PIA, L'OUTILLAGE

ÉTUDE D'IMPACT SUR LA VIE PRIVÉE (EIVP)

PRIVACY IMPACT ASSESSMENT (PIA)

Modèles et bases de connaissances

CNIL
Commission Nationale de l'Informatique et des Libertés

Édition juin 2015

Sommaire

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

Avant propos

Ce document doit être utilisé conjointement avec les guides suivants :

- [PIA-1-Methode], qui présente la méthode pour réaliser les PIA ;
- [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.

Attention : les modèles et bases de connaissances présentés dans ce guide constituent une aide à la mise en œuvre de la démarche. Il est tout à fait possible et même souhaitable de les adapter à chaque contexte particulier.

Rappel : 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.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

1. Outillage pour l'étude du contexte

1.1. La description générale

Modèle : description générale

Le modèle suivant peut être utilisé pour décrire le traitement de manière synthétique :

Description du traitement	
Finalités du traitement	❑
Enjeux du traitement	❑
Responsable du traitement	
Sous-traitants	❑

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

1.2. La description détaillée

Modèle : description des données à caractère personnel (DCP)

Le modèle suivant peut être utilisé pour présenter les DCP :

DCP	Catégories	Destinataires des DCP (et justifications)	Personnes pouvant y accéder (et justifications)	Durée de conservation (et justifications)

Notes

- On considère généralement les DCP dans leur ensemble dans la suite de l'étude.
- Toutefois, leur description devrait être détaillée dans cette partie. Selon la taille et la complexité du(des) traitement(s) de DCP considéré(s), mais aussi selon ce que l'on souhaite mettre en évidence, les DCP peuvent alors être regroupées en ensembles cohérents et faciles à étudier.

Base de connaissances : typologie des DCP

Les catégories de DCP sont généralement les suivantes :

Types de DCP	Catégories de DCP
DCP courantes	État-civil, identité, données d'identification
	Vie personnelle (habitudes de vie, situation familiale, hors données sensibles ou dangereuses…)
	Vie professionnelle (CV, scolarité formation professionnelle, distinctions…)
	Informations d'ordre économique et financier (revenus, situation financière, situation fiscale…)
	Données de connexion (adresses IP, journaux d'événements…)
	Données de localisation (déplacements, données GPS, GSM…)
DCP perçues comme sensibles	Numéro de sécurité sociale (NIR)
	Données biométriques
	Données bancaires
DCP sensibles au sens de la [Loi-I&L][1]	Opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciales ou ethniques, relatives à la santé ou à la vie sexuelle
	Infractions, condamnations, mesures de sécurité

Notes

- Les supports des DCP peuvent être regroupés en ensembles cohérents.

[1] Voir notamment les articles 8 et 9 de la [Loi-I&L] et l'article 8 de la [Directive-95-46].

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

Modèle : description des supports de DCP

Le modèle suivant peut être utilisé pour présenter les supports des DCP pour chaque processus du(des) traitement(s) de DCP considéré(s) :

Processus génériques	Description détaillée du processus	Systèmes informatiques[2] sur lesquels reposent les DCP	Autres supports[3] sur lesquelles reposent les DCP
Collecte			
Conservation			
Utilisation			
Transfert			
Destruction			

Notes

- Le processus d' « utilisation » a généralement besoin d'être décomposé en autant de processus mis en œuvre par le traitement.

Base de connaissances : typologie des supports de DCP

Les supports de DCP sont les composants du système d'information sur lesquels reposent les DCP :

Types de supports de DCP		Exemples
Systèmes informatiques	Matériels et supports de données électroniques	Ordinateurs, relais de communication, clés USB, disques durs
	Logiciels	Systèmes d'exploitation, messagerie, bases de données, applications métier
	Canaux informatiques	Câbles, WiFi, fibre optique
Organisations	Personnes	Utilisateurs, administrateurs informatiques, décideurs
	Supports papier	Impressions, photocopies, documents manuscrits
	Canaux de transmission papier	Envoi postal, circuit de validation

Notes

- Il convient de choisir le niveau de détail le plus approprié au sujet de l'étude.
- Les solutions de sécurité (produits, procédures, mesures…) ne sont pas des supports de DCP : il s'agit de mesures destinées à traiter les risques.

[2] Décomposables en matériels (et supports de données électroniques), logiciels et canaux informatiques.
[3] Décomposables en personnes, supports papier et canaux de transmission papier.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

2. Outillage pour l'étude des mesures

2.1. Les mesures de nature juridiques (obligatoires)

Modèle : dispositif de conformité pour respecter les exigences légales

Le modèle suivant peut être utilisé pour présenter les mesures existantes ou prévues :

Thèmes	Points de contrôle	Effet principal	Description des mesures / Justifications
1. Mesures de nature juridique (obligatoires)	Finalité : finalité déterminée, explicite et légitime[4]	Données	
	Minimisation : réduction des données à celles strictement nécessaires[5]	Données	
	Qualité : préservation de la qualité des données à caractère personnel[6]	Données	
	Durées de conservation : durée nécessaire à l'accomplissement des finalités, à défaut d'une autre obligation légale imposant une conservation plus longue [7]	Données	
	Information : respect du droit à l'information des personnes concernées[8]	Données	
	Consentement : obtention du consentement des personnes concernées ou existence d'un autre fondement légal justifiant le traitement [9]	Données	
	Droit d'opposition : respect du droit d'opposition des personnes concernées[10]	Données	
	Droit d'accès : respect du droit des personnes concernées d'accéder à leurs données[11]	Données	
	Droit de rectification : respect du droit des personnes concernées de corriger leurs données	Données	

[4] « *Elles sont collectées pour des finalités déterminées, explicites et légitimes* » (article 6 de la [Loi-I&L] et de la [Directive-95-46]).
[5] « *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]).
[6] « *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.
[7] « *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.
[8] Voir article 32 de la [Loi-I&L] et articles 10 et 11 de la [Directive-95-46].
[9] S'il y a lieu, voir article 7 de la [Loi-I&L].
[10] Voir article 38 de la [Loi-I&L] et article 14 de la [Directive-95-46].
[11] Voir article 39 de la [Loi-I&L] et article 12 de la [Directive-95-46].

