Analyse d'impact relative à la protection des données

Privacy Impact Assessment (PIA)

LES MODÈLES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Édition février 2018

Table des matières

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Avant-propos

La méthode de la CNIL est composée de trois guides, décrivant respectivement la démarche, des modèles utiles pour formaliser l'étude et des bases de connaissances (un catalogue de mesures destinées à respecter les exigences légales et à traiter les risques, et des exemples) utiles pour mener l'étude :

Ils sont téléchargeables sur le site de la CNIL :

https://www.cnil.fr/fr/PIA-privacy-impact-assessment

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

- le terme « **vie privée** » est employé comme raccourci pour évoquer l'ensemble des libertés et droits fondamentaux (notamment ceux évoqués dans le [RGPD], par les articles 7 et 8 de la [Charte-UE] 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), analyse d'impact relative à la protection des données, et *Data Protection Impact Assessment* (DPIA) ;
- les libellés entre crochets ([libellé]) correspondent aux références bibliographiques.

Attention : les bases de connaissances présentées 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.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

1 Modèles utiles à l'étude du contexte

1.1 Vue d'ensemble

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

Description du traitement[1]	
Finalités du traitement	
Enjeux du traitement	
Responsable du traitement	
Sous-traitant(s)	

Recensement des référentiels applicables au traitement[2]

Référentiels applicables au traitement	Prise en compte

1.2 Données, processus et supports

Description des données, destinataires et durées de conservation

Données	Destinataires	Durées de conservation

Description des processus et supports

[insérer un schéma des flux de données et la description détaillée des processus mis en œuvre]

Processus	Description détaillée du processus	Supports des données concernés

[1] Sa nature, sa portée, son contexte, *etc.*
[2] Voir article 35 (8) du [RGPD].

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

2 Modèles utiles à l'étude des principes fondamentaux

2.1 Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement

Explication et justification des finalités

Finalités	Légitimité

Explication et justification du fondement

Critères de licéité	Applicable	Justification
La personne concernée a consenti[3] au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques		
Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci		
Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis		
Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique		
Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement		
Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant[4]		

[3] Concernant le recueil du consentement de la personne et son information, voir le 2.2.
[4] Ce point ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Explication et justification de la minimisation des données

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation

Explication et justification de la qualité des données

Mesures pour la qualité des données	Justification

Explication et justification des durées de conservation

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Données courantes			
Données archivées			
Traces fonctionnelles			
Journaux techniques (logs)			

Évaluation des mesures

Mesures garantissant la proportionnalité et la nécessité du traitement	Acceptable / améliorable ?	Mesures correctives
Finalités : déterminées, explicites et légitimes		
Fondement : licéité du traitement, interdiction du détournement de finalité		
Minimisation des données : adéquates, pertinentes et limitées		
Qualité des données : exactes et tenues à jour		
Durées de conservation : limitées		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

2.2 Évaluation des mesures protectrices des droits des personnes des personnes concernées

Détermination et description des mesures pour l'information des personnes

Si le traitement bénéficie d'une exemption au droit d'information, prévue par l'article 32 de la [Loi-I&L] et les articles 12, 13 et 14 du [RGPD] :

Dispense d'information des personnes concernées	Justification

Dans le cas contraire :

Mesures pour le droit à l'information	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
Présentation des conditions d'utilisation/confidentialité		
Possibilité d'accéder aux conditions d'utilisation/confidentialité		
Conditions lisibles et compréhensibles		
Existence de clauses spécifiques au dispositif		
Présentation détaillée des finalités des traitements de données (objectifs précis, croisements de données s'il y a lieu, etc.)		
Présentation détaillée des données personnelles collectées		
Présentation des éventuels accès à des identifiants de l'appareil, en précisant si ces identifiants sont communiqués à des tiers		
Présentation des droits de la personne concernée (retrait du consentement, suppression de données, etc.)		
Information sur le mode de stockage sécurisé des données, notamment en cas d'externalisation		
Modalités de contact de l'entreprise (identité et coordonnées) pour les questions de confidentialité		
Le cas échéant, information de la personne concernée de tout changement concernant les données collectées, les finalités, les clauses de confidentialité		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures pour le droit à l'information	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
Dans le cas de transmission de données à des tiers :		
- présentation détaillée des finalités de transmission à des tiers		
- présentation détaillée des données personnelles transmises		
- indication de l'identité des entreprises tierces		

Détermination et description des mesures pour le recueil du consentement[5]

Mesures pour le recueil du consentement	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
Consentement exprès à l'inscription		
Consentement segmenté par catégorie de données ou types de traitement		
Consentement exprès avant le partage de données avec des tiers		
Consentement présenté de manière compréhensible et adapté à la personne cible (notamment pour les enfants)		
Recueil du consentement des parents pour les mineurs de moins de 13 ans		
Pour une nouvelle personne, mise en œuvre d'un nouveau recueil de consentement		
Après une longue période sans utilisation, demande à la personne concernée de réaffirmer son consentement		
Si l'utilisateur a consenti au traitement de données particulières (par ex. sa localisation), l'interface signale clairement que ce traitement a lieu (icône, voyant lumineux)		
Si l'utilisateur change de contrat, les paramètres liés à son consentement sont maintenus		

Détermination et description des mesures pour les droits d'accès et à la portabilité

[5] Si la licéité du traitement repose sur le consentement.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Si le traitement bénéficie d'une exemption au droit d'accès, prévue par les articles 39 et 41 de la loi [Loi-I&L] et les articles 15 et 20 du [RGPD] :

Exemption du droit d'accès	Justification	Modalités de réponse aux personnes concernées

Dans le cas contraire :

Mesures pour le droit d'accès	Données internes	Données externes	Justification
Possibilité d'accéder à l'ensemble des données personnelles de l'utilisateur, via les interfaces courantes			
Possibilité de consulter, de manière sécurisée, les traces d'utilisation liées à la personne concernée			
Possibilité de télécharger une archive de l'ensemble des données à caractère personnel liées à la personne concernée			

Enfin, quand le droit à la portabilité est applicable au traitement prévu par l'article 20 du [RGPD] :

Mesures pour le droit à la portabilité	Données internes	Données externes	Justification
Possibilité de récupérer, sous une forme aisément réutilisable, les données personnelles qui ont été fournies par la personne concernée, afin de pouvoir les transférer à un service tiers			

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Détermination et description des mesures pour les droits de rectification et d'effacement

Si le traitement bénéficie d'une exemption au droit de rectification et d'effacement, prévue par l'article 41 de la [Loi-I&L] et l'article 17 du [RGPD] :

Exemption des droits de rectification et d'effacement	Justification	Modalités de réponse aux personnes concernées

Dans le cas contraire :

Mesures pour les droits de rectification et d'effacement	Données internes	Données externes	Justification
Possibilité de rectifier les données personnelles			
Possibilité de supprimer les données personnelles			
Indication des données personnelles qui seront conservées malgré tout (contraintes techniques, obligations légales, etc.)			
Mise en œuvre du droit à l'oubli pour les mineurs			
Indications claires et étapes simples pour effacer les données avant de mettre l'appareil au rebut			
Conseils fournis pour remise à zéro en cas de vente de l'appareil			
Possibilité d'effacer les données en cas de vol de l'appareil			

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Détermination et description des mesures pour les droits de limitation du traitement et d'opposition

Si le traitement bénéficie d'une exemption au droit de limitation et d'opposition, prévue par l'article 38 de la [Loi-I&L] ou l'article 21 du [RGPD] :

Exemption des droits de limitation et d'opposition	Justification	Modalités de réponse aux personnes concernées

Dans le cas contraire :

Mesures pour les droits de limitation et d'opposition	Données internes	Données externes	Justification
Existence de paramètres « Vie privée »			
Invitation à changer les paramètres par défaut			
Paramètres « Vie privée » accessibles pendant l'inscription			
Paramètres « Vie privée » accessibles après l'inscription			
Existence d'un dispositif de contrôle parental pour les enfants de moins de 13 ans			
Conformité en matière de traçage (Cookies, Publicité, etc.)			
Exclusion des enfants de moins de 13 ans des traitements de profilage automatisé			
Exclusion effective de traitement des données de l'utilisateur en cas de retrait du consentement			

Détermination et description des mesures pour la sous-traitance

Nom du sous-traitant	Finalité	Périmètre	Référence du contrat	Conformité art.28[6]

[6] Un contrat de sous-traitance doit être conclu avec chacun des sous-traitants, précisant l'ensemble des éléments prévus à l'art. 28 du [RGPD] : durée, périmètre, finalité, des instructions de traitement documentées, l'autorisation préalable en cas de recours à un sous-traitant, mise à disposition de toute documentation apportant la preuve du respect du [RGPD], notification immédiate de toute violation de données, *etc.*

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Détermination et description des mesures pour le transfert de données en dehors de l'Union européenne

Données	France	UE	Pays reconnu adéquat par l'UE	Autre pays	Justification et encadrement (clauses contractuelles types, règles internes d'entreprise)

Évaluation des mesures

Mesures protectrices des droits des personnes concernées	Acceptable / améliorable ?	Mesures correctives
Information des personnes concernées (traitement loyal et transparent)		
Recueil du consentement		
Exercice des droits d'accès et à la portabilité		
Exercice des droits de rectification et d'effacement		
Exercice des droits de limitation du traitement et d'opposition		
Sous-traitance : identifiée et contractualisée		
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

3 Modèles utiles à l'étude des risques liés à la sécurité des données

3.1 Évaluation des mesures

Description et évaluation des mesures contribuant à traiter des risques liés à la sécurité des données

Mesures portant spécifiquement sur les données du traitement	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
Chiffrement	[*Décrivez ici les moyens mis en œuvre pour assurer la confidentialité des données conservées (en base de données, dans des fichiers plats, les sauvegardes, etc.), ainsi que les modalités de gestion des clés de chiffrement (création, conservation, modification en cas de suspections de compromission, etc.).* *Détaillez les moyens de chiffrement employés pour les flux de données (VPN, TLS, etc.) mis en œuvre dans le traitement.*]		
Anonymisation	[*Indiquez ici si des mécanismes d'anonymisation sont mis en œuvre, lesquels et à quelle fin.*]		
Cloisonnement des données (par rapport au reste du système d'information)	[*Indiquez ici si un cloisonnement du traitement est prévu, et comment il est réalisé.*]		
Contrôle des accès logiques	[*Indiquez ici comment les profils utilisateurs sont définis et attribués.* *Précisez les moyens d'authentification mis en œuvre*[7]. *Le cas échéant, précisez les*		

[7] Voir la délibération de la CNIL n°2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures portant spécifiquement sur les données du traitement	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
	règles applicables aux mots de passe (longueur minimale, structure obligatoire, durée de validité, nombre de tentatives infructueuses avant blocage du compte, etc.).]		
Traçabilité (journalisation)	[*Indiquez ici si des événements sont journalisés et la durée de conservation de ces traces.*]		
Contrôle d'intégrité	[*Indiquez ici si des mécanismes de contrôle d'intégrité des données stockées sont mis en œuvre, lesquels et à quelle fin.* *Détaillez les mécanismes de contrôle d'intégrité employés sur les flux de données.*]		
Archivage	[*Décrivez ici le processus de gestion des archives (versement, stockage, consultation, etc.) relevant de votre responsabilité. Précisez les rôles en matière d'archivage (service producteur, service versant, etc.) et la politique d'archivage.* *Indiquez si les données sont susceptibles de relever des archives publiques.*]		
Sécurité des documents papier	[*Si des documents papiers contenant des données sont utilisés dans le cadre du traitement, indiquez ici comment ils sont imprimés, stockés, détruits et échangés.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Description et évaluation des mesures générales de sécurité

Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
Sécurité de l'exploitation	[*Décrivez ici comment les mises à jour des logiciels (systèmes d'exploitation, applications, etc.) et l'application des correctifs de sécurité sont réalisées.*]		
Lutte contre les logiciels malveillants	[*Précisez si un antivirus est installé et régulièrement mis à jour sur tous les postes.*]		
Gestion des postes de travail	[*Détaillez ici les mesures mises en œuvre sur les postes de travail (verrouillage automatique, pare-feu, etc.).*]		
Sécurité des sites web	[*Indiquez ici si les "recommandations pour la sécurisation des sites web" de l'ANSSI sont mises en œuvre.*]		
Sauvegardes	[*Indiquez ici comment les sauvegardes sont gérées. Précisez si elles sont stockées dans un endroit sûr.*]		
Maintenance	[*Décrivez ici comment est gérée la maintenance physique des équipements, et précisez si elle est sous-traitée.* *Indiquez si la maintenance à distance des applications est autorisée, et suivant quelles modalités.* *Précisez si les matériels défectueux sont gérés spécifiquement.*]		
Sécurité des canaux informatiques (réseaux)	[*Indiquez ici sur quel type de réseau le traitement est mis en œuvre (isolé, privé, ou Internet).* *Précisez quels système de pare-feu, sondes de*		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
	détection d'intrusion, ou autres dispositifs actifs ou passifs sont chargés d'assurer la sécurité du réseau.]		
Surveillance	[*Indiquez ici si une surveillance en temps réel du réseau local est mise en œuvre et avec quels moyens.* *Indiquez si un contrôle des configurations matérielles et logicielles est effectué et par quels moyens.*]		
Contrôle d'accès physique	[*Indiquez ici la manière dont est réalisé le contrôle d'accès physique aux locaux hébergeant le traitement (zonage, accompagnement des visiteurs, port de badge, portes verrouillées, etc.).* *Indiquez s'il existe des moyens d'alerte en cas d'effraction.*]		
Sécurité des matériels	[*Indiquez ici les mesures de sécurité physique des serveurs et des postes clients (stockage sécurisé, câbles de sécurité, filtres de confidentialité, effacement sécurisé avant mise au rebut, etc.).*]		
Éloignement des sources de risques	[*Indiquez ici si la zone d'implantation est sujette à des sinistres environnementaux (zone inondable, proximité d'industries chimiques, zone sismique ou volcanique, etc.)* *Précisez si la zone contient des produits dangereux.*]		
Protection contre les sources de risques non humaines	[*Décrivez ici les moyens de prévention, de détection et de lutte contre l'incendie.* *Le cas échéant, indiquez les*		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
	moyens de prévention de dégâts des eaux. *Précisez également les moyens de surveillance et de secours de l'alimentation électrique.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Description et évaluation des mesures organisationnelles (gouvernance)

Mesures organisationnelles (gouvernance)	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
Organisation	[*Indiquez si les rôles et responsabilités en matière de protection des données sont définis.* *Précisez si une personne est chargée de la mise en application des lois et règlements touchant à la protection de la vie privée.* *Précisez s'il existe un comité de suivi (ou équivalent) chargé des orientations et du suivi des actions concernant la protection de la vie privée.*]		
Politique (gestion des règles)	[*Indiquez ici s'il existe une charte informatique (ou équivalent) traitant de la protection des données et de la bonne utilisation des moyens informatiques.*]		
Gestion des risques	[*Indiquez ici si les risques que les traitements font peser sur la vie privée des personnes concernées sont étudiés pour les nouveaux traitements, si c'est systématique ou non, et le cas échéant, selon quelle méthode.* *Précisez s'il existe, au niveau de l'organisme, une cartographie des risques sur la vie privée.*]		
Gestion des projets	[*Indiquez ici si les tests des dispositifs sont réalisés sur des données fictives/anonymes.*]		
Gestion des incidents et des violations de données	[*Indiquez ici si les incidents font l'objet d'une gestion documentée et testée, notamment en ce qui concerne les violations de données à caractère personnel.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures organisationnelles (gouvernance)	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
Gestion des personnels	[*Indiquez ici les mesures de sensibilisation prises à l'arrivée d'une personne dans sa fonction.* *Indiquez les mesures prises au départ des personnes accédant aux données.*]		
Relations avec les tiers	[*Indiquez ici, notamment pour les sous-traitants amenés à avoir accès aux données, les modalités et les mesures de sécurité mises en œuvre pour ces accès.*]		
Supervision	[*Indiquez ici si l'effectivité et l'adéquation des mesures touchant à la vie privée sont contrôlées.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

3.2 Appréciation des risques : les atteintes potentielles à la vie privée

Analyse et estimation des risques

Risque	Principales sources de risques	Principales menaces	Principaux impacts potentiels	Principales mesures réduisant la gravité et la vraisemblance	Gravité	Vraisemblance
Accès illégitime à des données						
Modification non désirée de données						
Disparition de données						

Évaluation des risques

Risques	Acceptable / améliorable ?	Mesures correctives	Gravité résiduelle	Vraisemblance résiduelle
Accès illégitime à des données	[*L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.*]	[*Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.*]		
Modification non désirée de données	[*L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.*]	[*Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.*]		
Disparition de données	[*L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.*]	[*Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

4 Modèles utiles à la validation du PIA

4.1 Préparation des éléments utiles à la validation

Élaboration de la synthèse relative à la conformité au [RGPD] des mesures permettant de respecter les principes fondamentaux

Légende				
Symbole :	●●●	●○○	○●○	○○●
Signification :	Non applicable	Insatisfaisant	Amélioration prévue	Satisfaisant

Mesures permettant de respecter les principes fondamentaux	Évaluation
Mesures garantissant la proportionnalité et la nécessité du traitement	
Finalités : déterminées, explicites et légitimes	○○○
Fondement : licéité du traitement, interdiction du détournement de finalité	○○○
Minimisation des données : adéquates, pertinentes et limitées	○○○
Qualité des données : exactes et tenues à jour	○○○
Durées de conservation : limitées	○○○
Mesures protectrices des droits des personnes des personnes concernées	
Information des personnes concernées (traitement loyal et transparent)	○○○
Recueil du consentement	○○○
Exercice des droits d'accès et à la portabilité	○○○
Exercice des droits de rectification et d'effacement	○○○
Exercice des droits de limitation du traitement et d'opposition	○○○
Sous-traitance : identifiée et contractualisée	○○○
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne	○○○

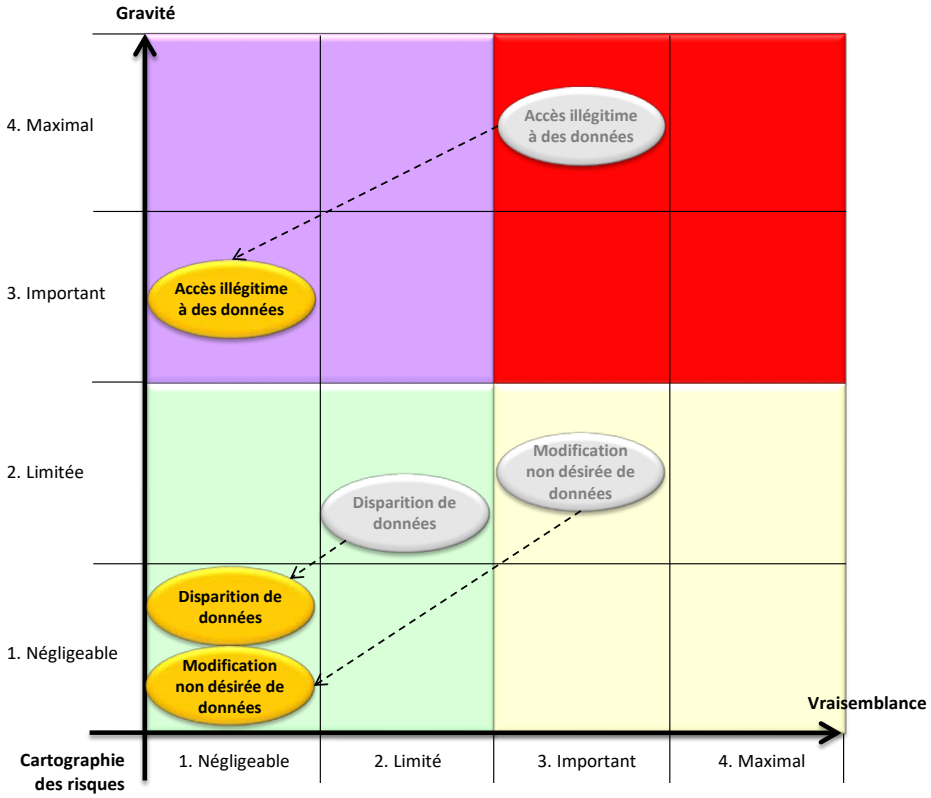
Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Élaboration de la synthèse relative à la conformité aux bonnes pratiques des mesures des mesures contribuant à traiter les risques liés à la sécurité des données

Mesures contribuant à traiter les risques liés à la sécurité des données	Évaluation
Mesures portant spécifiquement sur les données du traitement	
Chiffrement	○○○
Anonymisation	○○○
Cloisonnement des données (par rapport au reste du système d'information)	○○○
Contrôle des accès logiques des utilisateurs	○○○
Traçabilité (journalisation)	○○○
Contrôle d'intégrité	○○○
Archivage	○○○
Sécurité des documents papier	○○○
Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	
Sécurité de l'exploitation	○○○
Lutte contre les logiciels malveillants	○○○
Gestion des postes de travail	○○○
Sécurité des sites web	○○○
Sauvegardes	○○○
Maintenance	○○○
Sécurité des canaux informatiques (réseaux)	○○○
Surveillance	○○○
Contrôle d'accès physique	○○○
Sécurité des matériels	○○○
Éloignement des sources de risques	○○○
Protection contre les sources de risques non humaines	○○○
Mesures organisationnelles (gouvernance)	
Organisation	○○○
Politique (gestion des règles)	○○○
Gestion des risques	○○○
Gestion des projets	○○○
Gestion des incidents et des violations de données	○○○
Gestion des personnels	○○○
Relations avec les tiers	○○○
Supervision	○○○

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Élaboration de la cartographie des risques liés à la sécurité des données



Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Élaboration du plan d'action

Mesures complémentaires demandées	Responsable	Terme	Difficulté	Coût	Avancement

Formalisation du conseil de la personne en charge des aspects « Informatique et libertés »[8]

Le [jj/mm/aaaa], le délégué à la protection des données de [nom de l'organisme] a rendu l'avis suivant concernant la conformité du traitement et le PIA mené :

[Signature]

Formalisation de l'avis des personnes concernées ou de leurs représentants[9]

Les personnes concernées [ont/n'ont pas été] consultées [et ont émis l'avis suivant sur la conformité du traitement au vu du PIA mené] :

Justification de la décision du responsable de traitement :

[8] Voir l'article 35 (2) du [RGPD].
[9] Voir l'article 35 (9) du [RGPD].

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

4.2 Validation formelle

Formalisation de la validation

Le [jj/mm/aaaa], le [poste du responsable de traitement] de [nom de l'organisme] valide le PIA du traitement [nom du PIA], au vu du PIA mené, en sa qualité de responsable du traitement.

Le traitement a pour finalité de [rappel de la finalité du traitement].

Les mesures prévues pour respecter les principes fondamentaux de la protection de la vie privée et pour traiter les risques sur la vie privée des personnes concernées sont en effet jugées acceptables au regard de cet enjeu. La mise en œuvre des mesures complémentaires devra toutefois être démontrée, ainsi que l'amélioration continue du PIA.

[Signature]

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".