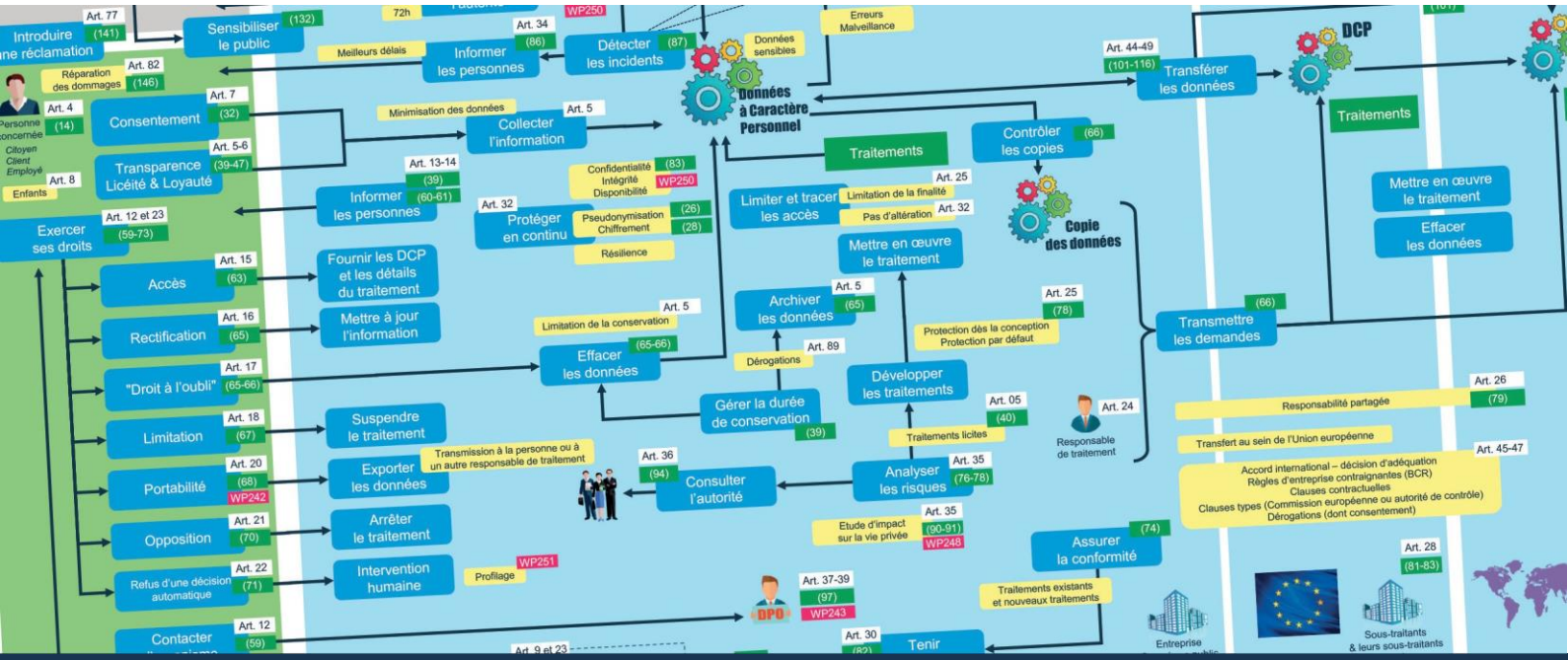
LES FICHES PRATIQUES du CLUSIF - RGPD



ANALYSE D'IMPACT

1. QU'EST'CE QU'UN PIA ?

L'acronyme « PIA » est utilisé indifféremment pour désigner Privacy Impact Assessment, étude d'impact sur la vie privée (EIVP), analyse d'impact relative à la protection des données (AIPD) ou encore Data Protection Impact Assessment (DPIA).
Il s'agit d'un processus dont l'objet est de décrire le traitement, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire face.
Un PIA est un processus qui vise à assurer la conformité aux règles et à pouvoir en apporter la preuve.

Une fois la description du traitement réalisée, le PIA repose sur deux piliers :

- L'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données, durées de conservation, information et droits des personnes, ...) non négociables, qui sont fixés par la loi et doivent être respectés, quelle que soit la nature, gravité et vraisemblance des risques ;
- L'étude, de nature plus technique, des risques sur la sécurité des données à caractère personnel (accès non autorisé, modification et disparition de données, et leurs impacts potentiels sur la vie privée) qui permet de déterminer les mesures techniques et d'organisation pour les protéger.

2. EST-IL OBLIGATOIRE ?

L'article 35 précise que, lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable de traitement doit effectuer un PIA préalablement à la mise en service du traitement.
Cette obligation est précisée par les lignes directrices relatives aux PIA (*WP248*) qui stipulent qu'il est obligatoire lorsque le traitement envisagé concerne **au moins deux des neuf critères suivants** :

1. **Évaluation ou notation** notamment d'aspects des personnes relatifs à leur :
   - Performance au travail ;
   - Situation économique ;
   - Santé ;
   - Centres d'intérêt et préférences personnelles ;
   - Fiabilité ou comportement ;
   - Localisation ou mouvements.
2. **Prise de décision automatisée** avec effet juridique ou similaire significatif : traitement ayant pour finalité la prise de décisions à l'égard des personnes concernées produisant *des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.*
3. **Surveillance automatique** : traitement utilisé pour observer, surveiller ou contrôler les personnes concernées, y compris la collecte de données via des réseaux ou par « *la surveillance systématique […] d'une zone accessible au public.* »
4. **Données sensibles** ou données à caractère hautement personnel incluant, en plus de l'article 9 (données génétiques, de santé, origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, l'appartenance syndicale, etc.) des données :
   - De communications électroniques ;
   - De localisation ;
   - Financières (permettant des paiements frauduleux) ;
   - Les documents personnels, les courriers électroniques, les agendas ainsi que les informations à caractère très personnel contenues dans les applications de « life-logging »…
5. Données traitées à grande échelle du fait de :
   - Un grand nombre de personnes concernées ou forte proportion de la population concernée ;
   - Une grande quantité de données ;
   - La durée ou la permanence du traitement ;
   - L'étendue géographique de ce traitement.
6. **Données croisées** ou combinées en provenance de deux ou plus traitements opérés pour des fins différentes ou par des RT différents.
7. **Données concernant une population vulnérable** dont, les enfants, les personnes dont le jugement est altéré et les employés qui ne pourraient s'opposer au traitement de leurs données.
8. **Usage innovant de technologies** comme la combinaison d'empreintes digitales et de reconnaissance faciale pour améliorer le contrôle d'accès physique : par exemple certaines applications de l'internet des objets qui impactent la vie quotidienne ou la protection des données privées.
9. **Traitement empêchant** la personne concernée **d'exercer un droit** ou de bénéficier d'un service ou d'un contrat.

Les lignes directrices contiennent un certain nombre d'exemples sur la façon dont il convient d'utiliser ces critères. Toutefois un PIA peut être nécessaire même si un seul de ces neuf critères est observé.

3. QUELLE ALTERNATIVE AU PIA ?

Si un RT estime que le PIA n'est pas requis, il devrait faire valider sa position par le DPO, ou du moins recueillir son avis.

Des listes de finalités pour lesquelles un PIA est obligatoire ou au contraire inutile (liste blanche / liste noire) seront publiées par les autorités de contrôle.

Lorsque le traitement est très similaire en termes de nature, de portée, de contexte et de finalités à un autre traitement qui a fait l'objet d'un PIA, les résultats du PIA réalisé pour le traitement similaire peuvent être utilisés.

Le fait de ne pas effectuer de PIA alors que le traitement est soumis à l'obligation d'une telle analyse, de la réaliser d'une manière incorrecte ou de ne pas consulter l'autorité de contrôle compétente lorsque la situation l'exige, est passible d'une amende administrative. Celle-ci peut s'élever à 10 000 000 € ou, dans le cas d'une entreprise, à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

4. QUI RÉALISE LE PIA ?

La responsabilité de veiller à ce qu'un PIA soit effectué incombe au RT. Le PIA peut être réalisé par quelqu'un d'autre, à l'intérieur ou à l'extérieur de l'organisation mais le RT reste responsable en dernier ressort de cette tâche. Le RT est également tenu de demander l'avis du DPO, si un tel délégué a été désigné.

Il convient que le PIA documente les conseils ainsi recueillis (représentant du personnel, cellule sécurité du SI, juridique…), l'avis du DPO, et les décisions prises par le RT.

Si le traitement est entièrement ou partiellement effectué par un sous-traitant, ce dernier doit aider le responsable du traitement à effectuer le PIA et fournir toutes les informations.

5. QUELS OUTILS ?

Le RGPD stipule qu'un PIA doit au moins contenir :

- *Une description systématique des opérations de traitement envisagées et des finalités du traitement* ;
- *Une évaluation de la nécessité et de la proportionnalité des opérations de traitement* ;
- *Une évaluation des risques pour les droits et libertés des personnes concernées* ;
- *Les mesures envisagées pour faire face aux risques et apporter la preuve du respect du règlement*.

Un PIA a pour objectif d'aider à gérer les risques pour les droits et libertés des personnes physiques en :

- Établissant le contexte : *compte tenu de la nature, de la portée, du contexte et des finalités du traitement et des sources du risque* ;
- Vérifiant le respect des principes fondamentaux : *proportionnalité, nécessité et mesures protectrices des droits* ;
- Appréciant le risque : *évaluer la probabilité et la gravité particulières du risque élevé* ;
- Traitant le risque : *atténuer ce risque et assurer la protection des données à caractère personnel, et démontrer le respect du présent règlement* ;

Il n'y a pas de formalisme obligatoire et la plupart des méthodes d'analyse de risque conviennent pour réaliser un PIA.

> ⓘ ***Du point de vue du RSSI***
>
> En fonction du secteur d'activité, plusieurs autres réglementations sont potentiellement à prendre en compte. Celles-ci sont prises en compte lors de l'étude du contexte.

En complément : La CNIL met à disposition sur son site un outil permettant de réaliser ces PIA[1]. Cet outil s'adresse principalement aux responsables de traitement moins familiers avec la démarche PIA.

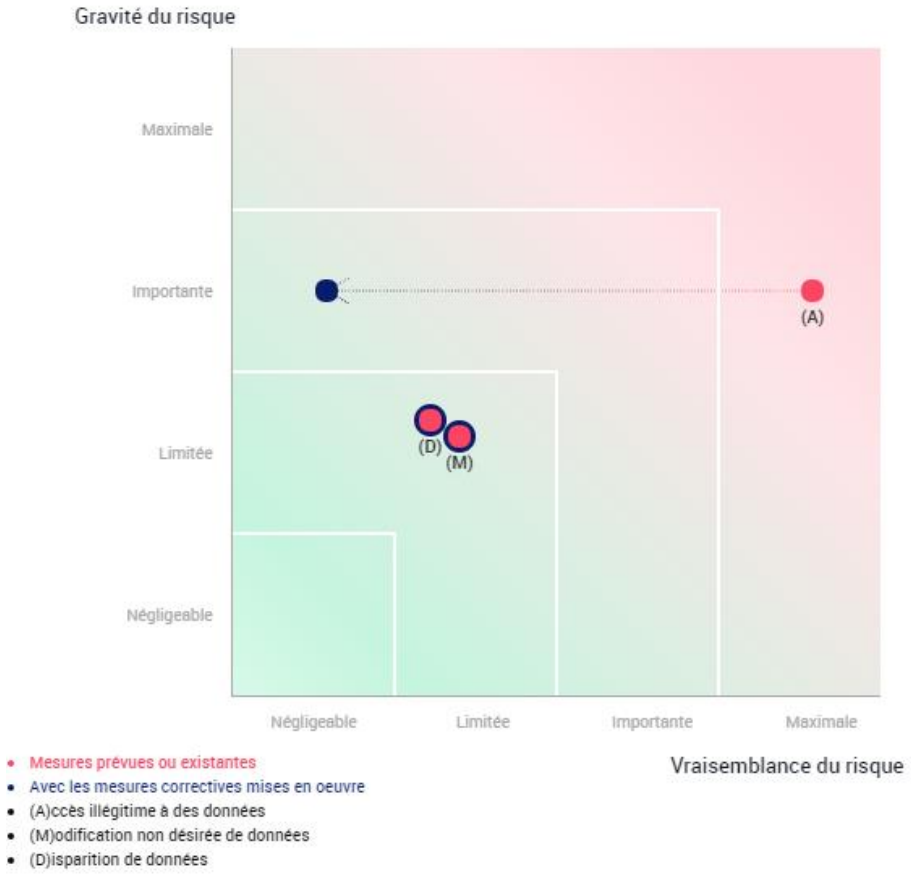


Figure 1 : Vue de la cartographie produite par l'outil PIA v1.6.3

6. QUELS LIENS AVEC LA DÉMARCHE D'ANALYSE DE RISQUES ?

Le PIA au sens du RGPD est un outil de gestion des risques pour les droits des personnes concernées et se place ainsi sous l'angle de leurs droits, comme c'est également le cas dans certains autres domaines tels que la sécurité sociétale, par exemple.

À l'inverse, dans d'autres domaines encore (par exemple la sécurité de l'information), la gestion des risques est axée sur l'organisation.

La méthode de raisonnement est donc commune, mais le référentiel de gravité doit être celui qui est spécifique aux données personnelles. Ce référentiel figure dans les documents PIA publiés par la CNIL.

[1] https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

L’échelle proposée dans ce guide est reproduite ci-après :

Échelle d'impact (PIA)				
Domaine	**1. Impact négligeable**	**2. Impact limité**	**3. Impact important**	**4. Impact maximal**
Impacts corporels	Absence de prise en charge adéquate d’une personne non autonome (mineur, personne sous tutelle)	Absence de prise en charge causant un préjudice minime ou affection physique mineure	Affection physique grave causant un préjudice à long terme ou altération de l’intégrité corporelle (à la suite d’une agression, d’un accident domestique, de travail, etc.)	Affection physique de longue durée ou permanente, décès (meurtre, suicide, accident mortel) ou altération définitive de l’intégrité physique
Impacts matériels	Perte de temps lors de démarches, réception de courriers non sollicités ou réutilisation de données publiées sur des sites Internet à des fins de publicité ciblée	Paiements non prévus, frais supplémentaires, défauts de paiement, élévation de coûts, refus d’accès à des services, promotion professionnelle manquée, publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel	Difficultés financières non temporaires, opportunités ciblées uniques et non récurrentes perdues, interdiction bancaire, dégradation de biens, perte de logement, perte d’emploi, séparation ou divorce, perte financière à la suite d’une escroquerie	Péril financier, dettes importantes, impossibilité de travailler, impossibilité de se reloger, perte de preuves dans le cadre d’un contentieux ou perte d’accès à une infrastructure vitale (eau, électricité)
Impacts moraux	Contrariété par rapport à l’information reçue ou demandée, sentiment d’atteinte à la vie privée sans préjudice réel (intrusion commerciale)	Affection psychologique mineure (diffamation, réputation), difficultés relationnelles avec l’entourage personnel ou professionnel (image, perte de reconnaissance)	Affection psychologique grave, 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, victime de chantage, cyberbullying et harcèlement moral	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

7. QUELLES SUITES ?

Lorsque le RT ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable (à savoir que les risques résiduels demeurent élevés), une consultation de l'autorité de contrôle est obligatoire.

Un risque résiduel peut notamment être considéré comme élevé et inacceptable dès lors qu'il exposerait les personnes à des conséquences importantes, voire irréversibles, qu'elles seraient susceptibles de ne pas pouvoir surmonter (par exemple : un accès illégitime à leurs données qui pourrait menacer leur vie, entraîner une mise à pied, mettre en péril leur situation financière) et/ou lorsqu'il semble évident que le risque se concrétisera (par exemple : dans la mesure où il n'est pas possible de réduire le nombre de personnes accédant aux données en raison de leurs modes de partage, d'utilisation ou de distribution, ou en présence d'une vulnérabilité bien connue non corrigée).

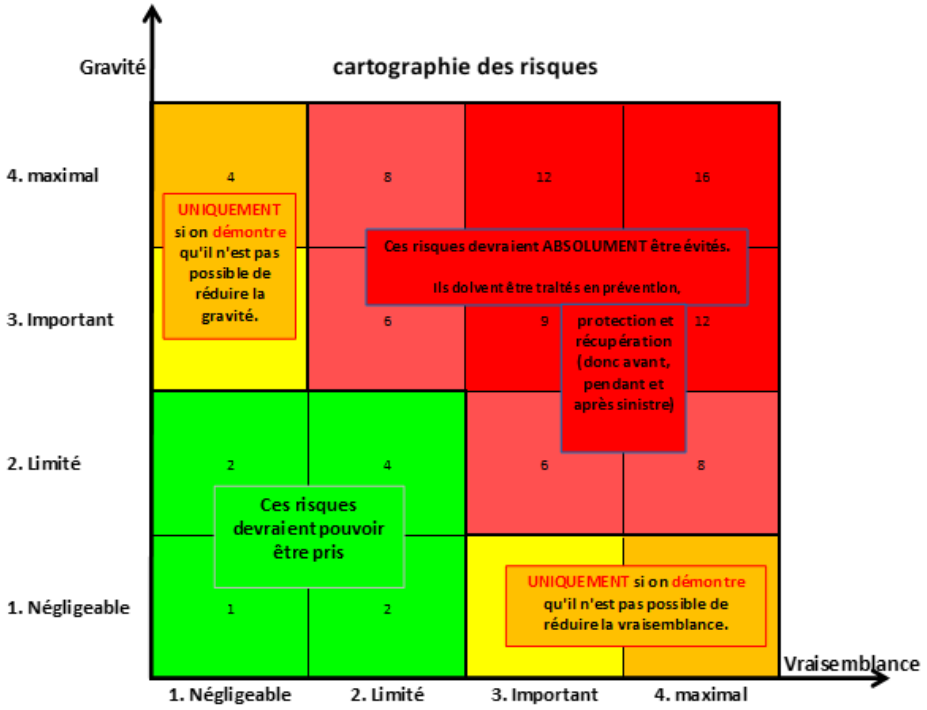


Figure 2 : Exemple de cartographie

Dans cet exemple, l'organisme n'a pas besoin de demander l'avis de l'autorité de contrôle (la CNIL en France) dans la zone verte du schéma. Dans le cas où la gravité est importante et la vraisemblance négligeable et dans le cas où la gravité est négligeable et la vraisemblance importante (les deux carrés jaunes du schéma), l'organisme doit sérieusement se poser la question d'un avis de la CNIL, mais dans la majorité des cas il devrait pouvoir autoriser le traitement. Dans les autres cas, l'avis de la CNIL est obligatoire.

Le RGPD ne fait pas obligation de publier le PIA. Cependant, une publication au moins partielle, sous la forme d'un résumé ou d'une conclusion de son PIA, devrait être envisagée par le responsable du traitement. Dans tous les cas, le PIA complet doit être communiqué à l'autorité de contrôle en cas de consultation préalable ou sur sa demande.

LES FICHES PRATIQUES

L'intégralité de la FAQ RGPD (version 2018) et la liste des membres qui ont contribué à son élaboration sont consultables sur le site du CLUSIF : **www.clusif.fr/publications**

CLUSIF