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

Thèmes	Points de contrôle	Effet principal	Description des mesures / Justifications
	et de les effacer[12]		
	Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne[13]	Données	
	Formalités : définition et accomplissement des formalités préalables applicables au traitement	Données	

[12] 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]).
[13] Voir articles 68 et 69 de la [Loi-I&L] et articles 25 et 26 de la [Directive-95-46]).

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

2.2. Les mesures destinées à traiter les risques

Modèle : dispositif de conformité pour traiter les risques

Le modèle suivant peut être utilisé pour présenter les mesures existantes ou prévues :

Thèmes	Points de contrôle	Effet principal	Description des mesures / Justifications
2. Mesures organisationnelles	Organisation	Transverse	
	Politique (gestion des règles)	Transverse	
	Gestion des risques	Transverse	
	Gestion des projets	Transverse	
	Gestion des incidents et des violations de données	Impacts	
	Gestion des personnels	Sources	
	Relations avec les tiers	Sources	
	Maintenance	Sources	
	Supervision (audits, tableaux de bord…)	Transverse	
	Marquage des documents	Sources	
	Archivage	Transverse	
3. Mesures de sécurité logique	Anonymisation	Données	
	Chiffrement	Sources	
	Contrôle d'intégrité	Impacts	
	Sauvegardes	Impacts	
	Cloisonnement des données	Sources	
	Contrôle d'accès logique	Sources	
	Traçabilité	Sources	
	Exploitation	Supports	
	Surveillance (paramétrages, contrôles de configurations, surveillance en temps réel…)	Supports	
	Gestion des postes de travail	Supports	
	Lutte contre les codes malveillants (virus, logiciels espions, bombes logicielles…)	Sources	
	Protection des canaux informatiques (réseaux)	Supports	
4. Mesures de sécurité physique	Éloignement des sources de risques (produits dangereux, zones géographiques dangereuses…)	Sources	
	Contrôle d'accès physique	Sources	
	Sécurité des matériels	Supports	
	Sécurité des documents papier	Supports	
	Sécurité des canaux papier	Supports	
	Protection contre les sources de risques non humaines (feu, eau…)	Sources	

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

3. Outillage pour l'étude des risques

3.1. Les sources de risques

Modèle : étude des sources de risques

Le modèle suivant peut être utilisé pour présenter les sources de risques retenues :

Types de sources de risques	Sources de risques pertinentes	Description des capacités[14]
Sources humaines internes agissant accidentellement		
Sources humaines internes agissant de manière délibérée		
Sources humaines externes agissant accidentellement		
Sources humaines externes agissant de manière délibérée		
Sources non humaines internes		
Sources non humaines externes		

Notes

- Si plusieurs sources de risques sont identifiées pour un même type, alors il convient de se baser sur celle qui a le plus de capacité dans la réflexion sur les risques.

Base de connaissances : typologie de sources de risques

Le tableau suivant présente des exemples de sources de risques :

Types de sources de risques	Exemples
Sources humaines internes	Salariés, administrateurs informatiques, stagiaires, dirigeants
Sources humaines externes	Destinataires des DCP, tiers autorisés[15], prestataires, pirates informatiques, visiteurs, anciens employés, militants, concurrents, clients, personnels d'entretien, maintenance, délinquant, syndicats, journalistes, organisations non gouvernementales, organisations criminelles, organisations sous le contrôle d'un État étranger, organisations terroristes, activités industrielles environnantes
Sources non humaines	Codes malveillants d'origine inconnue (virus, vers…), eau (canalisations, cours d'eau…), matières inflammables, corrosives ou explosives, catastrophes naturelles, épidémies, animaux

[14] Leurs capacités recouvrent leur proximité aux supports de DCP, compétences, ressources financières, temps disponible, etc. ainsi que, dans le cas de sources humaines, les raisons de leur action dans les cas accidentels (maladresse, inconscience, faible conscience d'engagement, peu motivé dans sa relation avec l'organisme…) ou leur motivation dans les cas délibérés (jeu, égo, vengeance, appât du gain, sentiment d'impunité…).

[15] Par exemple, des autorités publiques et auxiliaires de justice peuvent demander communication de certaines données quand la loi les y autorise expressément.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

3.2. Les événements redoutés

Modèle : étude des événements redoutés

Le modèle suivant peut être utilisé pour présenter les événements redoutés :

Violations potentielles	Sources de risques	Suites / objectifs poursuivis	Impacts potentiels	Mesures	Gravité	Justification
Accès illégitime aux DCP		❑ Aucune ❑ Stockage ❑ Rediffusion ❑ Corrélation ❑ Exploitation ❑ Autres (préciser)				
Modification non désirée des DCP		❑ Dysfonctionnement ❑ Exploitation ❑ Autres (préciser)				
Disparition des DCP		❑ Dysfonctionnement ❑ Blocage ❑ Autres (préciser)				

Notes

- Le libellé des trois événements redoutés, étudiés de manière systématique dans un PIA, peut être adapté afin qu'il soit mieux compris des parties prenantes.
- Les sources de risques sont celles jugées comme pertinentes, dans le contexte considéré, pour être à l'origine de l'événement redouté.
- Les suites / objectifs poursuivis sont la(les) suite(s) de l'événement redouté jugée(s) comme pertinente(s) dans le contexte considéré.
- Les impacts potentiels sont la liste des conséquences possibles sur la vie privée des personnes concernées.
- Les sources de risques sont les sources pertinentes pour être à l'origine de chaque événement redouté dans le contexte considéré.
- Les mesures sont, le cas échéant, la liste des mesures existantes ou prévues qui agissent sur la gravité de l'événement redouté considéré.
- La gravité est estimée à l'aide des échelles et des règles de calculs retenues.
- La justification permet d'expliquer comment la gravité a été déterminée (par exemple, pour une gravité « limitée » dans un contexte donné : « les DCP sont parfaitement identifiantes et les impacts potentiels sont importants, mais les mesures permettent de réduire grandement le caractère préjudiciable »).
- Quand on divise les DCP en plusieurs sous-ensembles (quand on ne les considère pas dans leur ensemble), les événements redoutés sont démultipliées en autant de sous-ensemble.
- S'il apparait que les impacts diffèrent significativement selon les sources de risques (ex. : accès illégitime interne ou externe, accident ou attaque…) ou les suites d'un événement

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

redouté (ex. : modification en données qui n'ont plus de sens ou en d'autres DCP valides, disparition momentanée ou définitive…), il peut aussi être pertinent de décomposer les événements redoutés.

- Afin de bien distinguer d'une part les impacts sur la vie privée des personnes concernées, et d'autre part les impacts sur l'organisme (ex : perte d'image, perte financière, perturbation de l'activité, conséquence juridique…), il est peut être utile d'identifier et de présenter ces deux types d'impacts ; mais dans ce cas, seuls les premiers serviront à estimer la gravité des événements redoutés dans un PIA.

Base de connaissances : typologie de suites des événements redoutés

Les événements redoutés peuvent avoir différentes conséquences s'ils se produisent :

Événements redoutés	Types de suites	Description
Accès illégitime aux DCP	Aucune	Les données sont vues par des personnes qui n'ont pas à les connaître, sans que celles-ci ne les exploitent.
	Stockage	Les données sont copiées et sauvegardées à un autre endroit, sans être davantage exploitées.
	Rediffusion	Les données sont diffusées plus que nécessaire et échappent à la maîtrise des personnes concernées (ex. : diffusion non désirée d'une photo sur Internet, perte de contrôle d'informations publiées dans un réseau social...)
	Exploitation	Les données sont exploitées à d'autres fins que celles prévues et/ou de manière injuste (ex. : fins commerciales, usurpation d'identité, utilisation à l'encontre des personnes concernées...) ou corrélées avec d'autres informations relatives aux personnes concernées (ex. : corrélation d'adresses de résidence et de données de géolocalisation en temps réel...) dans un premier temps
Modification non désirée des DCP	Dysfonctionnement	Les données sont modifiées en des données valides ou invalides, qui ne seront pas utilisées de manière correcte, le traitement pouvant engendrer des erreurs, des dysfonctionnements, ou ne plus fournir le service attendu (ex. : altération du bon déroulement de démarches importantes...)
	Exploitation	Les données sont modifiées en d'autres données valides, de telle sorte que les traitements ont été ou pourraient être détournés (ex. : exploitation pour usurper des identités en changeant la relation entre l'identité des personnes et les données biométriques d'autres personnes...).
Disparition des DCP	Dysfonctionnement	Les données sont manquantes à des traitements, ce qui génère des erreurs, des dysfonctionnements, ou fournit un service différent de celui attendu (ex. : certaines allergies ne sont plus signalées dans un dossier médical, certaines informations figurant dans des déclarations de revenus ont disparu, ce qui empêche le calcul du montant des impôts...)

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

Événements redoutés	Types de suites	Description
	Blocage	Les données sont manquantes à des traitements qui ne peuvent plus du tout fournir le service attendu (ex. : ralentissement ou blocage de processus administratifs ou commerciaux, impossibilité de fournir des soins du fait de la disparition de dossiers médicaux, impossibilité pour des personnes concernées d'exercer leurs droits...).

Base de connaissances : échelles et règles pour estimer les risques

Les éléments suivants peuvent être utilisés pour estimer la gravité et la vraisemblance.

Notes

- L'estimation des risques peut être réalisée de différentes manières, dans la mesure où l'on obtient une gravité et une vraisemblance pour chaque risque.
- L'estimation des risques est forcément subjective, mais cette subjectivité est contrebalancée par des échelles et des règles claires et une estimation qui repose sur le consensus des parties prenantes.
- Les échelles et règles utilisées sont des éléments de communication importants, qui doivent être comprises, acceptées et utilisables par les parties prenantes.

Échelle et règles pour estimer la gravité

La gravité représente l'ampleur d'un risque. Elle est essentiellement estimée au regard de la hauteur des impacts potentiels sur les personnes concernées, compte tenu des mesures existantes, prévues ou complémentaires (qu'il convient de mentionner en tant que justification).

L'échelle suivante peut être utilisée pour estimer la gravité des événements redoutés (**attention : ce ne sont que des exemples, qui peuvent être très différents selon le contexte**) :

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[16]	Exemples d'impacts matériels[17]	Exemples d'impacts moraux[18]
1. Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront	- Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle)	- Perte de temps pour réitérer des démarches ou pour attendre de les réaliser - Réception de courriers non sollicités (ex. : *spams*) - Réutilisation de données publiées sur des sites Internet à des fins de	- Simple contrariété par rapport à l'information reçue ou demandée - Peur de perdre le contrôle de ses données - Sentiment d'atteinte à

[16] Préjudice d'agrément, d'esthétique ou économique lié à l'intégrité physique.
[17] Perte subie ou gain manqué concernant le patrimoine des personnes.
[18] Souffrance physique ou morale, préjudice esthétique ou d'agrément.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[16]	Exemples d'impacts matériels[17]	Exemples d'impacts moraux[18]
	sans difficulté	- Maux de tête passagers	publicité ciblée (information des réseaux sociaux réutilisation pour un mailing papier) - Publicité ciblée pour des produits de consommation courants	la vie privée sans préjudice réel ni objectif (ex : intrusion commerciale) - Perte de temps pour paramétrer ses données - Non respect de la liberté d'aller et venir en ligne du fait du refus d'accès à un site commercial (ex : alcool du fait d'un âge erroné)
2. Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	- Affection physique mineure (ex. : maladie bénigne suite au non respect de contre-indications) - Absence de prise en charge causant un préjudice minime mais réel (ex : handicap) - Diffamation donnant lieu à des représailles physiques ou psychiques	- Paiements non prévus (ex. : amendes attribuées de manière erronée), frais supplémentaires (ex. : agios, frais d'avocat), défauts de paiement - Refus d'accès à des services administratifs ou prestations commerciales - Opportunités de confort perdues (ex. : annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne) - Promotion professionnelle manquée - Compte à des services en ligne bloqué (ex. : jeux, administration) - Réception de courriers ciblés non sollicités susceptible de nuire à la réputation des personnes concernées - Élévation de coûts (ex. : augmentation du prix d'assurance) - Données non mises à jour (ex. : poste antérieurement occupé) - Traitement de données erronées créant par exemple des dysfonctionnements de comptes (bancaires, clients, auprès d'organismes sociaux, etc.) - Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique) - Profilage imprécis ou abusif	- Refus de continuer à utiliser les systèmes d'information (*whistleblowing*, réseaux sociaux) - Affection psychologique mineure mais objective (diffamation, réputation) - Difficultés relationnelles avec l'entourage personnel ou professionnel (ex. : image, réputation ternie, perte de reconnaissance) - Sentiment d'atteinte à la vie privée sans préjudice irrémédiable - Intimidation sur les réseaux sociaux
3. Importante	Les personnes concernées	- Affection physique grave causant un	- Détournements d'argent non indemnisé	- Affection psychologique grave

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[16]	Exemples d'impacts matériels[17]	Exemples d'impacts moraux[18]
	pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives	préjudice à long terme (ex. : aggravation de l'état de santé suite à une mauvaise prise en charge, ou au non respect de contre-indications) - Altération de l'intégrité corporelle par exemple à la suite d'une agression, d'un accident domestique, de travail, etc.	- Difficultés financières non temporaires (ex. : obligation de contracter un prêt) - Opportunités ciblées, uniques et non récurrentes, perdues (ex. : prêt immobilier, refus d'études, de stages ou d'emploi, interdiction d'examen) - Interdiction bancaire - Dégradation de biens - Perte de logement - Perte d'emploi - Séparation ou divorce - Perte financière à la suite d'une escroquerie (ex. : après une tentative d'hameçonnage - *phishing*) - Bloqué à l'étranger - Perte de données clientèle	(ex. : dépression, développement d'une phobie) - Sentiment d'atteinte à la vie privée et de préjudice irrémédiable - Sentiment de vulnérabilité à la suite d'une assignation en justice - Sentiment d'atteinte aux droits fondamentaux (ex. : discrimination, liberté d'expression) - Victime de chantage - *Cyberbullying* et harcèlement moral
4. Maximale	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter	- Affection physique de longue durée ou permanente (ex. : suite au non respect d'une contre-indication) - Décès (ex. : meurtre, suicide, accident mortel) - Altération définitive de l'intégrité physique	- Péril financier - Dettes importantes - Impossibilité de travailler - Impossibilité de se reloger - Perte de preuves dans le cadre d'un contentieux - Perte d'accès à une infrastructure vitale (eau, électricité)	- Affection psychologique de longue durée ou permanente - Sanction pénale - Enlèvement - Perte de lien familial - Impossibilité d'ester en justice - Changement de statut administratif et/ou perte d'autonomie juridique (tutelle)

On retient la valeur dont la description correspond le mieux aux impacts potentiels identifiés, en comparant les impacts identifiés dans le contexte considéré avec les impacts génériques de l'échelle.

Elle peut être augmentée ou diminuée en fonction d'autres facteurs, tels que les suivants :

- le caractère identifiant des DCP ;
- la nature des sources de risques ;
- le nombre d'interconnexions (notamment avec l'étranger) ;
- le nombre de destinataires (ce qui facilite la corrélation de DCP initialement séparées).

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

Échelle et règles pour estimer la vraisemblance

La vraisemblance traduit la possibilité qu'un risque se réalise. Elle est essentiellement estimée au regard des vulnérabilités des supports concernés et de la capacité des sources de risques à les exploiter, compte tenu des mesures existantes, prévues ou complémentaires (qu'il convient de mentionner en tant que justification).

L'échelle suivante peut être utilisée pour estimer la vraisemblance des menaces :

1. Négligeable : il ne semble pas possible que les sources de risques retenues puissent réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge et code d'accès).
2. Limité : il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge).
3. Important : il semble possible pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans les bureaux d'un organisme dont l'accès est contrôlé par une personne à l'accueil).
4. Maximal : il semble extrêmement facile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papier stockés dans le hall public de l'organisme).

On retient la valeur dont la description correspond le mieux aux vulnérabilités des supports et aux sources de risques identifiés.

Elle peut être augmentée ou diminuée en fonction d'autres facteurs, tels que les suivants :

- une ouverture sur Internet ou un système fermé ;
- des échanges de données avec l'étranger ou non ;
- des interconnexions avec d'autres systèmes ou aucune interconnexion ;
- l'hétérogénéité ou l'homogénéité du système ;
- la variabilité ou la stabilité du système ;
- l'image de l'organisme.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

3.3. Les menaces

Modèle : étude des menaces

Le modèle suivant peut être utilisé pour présenter les menaces :

Menaces	Sources de risques	Mesures	Vraisemblance	Justification

Notes

- Le libellé des menaces issues des bases de connaissances présentées ci-après peut être adapté afin qu'il soit mieux compris des parties prenantes ou qu'il reflète plus explicitement les menaces auxquelles on est exposé.
- Si certaines menaces ne sont pas applicables (par exemple les menaces relatives aux documents papier dans un contexte où il n'y a pas de documents papier), alors il est préférable de les laisser dans le tableau et de l'expliquer dans la justification.
- Les sources de risques sont les sources pertinentes pour être à l'origine de chaque menace dans le contexte considéré.
- Les mesures sont, le cas échéant, la liste des mesures existantes ou prévues qui agissent sur la vraisemblance de la menace considérée.
- La vraisemblance est estimée à l'aide des échelles et des règles de calculs retenues.
- La justification permet d'expliquer comment la vraisemblance a été déterminée (par exemple, pour une vraisemblance « négligeable » dans un contexte donné : « les vulnérabilités des supports sont importantes et les capacités des sources de risques à les exploiter sont maximales, mais les mesures permettent de les réduire grandement »).

Base de connaissances : typologie de menaces

L'action des sources de risques sur les supports constitue une menace peut prendre la forme de différentes menaces. Les supports peuvent être :

- utilisés de manière inadaptée : les supports sont utilisés hors de leur cadre d'utilisation prévu, voire détournés, sans être modifiés ni endommagés ;
- observés : les supports sont observés ou espionnés sans être endommagés ;
- surchargés : les limites de fonctionnement des supports sont dépassées, ils sont surchargés, surexploités ou utilisés dans des conditions ne leur permettant pas de fonctionner correctement ;
- détériorés : les supports sont endommagés, partiellement ou totalement ;
- modifiés : les supports sont transformés ;
- perdus : les supports sont perdus, volés, vendus ou donnés, de telle sorte qu'il n'est plus possible d'exercer les droits de propriété.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

Les menaces génériques qui suivent sont conçues pour être exhaustives, indépendantes et appliquées aux spécificités de la protection de la vie privée.

Menaces qui peuvent mener à un accès illégitime aux DCP

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
C	Matériels	Utilisés de manière inadaptée	Utilisation de clefs USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles,le disque dur contenant les informations est utilisé pour une fin non prévue (par exemple pour transporter d'autres données chez un prestataire, pour transférer d'autres données d'une base de données à une autre, etc.)	Utilisable en dehors de l'usage prévu, disproportion entre le dimensionnement des matériels et le dimensionnement nécessaire (par exemple : disque dur de plusieurs To pour stocker quelques Go de données)
C	Matériels	Observés	Observation d'un écran à l'insu de son utilisateur dans un train, photographie d'un écran, géolocalisation d'un matériel, captation de signaux électromagnétiques à distance	Permet d'observer des données interprétables, émet des signaux compromettants
C	Matériels	Modifiés	Piégeage par un keylogger, retrait d'un composant matériel, branchement d'un appareil (ex. : clé USB) pour lancer un système d'exploitation ou récupérer des données	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)
C	Matériels	Perdus	Vol d'un ordinateur portable dans une chambre d'hôtel, vol d'un téléphone portable professionnel par un pickpocket, récupération d'un matériel ou d'un support mis au rebut, perte d'un support de stockage électronique	Petite taille, attractif (valeur marchande)
C	Logiciels	Utilisés de manière inadaptée	Fouille de contenu, croisement illégitime de données, élévation de privilèges, effacement de traces, envoi de *spams* depuis la messagerie, détournement de fonctions réseaux	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées
C	Logiciels	Observés	Balayage d'adresses et ports réseau, collecte de données de configuration, étude d'un code source pour déterminer les défauts exploitables, test des réponses d'une base de données à des requêtes malveillantes	Possibilité d'observer le fonctionnement du logiciel, accessibilité et intelligibilité du code source
C	Logiciels	Modifiés	Piégeage par un keylogger logiciel, contagion par un code malveillant, installation d'un outil de prise de contrôle à distance, substitution d'un composant par un autre lors d'une mise à jour, d'une opération de maintenance ou d'une installation (des bouts de codes ou applications sont installés ou remplacés)	Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes
C	Canaux informatiques	Observés	Interception de flux sur le réseau Ethernet, acquisition de données sur un réseau wifi	Perméable (émission de rayonnements parasites ou non), permet d'observer des données interprétables
C	Personnes	Observées	Divulgation involontaire en conversant, écoute d'une salle de réunion avec un matériel d'amplification sensorielle	Peu discret (loquace, sans réserve), routinier (habitudes facilitant l'espionnage récurrent)
C	Personnes	Détournées	Influence (hameçonnage, filoutage, ingénierie sociale, corruption), pression (chantage, harcèlement moral)	Influençable (naïf, crédule, obtus, faible estime de soi, faible loyauté), manipulable (vulnérable aux pressions sur soi ou son entourage)
C	Personnes	Perdues	Débauchage d'un employé, changement d'affectation, rachat de tout ou partie de l'organisation	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel
C	Documents	Observés	Lecture, photocopie, photographie	Permet d'observer des données

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
	papier			interprétables
C	Documents papier	Perdus	Vol de dossiers dans les bureaux, vol de courriers dans la boîte aux lettres, récupération de documents mis au rebut	Portable
C	Canaux papier	Observés	Lecture de parapheurs en circulation, reproduction de documents en transit	Observable

Menaces qui peuvent mener à une modification non désirées des DCP

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
I	Matériels	Modifiés	Ajout d'un matériel incompatible menant à un dysfonctionnement, retrait d'un matériel indispensable au fonctionnement correct d'une application	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)
I	Logiciels	Utilisés de manière inadaptée	Modifications inopportunes dans une base de données, effacement de fichiers utiles au bon fonctionnement, erreur de manipulation menant à la modification de données	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées
I	Logiciels	Modifiés	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre	Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes
I	Canaux informatiques	Utilisés de manière inadaptée	*Man in the middle* pour modifier ou ajouter des données à un flux réseau, rejeu (réémission d'un flux intercepté)	Permet d'altérer les flux communiqués (interception puis réémission, éventuellement après altération), seule ressource de transmission pour le flux, permet de modifier les règles de partage du canal informatique (protocole de transmission qui autorise l'ajout de nœuds)
I	Personnes	Surchargées	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées à la fonction Incapacité à s'adapter au changement
I	Personnes	Détournées	Influence (rumeur, désinformation)	Influençable (naïf, crédule, obtus)
I	Documents papier	Modifiés	Modification de chiffres dans un dossier, remplacement d'un document par un faux	Falsifiable (support papier au contenu modifiable)
I	Canaux papier	Modifiés	Modification d'une note à l'insu du rédacteur, changement d'un parapheur par un autre, envoi multiple de courriers contradictoires	Permet d'altérer les documents communiqués, seule ressource de transmission pour le canal, permet la modification du circuit papier

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

Menaces qui peuvent mener à une disparition des DCP

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
D	Matériels	Utilisés de manière inadaptée	Stockage de fichiers personnels, utilisation à des fins personnelles	Utilisable en dehors de l'usage prévu
D	Matériels	Surchargés	Unité de stockage pleine, panne de courant, surexploitation des capacités de traitement, échauffement, température excessive, attaque par dénis de service	Dimensionnement inapproprié des capacités de stockage, dimensionnement inapproprié des capacités de traitement, n'est pas approprié aux conditions d'utilisation, requiert en permanence de l'électricité pour fonctionner, sensible aux variations de tension
D	Matériels	Modifiés	Ajout d'un matériel incompatible menant à une panne, retrait d'un matériel indispensable au fonctionnement du système	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)
D	Matériels	Détériorés	Inondation, incendie, vandalisme, dégradation du fait de l'usure naturelle, dysfonctionnement d'un dispositif de stockage	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement) ; n'est pas approprié aux conditions d'utilisation ; effaçable (vulnérable aux effets magnétiques ou vibratoires)
D	Matériels	Perdus	Vol d'un ordinateur portable, perte d'un téléphone portable, mise au rebut d'un support ou d'un matériel, disques sous dimensionnés amenant à une multiplication des supports et à la perte de certains	Portable, attractif (valeur marchande)
D	Logiciels	Utilisés de manière inadaptée	Effacement de données, utilisation de logiciels contrefaits ou copiés, erreur de manipulation menant à la suppression de données	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées
D	Logiciels	Surchargés	Dépassement du dimensionnement d'une base de données, injection de données en dehors des valeurs prévues, attaque par dénis de service	Permet de saisir n'importe quelle donnée, permet de saisir n'importe quel volume de données, permet d'exécuter des actions avec les données entrantes, peu interopérable
D	Logiciels	Modifiés	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre	Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes
D	Logiciels	Détériorés	Effacement d'un exécutable en production ou de code sources, virus, bombe logique	Possibilité d'effacer ou de supprimer des programmes, exemplaire unique, utilisation complexe (mauvaise ergonomie, peu d'explications)
D	Logiciels	Perdus	Non renouvellement de la licence d'un logiciel utilisé pour accéder aux données, arrêt des mises à jour de maintenance de sécurité par l'éditeur, faillite de l'éditeur, corruption du module de stockage contenant les numéros de licence	Exemplaire unique (des contrats de licence ou du logiciel, développé en interne), attractif (rare, novateur, grande valeur commerciale), cessible (clause de cessibilité totale dans la licence)
D	Canaux informatiques	Surchargés	Détournement de la bande passante, téléchargement non autorisé, coupure d'accès Internet	Dimensionnement fixe des capacités de transmission (dimensionnement insuffisant de la bande passante, plage de numéros téléphoniques limitée)
D	Canaux informatiques	Détériorés	Sectionnement de câblage, mauvaise réception du réseau wifi, oxydation des câbles	Altérable (fragile, cassable, câble de faible structure, à nu, gainage

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
				disproportionné), unique
D	Canaux informatiques	Perdus	Vol de câbles de transmission en cuivre	Attractif (valeur marchande des câbles), transportable (léger, dissimulable), peu visible (oubliable, insignifiant, peu remarquable)
D	Personnes	Surchargées	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées aux conditions d'exercice de ses fonctions, incapacité à s'adapter au changement
D	Personnes	Détériorées	Accident du travail, maladie professionnelle, autre blessure ou maladie, décès, affection neurologique, psychologique ou psychiatrique	Limites physiques, psychologiques ou mentales
D	Personnes	Perdues	Décès, retraite, changement d'affectation, fin de contrat ou licenciement, rachat de tout ou partie de l'organisation	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel
D	Documents papier	Utilisés de manière inadaptée	Effacement progressif avec le temps, effacement volontaire de parties d'un texte, réutilisation des papiers pour prendre des notes sans relation avec le traitement, pour faire la liste de course, utilisation des cahiers pour faire autre chose	Modifiable (support papier au contenu effaçable, papiers thermiques non résistants aux modifications de températures)
D	Documents papier	Détériorés	Vieillissement de documents archivés, embrasement des dossiers lors d'un incendie	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement), n'est pas approprié aux conditions d'utilisation
D	Documents papier	Perdus	Vol de documents, perte de dossiers lors d'un déménagement, mise au rebut	Portable
D	Canaux papier	Surchargés	Surcharge de courriers, surcharge d'un processus de validation	Existence de limites quantitatives ou qualitatives
D	Canaux papier	Détériorés	Coupure du flux suite à une réorganisation, blocage du courrier du fait d'une grève	Instable, unique
D	Canaux papier	Modifiés	Modification dans l'expédition des courriers, réaffectation des bureaux ou des locaux, réorganisation de circuits papier, changement de langue professionnelle	Modifiable (remplaçable)
D	Canaux papier	Perdus	Réorganisation supprimant un processus, disparition d'un transporteur de documents, vacance de postes	Utilité non reconnue

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

3.4. Les risques

Modèle : évaluation des risques

Le tableau suivant peut être utilisé pour présenter les risques :

Risques	Exemples	Principales mesures	Principaux impacts	Gravité	Principales menaces	Vraisemblance
Accès illégitime aux DCP						
Modification non désirée des DCP						
Disparition des DCP						

Un schéma tel que le suivant peut être utilisé pour présenter la cartographie des risques :

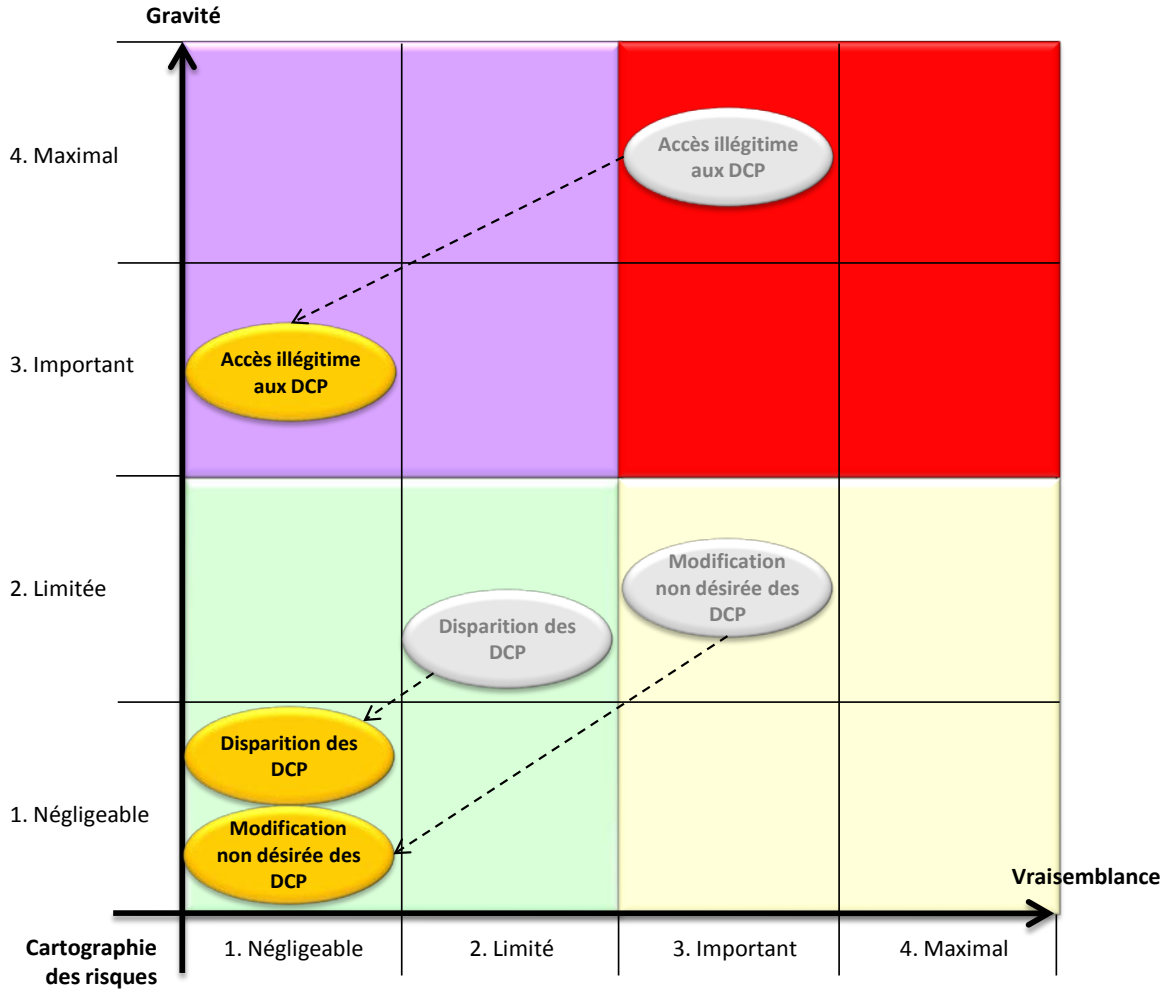

Figure 1 – Cartographie des risques

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

4. Outillage pour la validation du PIA

4.1. L'évaluation du PIA

Modèle : évaluation des mesures de nature juridique et des risques résiduels

Le tableau suivant peut être utilisé pour résumer l'évaluation du PIA :

	Libellé	Acceptabilité (et arguments)
Mesures de nature juridique	Finalité	
	Minimisation	
	Qualité	
	Durées de conservation	
	Information	
	Consentement	
	Droit d'opposition	
	Droit d'accès	
	Droit de rectification	
	Transferts	
	Formalités	
Risques	Accès illégitime aux DCP	
	Modification non désirée des DCP	
	Disparition des DCP	

Notes

- On peut démontrer à la fois que les risques sont bien traités et que les mesures sont toutes utiles en créant un tableau, avec les mesures en lignes, les risques en colonnes et une croix dans chaque cellule où une mesure contribue au traitement d'un risque.
- Donner des exemples de risques résiduels est utile pour démontrer qu'ils peuvent être acceptés.

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

Modèle : identification des objectifs

Le tableau suivant peut être utilisé pour formuler les objectifs :

	Libellé	Objectif
Mesures de nature juridique	Finalité	
	Minimisation	
	Qualité	
	Durées de conservation	
	Information	
	Consentement	
	Droit d'opposition	
	Droit d'accès	

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

	Libellé	Objectif
	Droit de rectification	
	Transferts	
	Formalités	
Risques	Accès illégitime aux DCP	
	Modification non désirée des DCP	
	Disparition des DCP	

Base de connaissances : typologie d'objectifs pour traiter les risques

Des objectifs peuvent être fixés en fonction du niveau des risques, par exemple :

1. pour les risques dont la gravité et la vraisemblance sont élevées[19] : ces risques devraient absolument être évités ou réduits par l'application de mesures de sécurité diminuant leur gravité et leur vraisemblance. Dans l'idéal, il conviendrait même de s'assurer qu'ils sont traités à la fois par des mesures indépendantes de prévention (actions avant le sinistre), de protection (actions pendant le sinistre) et de récupération (actions après le sinistre) ;

2. pour les risques dont la gravité est élevée, mais la vraisemblance faible[20] : ces risques devraient être évités ou réduits par l'application de mesures de sécurité diminuant leur gravité ou leur vraisemblance. Les mesures de prévention devraient être privilégiées. Ils peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur gravité et si leur vraisemblance est négligeable ;

3. pour les risques dont la gravité est faible mais la vraisemblance élevée : ces risques devraient être réduits par l'application de mesures de sécurité diminuant leur vraisemblance. Les mesures de récupération devraient être privilégiées. Ils peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur vraisemblance et si leur gravité est négligeable ;

4. pour les risques dont la gravité et la vraisemblance sont faibles : ces risques devraient pouvoir être pris, d'autant plus que le traitement des autres risques devrait également contribuer à leur traitement.

Notes

- Les risques peuvent généralement être réduits, transférés ou pris. Toutefois, certains risques ne peuvent l'être, notamment lorsque des données sensibles sont traitées ou quand les préjudices dont peuvent être victimes les personnes concernées sont très importants. Dans de tels cas, il pourra s'avérer nécessaire de les éviter, par exemple en ne mettant pas en œuvre tout ou partie d'un traitement.

[19] Niveaux 3. Important et 4. Maximal.
[20] Niveaux 1. Négligeable et 2. Limité.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.

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

Modèle : formalisation du plan d'action

Le tableau suivant peut être utilisé pour élaborer le plan d'action et suivre sa mise en œuvre :

Mesure	Responsable	Difficulté	Coût financier	Terme	Avancement

Base de connaissances : échelles pour le plan d'action

Les échelles suivantes peuvent être utilisées pour élaborer le plan d'action et suivre sa mise en œuvre :

Critère	Niveau 1	Niveau 2	Niveau 3
Difficulté	Faible	Moyenne	Élevée
Coût financier	Nul	Moyen	Important
Terme	Trimestre	Année	3 ans
Avancement	Non démarré	En cours	Terminé

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

Modèle : formalisation de la validation

La formule suivante illustre une manière de réaliser la validation formelle du PIA :

Validation du PIA	Le [date], [identité ou fonction] valide le PIA au vu de l'étude réalisée et du rapport de PIA. Le traitement doit permettre de [synthèse des enjeux]. La manière dont il est prévu de mettre en œuvre les mesures de nature juridique et de traiter les risques est en effet jugée acceptable au regard de ces enjeux. La mise en œuvre du plan d'action devra être démontrée, ainsi que l'amélioration continue du PIA. [Signature]

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés.