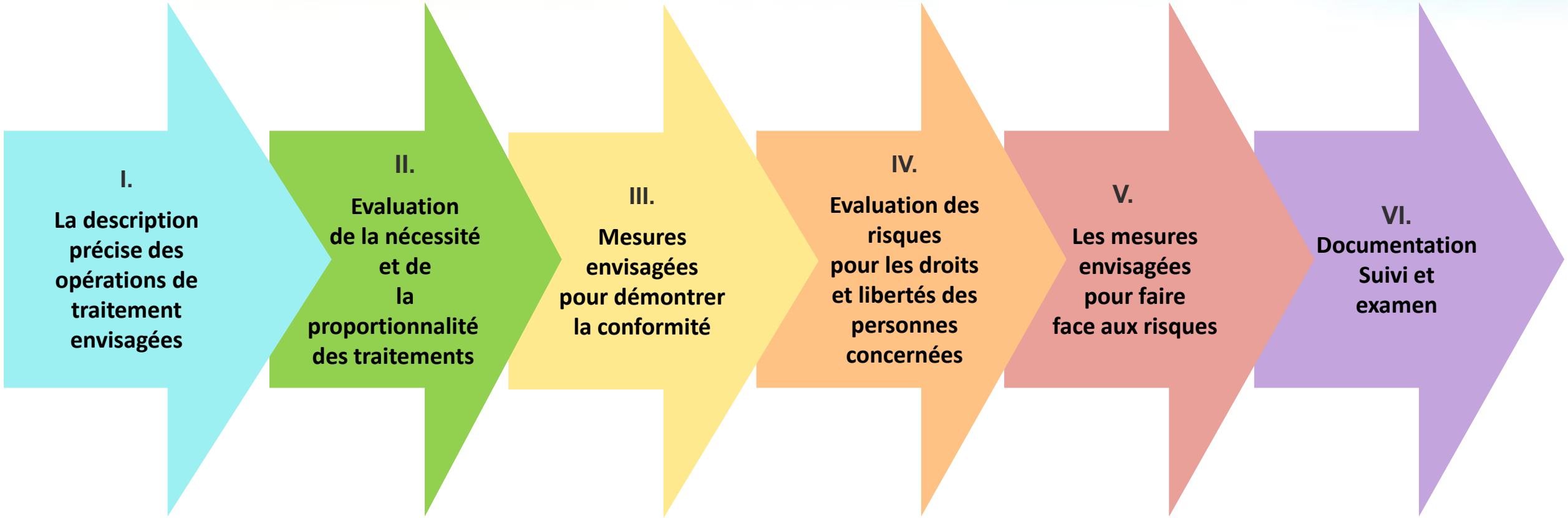
Idem sur la connaissance de technologies innovantes.

Le DPO

C'est le DPO qui va centraliser les analyses d'impact pour les remettre à la CNIL ou pour procéder à la déclaration en cas de réalisation du risque.

Le DPO peut demander l'intervention d'un expert ou d'un avocat s'il considère que le risque est extrêmement sensible.

Ce que doit comporter le rapport d'analyse d'impact :



I. Description des opérations de traitement envisagées

PRESENTATION GENERALE

- Présentation du traitement
- Présentation des finalités,
- Présentation des enjeux,
- Identification des acteurs

PRESENTATION DETAILLEE

- Délimitation et description du périmètre de manière détaillée
- Description des processus et des supports de données à caractère personnel pour l'ensemble du cycle de vie des données (de la collecte jusqu'à leur effacement)

II. Evaluation de la nécessité et de la proportionnalité

=> Pour être conforme aux principes de protection de la vie privée, un traitement de données doit avoir :

- Une finalité déterminée, explicite et légitime, (Présentation du traitement, des finalités, des enjeux, identification des acteurs),
- Des mesures de minimisation et une délimitation du sujet doivent avoir été mis en place,
- La qualité de préservation des données doit être assurée,
- Les données ne sont conservées que pour une durée strictement nécessaire,
- Les personnes concernées sont informées de leurs droits : ils disposent d'un droit d'opposition, d'un droit d'accès à tout moment, d'un droit de rectification et d'effacement, d'un droit à la portabilité, d'un droit à la limitation, d'un droit au transfert de leurs données). = Vérification de l'existence du droit, et des modalités de mises en place de ces droits.
- Les données sont récoltées en vertu d'un fondement légal justifiant le traitement ou bien avec le consentement des personnes.

III. Evaluation des risques

Définition des sources du risque

Evaluation des principales menaces pouvant aboutir à la réalisation du risque

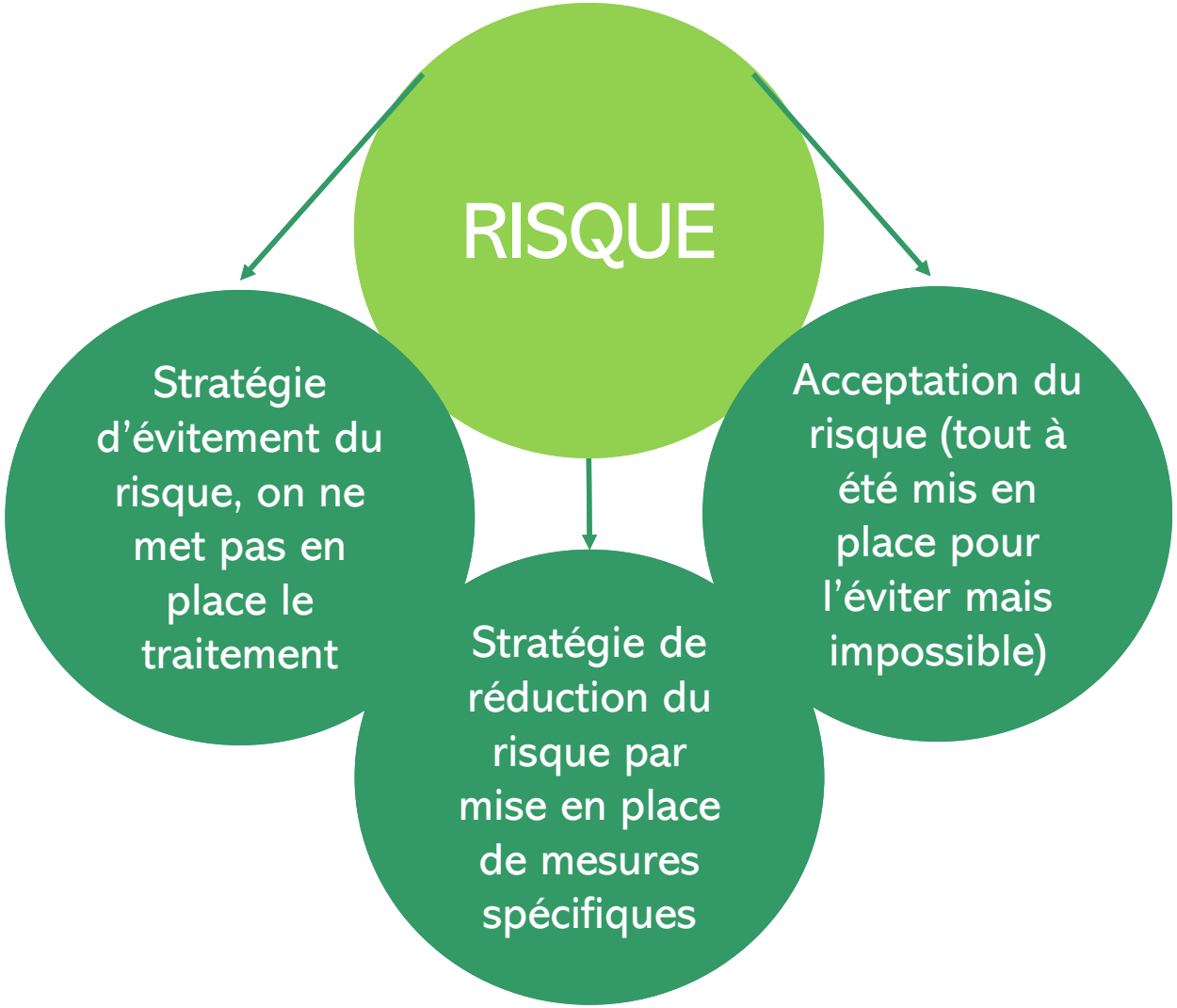
Définition et estimation de la gravité

Evaluation de la vraisemblance du risque et de sa réalisation ?

Evaluation des mesures mises en place pour traiter le potentiel risque

Evaluation des impacts sur les personnes concernées en cas de réalisation du risque

IV. Traitement du risque : 3 solutions



V. Description des mesures envisagées pour faire face au risque

Mesures juridiques :

- Consentement recueilli quand cela est possible,

- Définition des durées de conservation des données

Mesures de sécurité physique :

- Mise en place de contrôles d'accès physique sécurité des matériels, protection contre les sources de risques non humains

(sécurité incendie, locaux sécurisés, etc…)

Mesures de sécurité logique :

Anonymisation, chiffrement, sauvegardes, cloisonnement des données, contrôle d'accès logique,

(bien cloisonner les partages de données entre les services)

Mesures organisationnelles :

- Groupes de travail réflexion risques
- Etc…

VI . L'analyse d'impact est-elle « acceptable » ? (en amont de la décision de mise en place du traitement).

L'analyse d'impact est acceptable selon le DPO	L'analyse d'impact n'est pas acceptable en l'état selon le DPO	L'analyse d'impact est acceptable sous condition selon le DPO
↓	↓	↓
Validation	Détermination du plan d'action pour rendre l'analyse acceptable au regard des risques encore trop élevés et des objectifs ou bien refus du traitement.	On considère que l'analyse est acceptable sous condition que certaines mesures soient prises.

Faut-il transmettre son AIPD à la CNIL ?

Si le traitement relève du RGPD, l'AIPD doit être transmise à la CNIL dans les cas suivants :

• S'il apparait que le niveau de risque résiduel reste élevé (cas où la CNIL doit être consultée). Par exemple en cas de conséquentes importantes ou irréversibles pour la personne concernée, qui ne peuvent être dépassés ou lorsqu'il est évident que le risque va se réaliser ;
• Quand la législation nationale d'un État membre (dont la France) l'exige ;
• A la demande de la CNIL

Si le traitement relève de la directive « Police-Justice », l'AIPD doit être transmise à la CNIL dans les cas suivants :
• Elle présente des risques résiduels élevés ;
• En raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, le traitement présente des risques initiaux élevés.

Retours de la CNIL

Si la CNIL considère que le traitement ne constitue pas une violation du RGPD, le traitement peut être mis en œuvre.

Si la CNIL considère que le traitement constitue une violation du RGPD, un avis écrit est adressé au responsable de traitement.

- Soit tout recommencer
- Soit abandonner le traitement

La CNIL a alors un pouvoir d'enquête et de sanction.