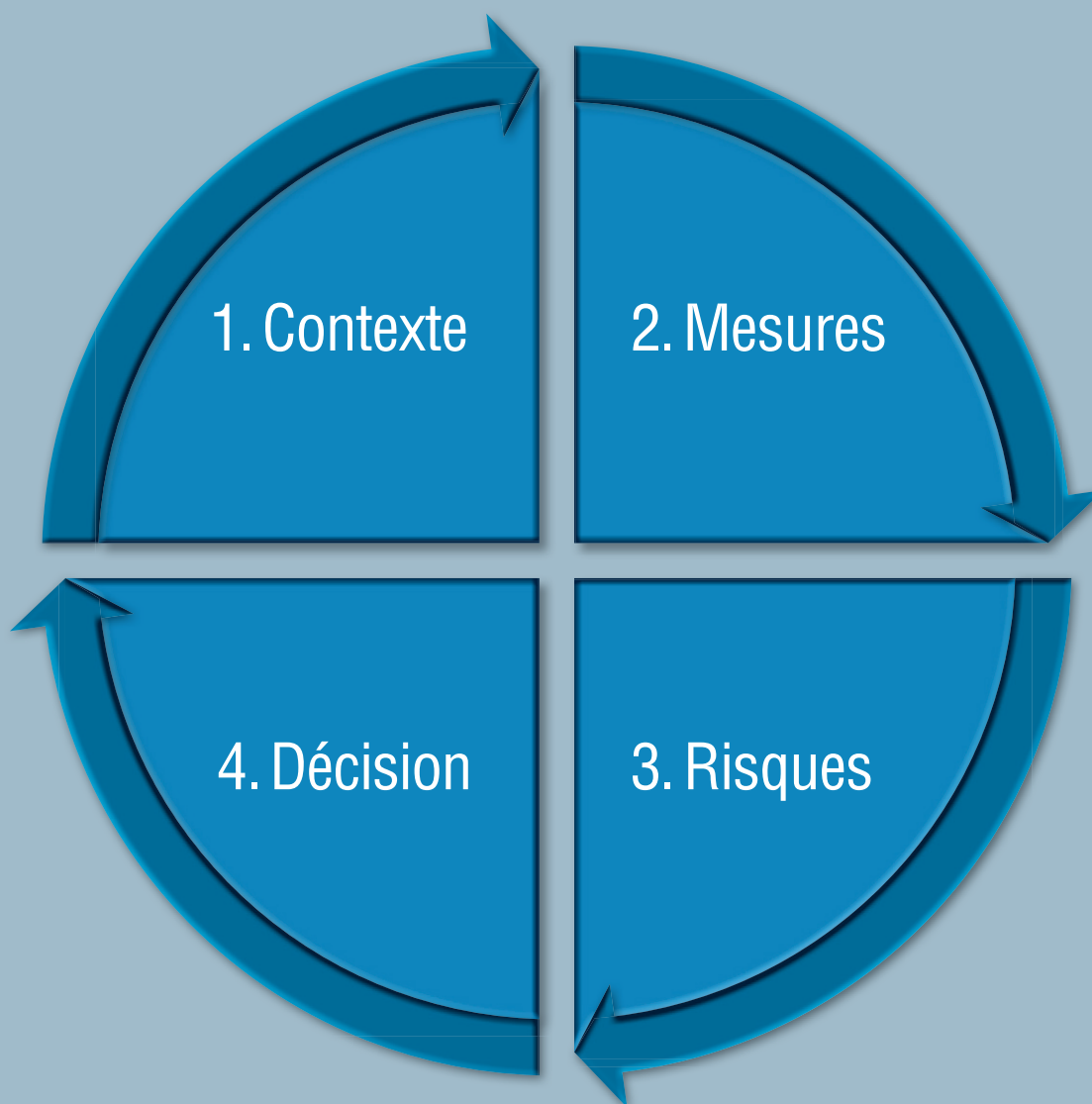


ÉTUDE D'IMPACT SUR LA VIE PRIVÉE (EIVP)

PRIVACY IMPACT
ASSESSMENT (PIA)

Comment mener une EIVP, un PIA



Sommaire

| | |
|---|-----------|
| AVANT PROPOS | 3 |
| INTRODUCTION | 4 |
| DOMAINE D'APPLICATION | 4 |
| POURQUOI MENER UN PIA ?..... | 5 |
| QU'EST-CE QU'UN RISQUE SUR LA VIE PRIVEE ? | 6 |
| COMMENT MENER UN PIA ?..... | 7 |
| QUI PARTICIPE AU PIA ?..... | 9 |
| QU'EST-CE QUE LE RAPPORT DE PIA ?..... | 10 |
| 1. CONTEXTE : LE PERIMETRE DU PIA..... | 11 |
| 1.1. LA DESCRIPTION GENERALE | 11 |
| 1.2. LA DESCRIPTION DETAILLEE | 11 |
| 2. MESURES : LE DISPOSITIF DE CONFORMITE | 12 |
| 2.1. LES MESURES DE NATURE JURIDIQUE (OBLIGATOIRES)..... | 12 |
| 2.2. LES MESURES DESTINEES A TRAITER LES RISQUES..... | 13 |
| 3. RISQUES : LES ATTEINTES POTENTIELLES A LA VIE PRIVEE..... | 14 |
| 3.1. LES SOURCES DE RISQUES..... | 14 |
| 3.2. LES EVENEMENTS REDOUTES | 14 |
| 3.3. LES MENACES..... | 15 |
| 3.4. LES RISQUES..... | 15 |
| 4. DECISION : LA VALIDATION DU PIA | 16 |
| 4.1. L'EVALUATION DU PIA..... | 16 |
| 4.2. CAS 1 – LE PIA N'EST PAS ENCORE JUGE ACCEPTABLE : OBJECTIFS | 16 |
| 4.3. CAS 2 – LE PIA EST JUGE ACCEPTABLE : PLAN D'ACTION | 16 |
| 4.4. CAS 2 – LE PIA EST JUGE ACCEPTABLE : LA VALIDATION FORMELLE | 16 |
| ANNEXE - REFERENCES UTILISEES..... | 17 |
| ACRONYMES | 17 |
| DEFINITIONS | 17 |
| REFERENCES BIBLIOGRAPHIQUES | 19 |

Avant propos

Ce document doit être utilisé conjointement avec les guides suivants :

- [\[PIA-2-Outillage\]](#), qui comprend des modèles et des bases de connaissances pour appliquer concrètement cette méthode ;
- [\[PIA-3-BonnesPratiques\]](#), qui constitue un catalogue de mesures, destinées à respecter les exigences légales et à traiter les risques appréciés avec cette méthode.

Conventions d'écriture pour l'ensemble de ces documents :

- le terme « vie privée » est employé comme raccourci pour évoquer l'ensemble des droits et libertés fondamentaux (notamment ceux évoqués par les articles 7 et 8 de la [\[CharteUE\]](#), l'article 1 de la [\[Directive-95-46\]](#) et l'article 1 de la [\[Loi-I&L\]](#) : « vie privée, identité humaine, droits de l'homme et libertés individuelles ou publiques ») ;
- l'acronyme « PIA » est utilisé pour désigner indifféremment *Privacy Impact Assessment* étude d'impact sur la vie privée (EIVP), *Data Protection Impact Assessment* (DPIA) et étude d'impact sur la protection des données ;
- les libellés entre crochets ([libellé]) correspondent aux références bibliographiques.

Introduction

Un PIA repose sur deux piliers :

- 1. les principes et droits fondamentaux**, « non négociables », qui sont fixés par la loi et doivent être respectés et ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
- 2. la gestion des risques sur la vie privée des personnes concernées**, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les DCP.

Domaine d'application

Ce document explique comment mener des PIA. Il décrit la manière d'employer la méthode [\[EBIOS\]](#)¹ dans le contexte spécifique « Informatique et libertés ».

Il s'adresse aux responsables de traitements qui souhaitent justifier de leur démarche de conformité et des mesures qu'ils ont choisies (notion d'*Accountability* en anglais), ainsi qu'aux fournisseurs de produits qui souhaitent montrer que leurs solutions ne portent pas atteinte à la vie privée dans une logique de conception respectueuse de la vie privée (notion de *Privacy by Design* en anglais)². Il est utile à toutes les parties prenantes dans la création ou l'amélioration de traitements de DCP ou de produits :

- ❑ les autorités décisionnaires, qui commanditent et valident la création de nouveaux traitements de DCP ou produits ;
- ❑ les maîtrises d'ouvrage (MOA), qui doivent apprécier les risques pesant sur leur système et donner des objectifs de sécurité ;
- ❑ les maîtrises d'œuvre (MOE), qui doivent proposer des solutions pour traiter les risques conformément aux objectifs identifiés par les MOA ;
- ❑ les correspondants « informatique et libertés » (CIL), qui doivent accompagner les MOA dans la protection des DCP et les autorités décisionnaires ;
- ❑ les responsables de la sécurité des systèmes d'information (RSSI), qui doivent accompagner les MOA dans le domaine de la sécurité des systèmes d'information (SSI).

¹ EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité – est la méthode de gestion des risques publiée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

² Dans la suite du document, le terme « traitement de DCP » est interchangeable avec le terme « produit ».

Pourquoi mener un PIA ?

Un PIA peut être mené sur tout traitement de DCP ou produit complexe, novateur, dont les enjeux sont importants. Il peut également y avoir une obligation légale de mener un PIA.

Les DCP peuvent avoir une valeur pour l'organisme qui les traite, mais leur traitement engendre également *de facto* une importante responsabilité du fait des risques qu'il fait encourir sur la vie privée des personnes concernées.

Elles ont également une valeur pour les personnes concernées. Si elles peuvent leur être utiles à réaliser des démarches administratives ou commerciales, ou contribuer à leur image, une atteinte à leur sécurité peut leur causer des préjudices corporels, matériels ou moraux.

Elles ont enfin une valeur pour autrui. Il peut notamment s'agir d'une valeur marchande dans le cas où elles sont exploitées à des fins commerciales (*spam*, publicité ciblée...), ou bien d'une valeur de nuisance dans le cas d'actions injustes (discrimination, refus de prestations...) ou malveillantes (transaction bancaire frauduleuse, usurpation, chantage à la destruction de données, cambriolage, diffamation, menaces, agression...).

Par ailleurs, on constate des phénomènes qui concourent à modifier notre vision des menaces : une culture consistant à exposer sa vie privée sans se soucier des impacts que cela pourra avoir sur son avenir professionnel et social et un renforcement des capacités des sources de risques (génération Y, structuration des organisations criminelles, outillage puissant facile à trouver sur Internet, espionnage entre États...). Les DCP sont donc d'autant plus exposées.

Étant donnés les enjeux souvent élevés, l'évolution des systèmes³ et des menaces, la gestion des risques permet de déterminer les mesures nécessaires et suffisantes. Elle permet en effet d'étudier méthodiquement les traitements de DCP ou les produits, de hiérarchiser les risques et de les traiter de manière proportionnée pour optimiser les coûts et prendre des décisions sur la base d'éléments rendus les plus objectifs possibles.

Enfin, un PIA contribue à démontrer la mise en œuvre des principes de protection de la vie privée afin que les personnes concernées gardent la maîtrise de leurs DCP.

³ Informatiques, de téléphonie, canaux papiers, organisationnels ou interpersonnels.

Qu'est-ce qu'un risque sur la vie privée ?

Un risque est un scénario hypothétique qui décrit :

- ❑ comment des sources de risques (ex. : un salarié soudoyé par un concurrent)
- ❑ pourraient exploiter les vulnérabilités des supports de DCP (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 aux DCP)
- ❑ sur les DCP (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...).

Le schéma suivant synthétise l'ensemble des notions présentées :

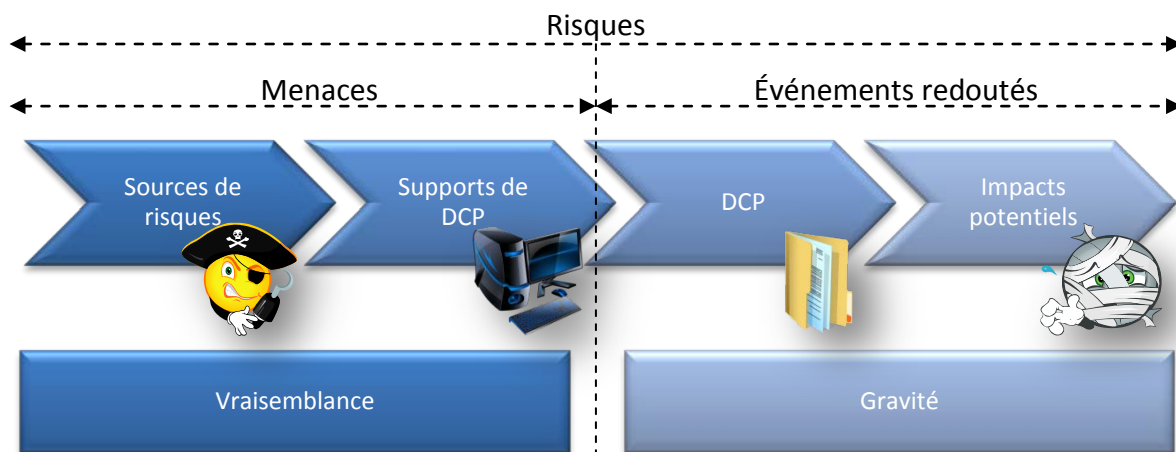


Figure 1 – Éléments composant les risques

Le niveau d'un risque est estimé en termes de gravité et de vraisemblance :

- ❑ la **gravité** représente l'ampleur d'un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels⁴ ;
- ❑ la **vraisemblance** traduit la possibilité qu'un risque se réalise. Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter.

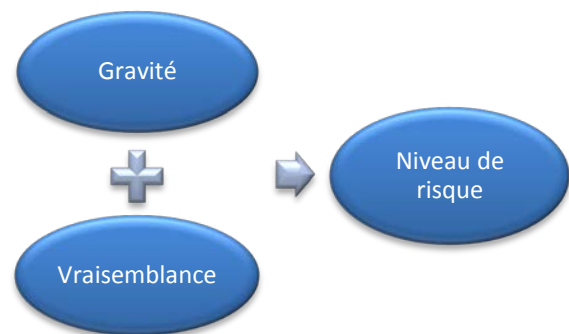


Figure 2 – Éléments permettant d'estimer les risques

⁴ Compte tenu du contexte du traitement (nature des données, personnes concernées, finalité du traitement...).

Comment mener un PIA ?

La démarche de conformité mise en œuvre en menant un PIA repose sur le respect des principes de protection de la vie privée :

- le respect des principes juridiques en matière de protection de la vie privée (finalité déterminée, explicite et légitime ; données adéquates, pertinentes et non excessives ; information claire et complète des personnes ; durée de conservation limitée ; droit d'opposition, d'accès, de rectification et suppression...), pour déterminer et justifier la pertinence des mesures destinées à satisfaire ces exigences ;
- la gestion des risques liés à la sécurité des DCP et ayant un impact sur la vie privée des personnes concernées, afin de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès » (article 34 de la [\[Loi-I&L\]](#)⁵).



Figure 3 – La démarche de conformité à l'aide d'un PIA

En synthèse, pour se conformer à la [\[Loi-I&L\]](#)⁶, il convient de :

1. délimiter et décrire le **contexte** du(des) traitement(s) considéré(s) et ses enjeux ;
2. identifier les **mesures** existantes ou prévues (pour respecter les exigences légales et traiter les risques sur la vie privée de manière proportionnée) ;
3. apprécier les **risques** sur la vie privée pour vérifier qu'ils sont convenablement traités ;
4. prendre la **décision** de valider la manière dont il est prévu de respecter les principes de protection de la vie privée et de traiter les risques, ou bien réviser les étapes précédentes.

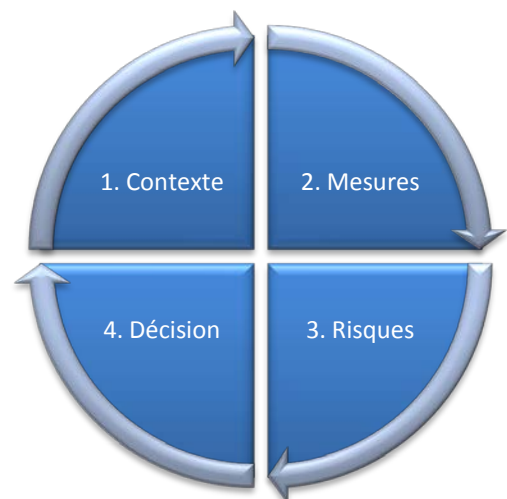


Figure 4 – Démarche générale pour mener un PIA

Il s'agit d'un processus d'amélioration continue. Il requiert donc parfois plusieurs itérations pour parvenir à un dispositif de protection de la vie privée acceptable. Il requiert en outre une surveillance des évolutions dans le temps (du contexte, des mesures, des risques...), par exemple tous les ans, et des mises à jour dès qu'une évolution significative a lieu.

⁵ Et article 17 de la [\[Directive-95-46\]](#).

⁶ Et à la [\[Directive-95-46\]](#).

Le schéma suivant présente la démarche détaillée :

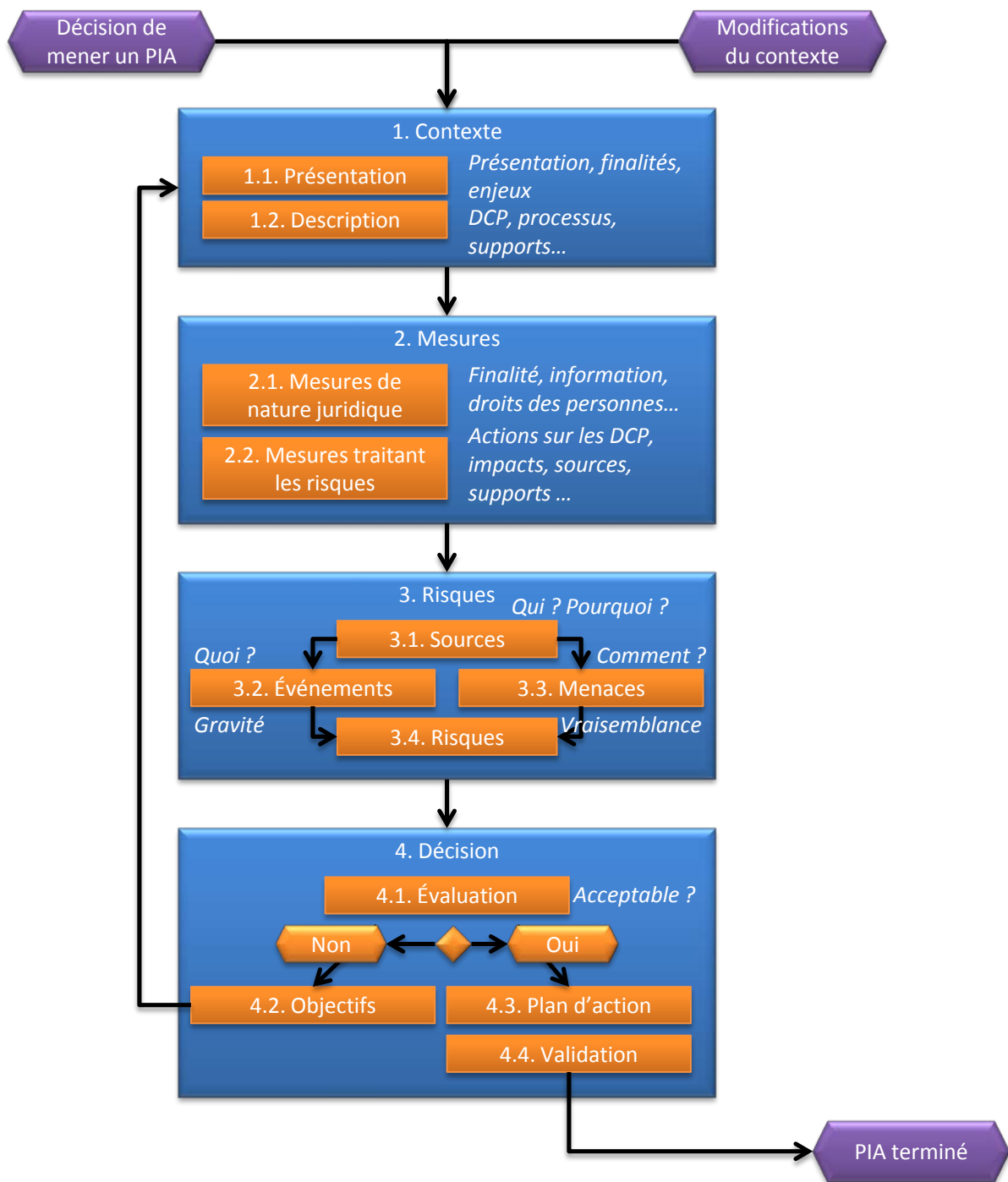


Figure 5 – D marche d taill e pour mener un PIA

La d marche devrait  tre employ e d s la conception d'un nouveau traitement de DCP. En effet, une application en amont permet de d terminer les mesures n cessaires et suffisantes, et donc d'optimiser les co ts. A contrario, une application tardive, alors que le syst me est d j  cr e et les mesures en place, peut remettre en question les choix effectu s.

Qui participe au PIA ?

D'une manière générale, un PIA est mené par un responsable de traitement ou un fournisseur de produit.

Un PIA requiert la participation de plusieurs parties prenantes du responsable de traitement⁷, avec des rôles et responsabilités différents selon les étapes :

| Étapes de la méthode | Responsable | Maîtrise d'ouvrage ⁸ | Maîtrise d'œuvre ⁹ | CIL ¹⁰ | RSSI ¹¹ |
|-----------------------------------|------------------------|---------------------------------|-------------------------------|-----------------------|--------------------|
| 1.1. Description générale | Approuve ¹² | Consultée ¹³ | Informée ¹⁴ | Réalise ¹⁵ | Informé |
| 1.2. Description détaillée | Approuve | Consultée | Informée | Réalise | Informé |
| 2.1. Mesures de nature juridique | Approuve | Consultée | Consultée | Réalise | Informé |
| 2.2. Mesures traitant les risques | Approuve | Consultée | Consultée | Informé | Réalise |
| 3.1. Sources de risques | Approuve | Consultée | Informée | Informé | Réalise |
| 3.2. Événements redoutés | Approuve | Consultée | Informée | Réalise | Consulté |
| 3.3. Menaces | Approuve | Informée | Consultée | Informé | Réalise |
| 3.4. Risques | Approuve | Informée | Informée | Réalise | Consulté |
| 4.1. Évaluation | Approuve | Informée | Informée | Réalise | Consulté |
| 4.2. Objectifs | Approuve | Consultée | Consultée | Réalise | Informé |
| 4.3. Plan d'action | Approuve | Réalise | Consultée | Informé | Informé |
| 4.4. Validation formelle | Réalise | Informée | Informée | Consultée | Informé |

Ces responsabilités peuvent être adaptées à chaque contexte particulier. Elles doivent notamment être adaptées aux processus de l'organisme, tels que la gestion de projet. En outre, des personnes extérieures à l'organisme peuvent devoir être impliquées ou informées.

⁷ Le PIA peut également être mené par un sous-traitant qui agit sous la responsabilité du responsable de traitement.

⁸ Il s'agit des métiers. Elle peut être déléguée, représentée ou sous-traitée.

⁹ Elle peut également être déléguée, représentée ou sous-traitée.

¹⁰ Ou la personne en charge des aspects « Informatique et libertés ».

¹¹ Responsable de la sécurité des systèmes d'information ou personne en charge des aspects « Sécurité ».

¹² Personne légitime pour approuver l'action.

¹³ Personne(s) consultée(s) pour obtenir les informations utiles à l'action.

¹⁴ Personne(s) informée(s) des résultats de l'action.

¹⁵ Personne(s) responsable(s) de la mise en œuvre de l'action.

Qu'est-ce que le rapport de PIA ?

Le rapport de PIA est le document à produire quand un PIA est mené. Il devrait au minimum comporter les parties suivantes :

Rapport de PIA

Introduction

- Présentation du(des) traitement(s) considéré(s)

Corps du PIA

- Description du périmètre
- Liste des mesures de nature juridique
- Liste des mesures destinées à traiter les risques
- Cartographie des risques

Conclusion

- Décision argumentée de validation du PIA

Annexes

- Description détaillée du périmètre
- Présentation détaillée des mesures
- Description détaillée des risques
- Plan d'action

Il doit être rendu accessible¹⁶ aux autorités de protection des données¹⁷.

Il est également parfois utile de publier et/ou de diffuser tout ou partie du rapport de PIA¹⁸.


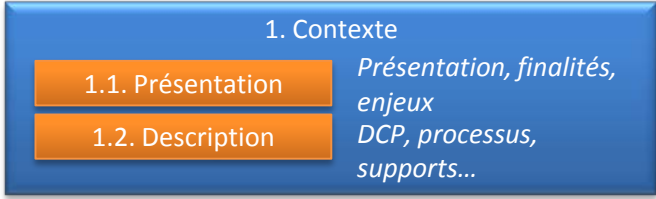
¹⁶ Il n'a pas à être systématiquement envoyé, mais doit être tenu à disposition des autorités qui le demanderaient.

¹⁷ En France, la CNIL.

¹⁸ Par exemple, si des obligations réglementaires l'imposent, s'il est requis en tant qu'élément d'*accountability*, ou si cela est jugé opportun pour des raisons d'image.

1. Contexte : le périmètre du PIA

🕒 Objectif : obtenir une vision claire du(des) traitement(s) de DCP considéré(s).

| Étape | Description | Rapport |
|---|--|--|
|  |  <p>1. Contexte</p> <p>1.1. Présentation <i>Présentation, finalités, enjeux</i></p> <p>1.2. Description <i>DCP, processus, supports...</i></p> | <input type="checkbox"/> Présentation du(des) traitement(s) considéré(s) <input type="checkbox"/> Description du périmètre <input type="checkbox"/> Description détaillée du périmètre |

1.1. La description générale

- Présenter le **traitement** considéré, ses **finalités** et ses **enjeux**¹⁹ de manière synthétique.
- Identifier le **responsable du traitement** et les **sous-traitants**.

1.2. La description détaillée

- Délimiter et décrire le périmètre de manière détaillée :
 - les **DCP** concernées, leurs **destinataires** et **durées de conservation** ;
 - une description des **processus** et des **supports** de DCP pour l'ensemble du cycle de vie des DCP (depuis leur collecte jusqu'à leur effacement).

Conseils pour réaliser les actions


- Il est possible d'étudier plusieurs traitements dans la même étude.
- Il est généralement utile de considérer et de distinguer les DCP :
 - celles directement liées au traitement ;
 - celles nécessaires à la mise en œuvre des mesures²⁰.
- Cette étape devrait être révisée à chaque changement de contexte.

¹⁹ Répondre à la question « Quels sont les bénéfices attendus (pour l'organisme, pour les personnes concernées, pour la société en général...) ? ».

²⁰ Mesures mises en œuvre pour respecter les exigences légales (information des personnes, consentement, droits d'opposition, d'accès, de rectification et de suppression) et pour traiter les risques (notamment les mesures de gestion d'identité, de contrôle d'accès, et de journalisation).

2. Mesures : le dispositif de conformité

🕒 **Objectif** : bâtir le dispositif de conformité aux principes de protection de la vie privée.

| Étape | Description | Rapport |
|---|---|---|
|  | <div style="background-color: #4a86e8; color: white; padding: 5px; text-align: center;">2. Mesures</div> <div style="background-color: #f79646; padding: 5px; margin-bottom: 5px;">2.1. Mesures de nature juridique</div> <div style="background-color: #f79646; padding: 5px;">2.2. Mesures traitant les risques</div> | <ul style="list-style-type: none"> ❑ Liste des mesures retenues ❑ Description détaillée des mesures |

Conseils pour réaliser les actions

- ❑ Les mesures peuvent être conçues de toute pièce, ou bien issues de bonnes pratiques diffusées par des institutions reconnues et adaptées au contexte spécifique.
- ❑ Les éventuels incidents qui auraient déjà eu lieu, ainsi que les difficultés rencontrées pour mettre en œuvre certaines mesures, peuvent servir à améliorer le dispositif.
- ❑ Pour améliorer la fiabilité des mesures, il est utile de déterminer les actions prévues en cas d'ineffectivité de ces mesures (si elles ne fonctionnent plus).
- ❑ Cette étape est révisée tant que le respect des exigences légales ou le traitement des risques est insuffisant.

2.1. Les mesures de nature juridique (obligatoires)

- ❑ Identifier ou déterminer les **mesures retenues** (existantes ou prévues) **pour respecter les exigences légales** suivantes (nécessitant d'expliquer comment il est prévu de les mettre en œuvre) :
 1. **finalité** : finalité déterminée, explicite et légitime²¹ ;
 2. **minimisation** : réduction des données à celles strictement nécessaires²² ;
 3. **qualité** : préservation de la qualité des données à caractère personnel²³ ;
 4. **durées de conservation** : durée nécessaire à l'accomplissement des finalités, à défaut d'une autre obligation légale imposant une conservation plus longue²⁴ ;
 5. **information** : respect du droit à l'information des personnes concernées²⁵ ;
 6. **consentement** : obtention du consentement des personnes concernées ou existence d'un autre fondement légal justifiant le traitement²⁶ ;

²¹ « Elles sont collectées pour des finalités déterminées, explicites et légitimes » (article 6 de la [\[Loi-I&L\]](#) et de la [\[Directive-95-46\]](#)).

²² « Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs » (article 6 de la [\[Loi-I&L\]](#) et de la [\[Directive-95-46\]](#)).

²³ « Elles sont exactes, complètes et, si nécessaire, mises à jour » (article 6 de la [\[Loi-I&L\]](#) et de la [\[Directive-95-46\]](#)).

L'exigence de qualité porte également sur le lien entre les données qui identifient les personnes et les données qui les concernent.

²⁴ « Elles sont conservées [...] pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées » (voir article 6 de la [\[Loi-I&L\]](#) et de la [\[Directive-95-46\]](#)), à défaut d'une autre obligation légale imposant une conservation plus longue.

²⁵ Voir article 32 de la [\[Loi-I&L\]](#) et articles 10 et 11 de la [\[Directive-95-46\]](#).

²⁶ S'il y a lieu, voir article 7 de la [\[Loi-I&L\]](#).

7. **droit d'opposition** : respect du droit d'opposition des personnes concernées²⁷ ;
8. **droit d'accès** : respect du droit des personnes concernées d'accéder à leurs données²⁸ ;
9. **droit de rectification** : respect du droit des personnes concernées de corriger leurs données et de les effacer²⁹ ;
10. **transferts** : respect des obligations en matière de transfert de données en dehors de l'Union européenne³⁰ ;
11. **formalités** : définition et accomplissement des formalités préalables applicables au traitement.

2.2. Les mesures destinées à traiter les risques

- Identifier ou déterminer les **mesures retenues** (existantes ou prévues) :
 1. **mesures organisationnelles** : organisation, politique, gestion des risques, gestion de projets, gestion des incidents, supervision...
 2. **mesures de sécurité logique** : anonymisation, chiffrement, sauvegardes, cloisonnement des données, contrôle d'accès logique...
 3. **mesures de sécurité physique** : contrôle d'accès physique, sécurité des matériels, protection contre les sources de risques non humaines...



Conseils pour réaliser les actions

- Pour traiter les risques, il est efficace de déterminer les mesures dans l'ordre suivant :
 1. d'abord **sur la gouvernance** de la protection de la vie privée : mesures transverses destinées à diriger et contrôler la protection de la vie privée (organisation, politique, gestion des risques, gestion de projets...) ;
 2. ensuite **sur les DCP** : mesures destinées à empêcher que leur sécurité ne puisse être atteinte (minimiser, anonymiser...) ;
 3. puis, si cela ne suffit pas à réduire les risques à un niveau acceptable, **sur les impacts potentiels** : mesures destinées à empêcher que les conséquences du risque ne puissent avoir lieu, à identifier et limiter leurs effets ou à les résorber (sauvegarder, contrôler l'intégrité, gérer les violations de DCP...) ;
 4. puis, si cela ne suffit pas, **sur les sources de risques** : mesures destinées à les empêcher d'agir, à identifier et limiter leur action ou à se retourner contre elles (contrôler les accès physiques et logiques, chiffrer, tracer l'activité, gérer les tiers, lutter contre les codes malveillants...) ;
 5. enfin, si cela ne suffit pas, **sur les supports** : mesures destinées à empêcher que les vulnérabilités puissent être exploitées, ou à détecter et limiter les menaces qui surviennent tout de même (exploiter, surveiller, protéger les canaux, réduire les vulnérabilités des logiciels, matériels, documents papiers...).

²⁷ Voir article 38 de la [\[Loi-I&L\]](#) et article 14 de la [\[Directive-95-46\]](#).



²⁸ Voir article 39 de la [\[Loi-I&L\]](#) et article 12 de la [\[Directive-95-46\]](#).

²⁹ La personne concernée peut demander que les « *données inexactes, incomplètes, équivoques, périmées* » ou dont « *la collecte, l'utilisation, la communication ou la conservation est interdite* » soient supprimées (voir article 40 de la [\[Loi-I&L\]](#) et article 12 de la [\[Directive-95-46\]](#)).

³⁰ Voir articles 68 et 69 de la [\[Loi-I&L\]](#) et articles 25 et 26 de la [\[Directive-95-46\]](#).

3. Risques : les atteintes potentielles à la vie privée

Objetif : obtenir une bonne compréhension des causes et conséquences des risques.

| Étape | Description | Rapport |
|---|--|---|
|  |  <p>3. Risques <i>Qui ? Pourquoi ?</i></p> <p>3.1. Sources <i>Quoi ?</i> <i>Comment ?</i></p> <p>3.2. Événements <i>Gravité</i></p> <p>3.3. Menaces <i>Vraisemblance</i></p> <p>3.4. Risques</p> | <ul style="list-style-type: none"> □ Cartographie des risques □ Description détaillée des risques |

3.1. Les sources de risques

- Identifier les **sources de risques** pertinentes dans le contexte considéré³¹.
- Décrire les **capacités** des sources de risques.

3.2. Les événements redoutés

- Pour chaque événement redouté (un accès illégitime aux DCP³², une modification non désirée des DCP³³, et une disparition des DCP³⁴) :
 - déterminer les **impacts** potentiels sur la vie privée des personnes concernées s'ils survenaient³⁵ ;
 - estimer sa **gravité**, notamment en fonction du caractère préjudiciable des impacts potentiels et, le cas échéant, des mesures susceptibles de les modifier ;
 - formaliser une **justification** de l'estimation au regard des éléments identifiés.



Exemples d'événements redoutés

- Des données sur les habitudes d'employés sont illégalement collectées à l'insu des personnes concernées et utilisées par leur hiérarchie pour orienter la recherche d'éléments permettant de les licencier (ex. : vidéosurveillance).
- Des coordonnées sont récupérées et utilisées à l'insu des intéressés à des fins commerciales (spam, publicité ciblée...).
- Des identités sont usurpées afin de réaliser des activités illégales au nom des personnes concernées, ces dernières risquant des poursuites pénales.
- Suite à la modification non désirée de données de santé, des patients sont pris en charge de manière inadaptée, ce qui aggrave leur état de santé et cause même des invalidités ou décès.
- Des demandes de prestations sociales disparaissent, empêchant ainsi les bénéficiaires de les toucher et les obligeant à relancer leurs démarches administratives.

³¹ Répondre à la question « Qui ou quoi pourrait être à l'origine des risques dans le contexte particulier du(des) traitement(s) considéré(s) ? ».

³² Elles sont connues de personnes non autorisées (atteinte à la confidentialité des DCP).

³³ Elles ne sont plus intègres ou sont changées (atteinte à l'intégrité des DCP).

³⁴ Elles ne sont pas ou plus disponibles (atteinte à la disponibilité des DCP).

³⁵ Répondre à la question « Que craint-on qu'il arrive aux personnes concernées ? ».



Conseils pour réaliser les actions

- ❑ Il est utile de différencier les mesures existantes ou prévues des mesures complémentaires, ainsi que la gravité initiale de la gravité résiduelle (qui subsiste, compte tenu des mesures complémentaires).
- ❑ L'analyse des impacts peut aussi être l'occasion de déterminer les besoins de sécurité (confidentialité, intégrité et disponibilité attendues), utiles à l'élaboration d'un cahier des charges.

3.3. Les menaces

- ❑ Identifier les **menaces** sur les supports des DCP qui pourraient mener à chaque événement redouté³⁶.
- ❑ Pour chaque menace identifiée :
 - sélectionner les **sources de risques** qui pourraient en être à l'origine ;
 - estimer sa **vraisemblance**, notamment en fonction des vulnérabilités des supports de DCP, des capacités des sources de risques à les exploiter et des mesures susceptibles de les modifier ;
 - formaliser une **justification** de l'estimation au regard des éléments identifiés.



Exemples de menaces

- Un individu malveillant injecte des requêtes non prévues dans le formulaire d'un site web.
- Un concurrent, en visite incognito, vole un disque dur portable.
- Un membre du personnel supprime des tables d'une base de données par inadvertance.
- Un dégât des eaux détruit les serveurs informatiques et de télécommunications.



Conseils pour réaliser les actions

- ❑ Identifier les menaces consiste à déterminer tout ce qui peut arriver aux supports des DCP pour que les événements redoutés se produisent ; ceci peut être fait soit de manière empirique (ex : *brainstorming*), soit de manière systématique (ex : on étudie toutes les actions possibles sur chaque support de DCP : il peut être observé, utilisé d'une autre manière que celle prévue, modifié, dégradé ou détruit, perdu ou volé).
- ❑ Bien que ce soit déconseillé, il est possible de ne pas étudier les menaces qui permettraient la survenance des événements redoutés dont la gravité est négligeable ou limitée, ou bien de n'étudier que les menaces jugées comme les plus vraisemblables.

3.4. Les risques


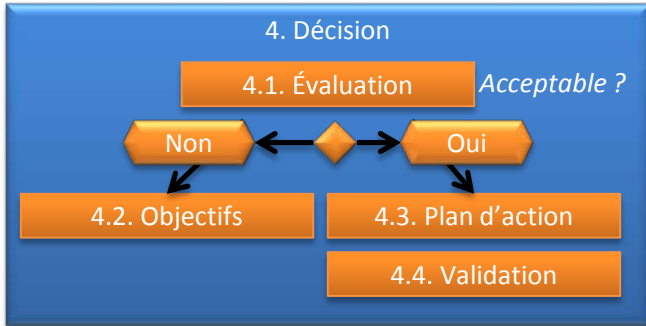
- ❑ Déterminer le niveau de chaque risque³⁷ :
 - sa **gravité** est égale à celle de l'événement redouté concerné par le risque ;
 - sa **vraisemblance** est égale à la valeur la plus élevée de la vraisemblance des menaces associées à l'événement redouté concerné par le risque.
- ❑ Présenter une cartographie de tous les risques en fonction de leur niveau.

³⁶ Répondre à la question « Comment cela pourrait-il arriver ? ».

³⁷ Un risque est composé d'un événement redouté et de toutes les menaces qui permettraient qu'il survienne.

4. Décision : la validation du PIA

🕒 **Objectif** : décider d'accepter ou non la manière dont le PIA a été géré et les risques résiduels³⁸.

| Étape | Description | Rapport |
|---|--|--|
|  |  | <ul style="list-style-type: none"> ❑ Décision argumentée de validation du PIA ❑ Le cas échéant, plan(s) d'action |

4.1. L'évaluation du PIA

- ❑ Étudier les résultats des étapes précédentes :
 - vérifier qu'il n'est pas utile, ou pas possible, d'améliorer la manière dont chaque mesure de nature juridique est mise en œuvre ;
 - vérifier qu'il n'est pas utile, ou pas possible, d'améliorer la manière dont chaque risque est traité ;
- ❑ Décider de leur acceptabilité ou non, de manière argumentée, notamment au regard des enjeux préalablement identifiés.

4.2. Cas 1 – Le PIA n'est pas encore jugé acceptable : objectifs

- ❑ Déterminer les **objectifs** pour les exigences légales et risques pour lesquels la manière de les traiter n'a pas été jugée acceptable.
- ❑ Reprendre les étapes précédentes.

4.3. Cas 2 – Le PIA est jugé acceptable : plan d'action

- ❑ Le cas échéant, élaborer un **plan d'action** pour toutes les mesures prévues.

Conseils pour réaliser les actions

- ❑ Les mesures spécifiées dans le plan d'action devraient être formalisées, mises en place, contrôlées de manière régulière et améliorées de manière continue.

4.4. Cas 2 – Le PIA est jugé acceptable : la validation formelle

- ❑ Valider formellement le PIA³⁹.

³⁸ Risques qui subsistent après application des mesures.

³⁹ La décision ne préjuge en rien de l'évaluation de conformité qui peut être faite, le cas échéant, par l'autorité de protection des données (en France, la CNIL), par exemple dans le cadre de formalités préalables ou de contrôles.

Annexe - Références utilisées

Acronymes

| | |
|-------|--|
| CIL | Correspondant Informatique et Libertés |
| CNIL | Commission Nationale de l'Informatique et des Libertés |
| DCP | Donnée à Caractère Personnel |
| EBIOS | Expression des Besoins et Identification des Objectifs de Sécurité |
| MOA | Maîtrise d'OuvrAge |
| MOE | Maîtrise d'Œuvre |
| RSSI | Responsable de la Sécurité des Systèmes d'Information |
| SSI | Sécurité des Systèmes d'Information |

Définitions

Note : les libellés entre parenthèses correspondent aux libellés courts employés dans ce document.

| | |
|---|---|
| Donnée à caractère personnel (DCP) | Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. [Loi-I&L] |
| Événement redouté | Atteinte à la sécurité de DCP pouvant mener à des impacts sur la vie privée des personnes concernées. |
| Gestion des risques | Processus itératif permettant de maîtriser objectivement les risques qui pèsent sur la vie privée des personnes concernées par un traitement de DCP. Il consiste essentiellement à les apprécier (identification, estimation en termes de gravité et de vraisemblance, et évaluation comparative), les traiter (détermination et mise en place de mesures proportionnées), accepter les risques résiduels, communiquer (consultation des parties prenantes, présentation de résultats...), et surveiller les évolutions dans le temps (du contexte, des risques, des mesures...). |
| Gravité | Estimation de l'ampleur des impacts potentiels sur la vie privée des personnes concernées. Elle dépend essentiellement du caractère |

| | |
|---------------------------------------|--|
| | préjudiciable des impacts potentiels. |
| Menace | Mode opératoire utilisé volontairement ou non par des sources de risques et pouvant provoquer un événement redoutés. |
| Mesure | Action à entreprendre pour traiter des risques. Elle peut consister à les éviter, les réduire, les transférer ou les prendre. |
| Personnes concernées | Les personnes concernées par un traitement de données à caractère personnel sont celles auxquelles se rapportent les données qui font l'objet du traitement. [Loi-I&L] |
| Responsable de traitement | Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. [Loi-I&L] |
| Risque | Scénario décrivant un événement redouté et toutes les menaces qui le rendent possibles. Il est estimé en termes de gravité et de vraisemblance. |
| Source de risque | Personne ou source non humaine qui peut être à l'origine d'un risque, de manière accidentelle ou délibérée. |
| Support | Bien sur lequel reposent des données à caractère personnel. Il peut s'agir de matériels, de logiciels, de canaux informatiques, de personnes, de supports papier ou de canaux de transmission papier. |
| Traitement de DCP (traitement) | Toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. [Loi-I&L] |
| Vraisemblance | Estimation de la possibilité qu'un risque se réalise. Elle dépend essentiellement des vulnérabilités exploitables et des capacités des sources de risques à les exploiter. |
| Vulnérabilité | Caractéristique d'un support de DCP, exploitable par des sources de risques et permettant à des menaces de se réaliser. |

Références bibliographiques

- [\[CharteUE\]](#) Charte des droits fondamentaux de l'Union européenne, 2010/C 83/02.
- [\[Directive-95-46\]](#) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- [\[Ordonnance-2011-1012\]](#) Ordonnance 2011-1012 relative aux communications électroniques transposant notamment la directive 2009/136/CE introduisant l'obligation de notification des violations de données à caractère personnel collectées dans le cadre de traitement mis en œuvre par des fournisseurs de services de télécommunication ouverts au public.
- [\[Loi-I&L\]](#) Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée⁴⁰.
- [\[ISO31000\]](#) ISO 31000:2009, Management du risque – Principes et lignes directrices, ISO.
- [\[PIA-1-Methode\]](#) Guide *PIA – Méthode* (démarche pour mener un PIA), CNIL.
- [\[PIA-2-Outillage\]](#) Guide *PIA – Outillage* (modèles et bases de connaissances), CNIL.
- [\[PIA-3-BonnesPratiques\]](#) Guide *PIA – Bonnes pratiques* (mesures pour traiter les risques), CNIL.
- [\[GuideSécurité\]](#) Guide « *La sécurité des données personnelles* », CNIL.
- [\[EBIOS\]](#) Expression des Besoins et Identification des Objectifs de Sécurité – EBIOS – Méthode de gestion des risques, 25 janvier 2010, ANSSI.

⁴⁰ Modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et par la loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures.