Jean-Marie Ferrières

RGPD – Conduite d'une analyse d'impact sur la protection des données (PIA)

Journée de formation CNEJITA du 19 juin 2018

Agenda

1 – Définitions

2 - Comment déterminer les traitements à risques élevés

3 – Ce que doit contenir un PIA

4 – Ressources

5 – PIA & Privacy by design

6 - PIA & Expertise

Article 35 du RGPD - Analyse d'impact relative à la protection des données

*« 1. Lorsqu'un type de traitement, en particulier par le recours à de **nouvelles technologies**, et compte tenu de la **nature**, de la **portée**, du **contexte** et des **finalités** du traitement, est susceptible d'engendrer un **risque élevé pour les droits et libertés des personnes physiques**, le responsable du traitement effectue, avant le traitement, une **analyse de l'impact** des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires. »*

1 - Définition

PIA = Privacy Impact Assessment ou **Analyse d'Impact relative à la protection des données**

Définition du PIA (*avis WP248 G29) :*

*« **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. »*

1 - Définition

PIA = processus qui assure que le traitement :

1) *prend en compte les obligations du **cycle de vie de la données***
   collecte → maintenance → conservation → destruction
2) *a été évalué au regard des **risques** en matière de vie privée*
3) *a été mis en place en prenant les **mesures** nécessaires pour réduire ou supprimer ces risques*

Ce processus doit être formalisé dans un document

Finalité du PIA = mettre en place des mesures pour contrer des risques qui ne sont pas toujours bien perçus par les responsable de traitement → une des difficultés est d'imaginer le pire

Le PIA fait référence aux certifications ISO : identifier les événement redoutés et réduire les risques

2 - Comment déterminer les traitements à risques élevés

Pour savoir si un traitement doit faire l'objet d'une étude d'impact :

- Art 35 RGPD
- Traitements soumis à autorisation préalable (biométrie, santé, listes noires, …)
- Avis du G29 (WP 248)
- Liste des traitements (CNIL)

Article 35 du RGPD - Analyse d'impact relative à la protection des données

*« 3. **L'analyse d'impact** relative à la protection des données visée au paragraphe 1 est, en particulier, **requise dans les cas suivants**:*

*a) l'**évaluation systématique et approfondie d'aspects personnels** concernant des personnes physiques, qui est fondée sur un **traitement automatisé**, y compris le **profilage,** et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;*

*b) le **traitement à grande échelle** de catégories particulières de données visées à l'article 9, paragraphe 1 (1), ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou*

*c) la **surveillance systématique à grande échelle d'une zone accessible au public**. »*

*« 4. L'autorité de contrôle établit et publie une **liste des types d'opérations de traitement** pour lesquelles une analyse d'impact relative à la protection des données est requise conformément au paragraphe 1. L'autorité de contrôle communique ces listes au comité visé à l'article 68. »*

(1) *origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques appartenance syndicale, données génétiques, biométriques, santé, vie sexuelle ou l'orientation sexuelle*

2 - Comment déterminer les traitements à risques élevés – Autorisations Préalables

Liste des traitements soumis à autorisation préalable

- **enregistrement de catégories de données suivantes :**
  - de données dites sensibles (*origine raciale ou ethnique ; opinion philosophique, politique, syndicale, ou religieuse ; vie sexuelle ou santé des personnes*),
  - de données biométriques, de données génétiques (*ADN*),
  - d'infractions, de condamnations ou mesures de sûreté,
  - le numéro de Sécurité sociale,
  - d'appréciations sur les difficultés sociales des personnes.

- **finalités spécifiques** :
  - enquêtes statistiques de l'INSEE,
  - traitements susceptibles d'exclure du bénéfice d'un droit, d'une prestation ou d'un contrat,
  - interconnexion de fichiers dont les finalités principales sont différentes ou correspondent à des intérêts publics différents,
  - traitements de recherche médicale et d'évaluation des pratiques de soins.

- **transferts de données hors de l'Union Européenne.**

2 -Comment déterminer les traitements à risques élevés – avis WP248

WP 248 : « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679 » (rév 01 – 4 oct 2017)

Une analyse d'impact est obligatoire quand les traitements qui remplissent au moins deux des critères suivants :

- évaluation/scoring (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ;
- collecte de données personnelles à large échelle (*nombre de personnes, volume de données, durée ou la permanence de l'activité de traitement de données; étendue géographique)* ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat (*ex : pour une banque, passer ses clients au crible d'une base de données de cote de crédit avant d'arrêter ses décisions d'octroi de prêt.)*

2 - Comment déterminer les traitements à risques élevés – CNIL

RGPD : « comment la CNIL vous accompagne dans cette période transitoire ? » (10 février 2018)

La CNIL travaille à l'élaboration de deux outils prévus par le RGPD :

- la liste des traitements obligatoirement soumis à analyse d'impact
- la liste des traitements pour lesquels, au contraire, aucune analyse n'est requise

3 -Ce que doit contenir un PIA

Article 35 du RGPD - Analyse d'impact relative à la protection des données

« 7. L'analyse contient au moins:

*a) une **description** systématique des opérations de traitement envisagées et des **finalités** du traitement, y compris, le cas échéant, l'**intérêt légitime** poursuivi par le responsable du traitement;*

*b) une évaluation de la nécessité et de la **proportionnalité des opérations de traitement au regard des finalités**;*

*c) une évaluation des **risques** pour les droits et libertés des personnes concernées conformément au paragraphe 1; et*

*d) les **mesures** envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées. »*

3 -Ce que doit contenir un PIA

Deux piliers :

→ **Juridique** : évaluation de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (*finalité, données et durées de conservation, information et droits des personnes, etc.)* non négociables, qui sont fixés par la loi et doivent être respectés, quelle que soit la nature, gravité et vraisemblance des risques ;

→ **Technique** : étude des risques sur la sécurité des données ➔déterminer les mesures techniques et d'organisation pour protéger les données.

Risque (ISO 31000) = « l'effet de l'incertitude sur l'atteinte des objectifs »

Risque (CNIL) sur la vie privée = scénario décrivant :

- un **événement redouté** (*accès non autorisé, modification non désirée ou disparition de données, et ses impacts potentiels sur les droits et libertés des personnes*) ;
- toutes les **menaces** qui permettraient qu'il survienne.

Il est estimé en termes de **gravité** et de **vraisemblance**. La gravité doit être évaluée pour les personnes concernées, et non pour l'organisme.

Le PIA doit être mené avant la mise en œuvre du traitement, et mis à jour régulièrement pour s'assurer que le niveau de risque reste acceptable

3 -Ce que doit contenir un PIA – les étapes

Les étapes - démarche CNIL – *(cf Etude de cas « Captoo ») :*

1 – contexte / registre des traitement (*description, finalités, enjeux, responsable/sous-traitants, référentiels, données/destinataires/durée, processus/support)*

2 –principes fondamentaux

- Évaluation des mesures garantissant la **proportionnalité** et la **nécessité du traitement (***justification des finalités et du fondement du traitement, de la minimisation et de l'exactitude des données, …)*
- Évaluation des mesures protectrices des **droits des personnes** *(information, consentement, accès, portabilité, rectification, droit à l'oubli, sous-traitance, transferts hors UE, …)*

3 – risques liés à la sécurité des données

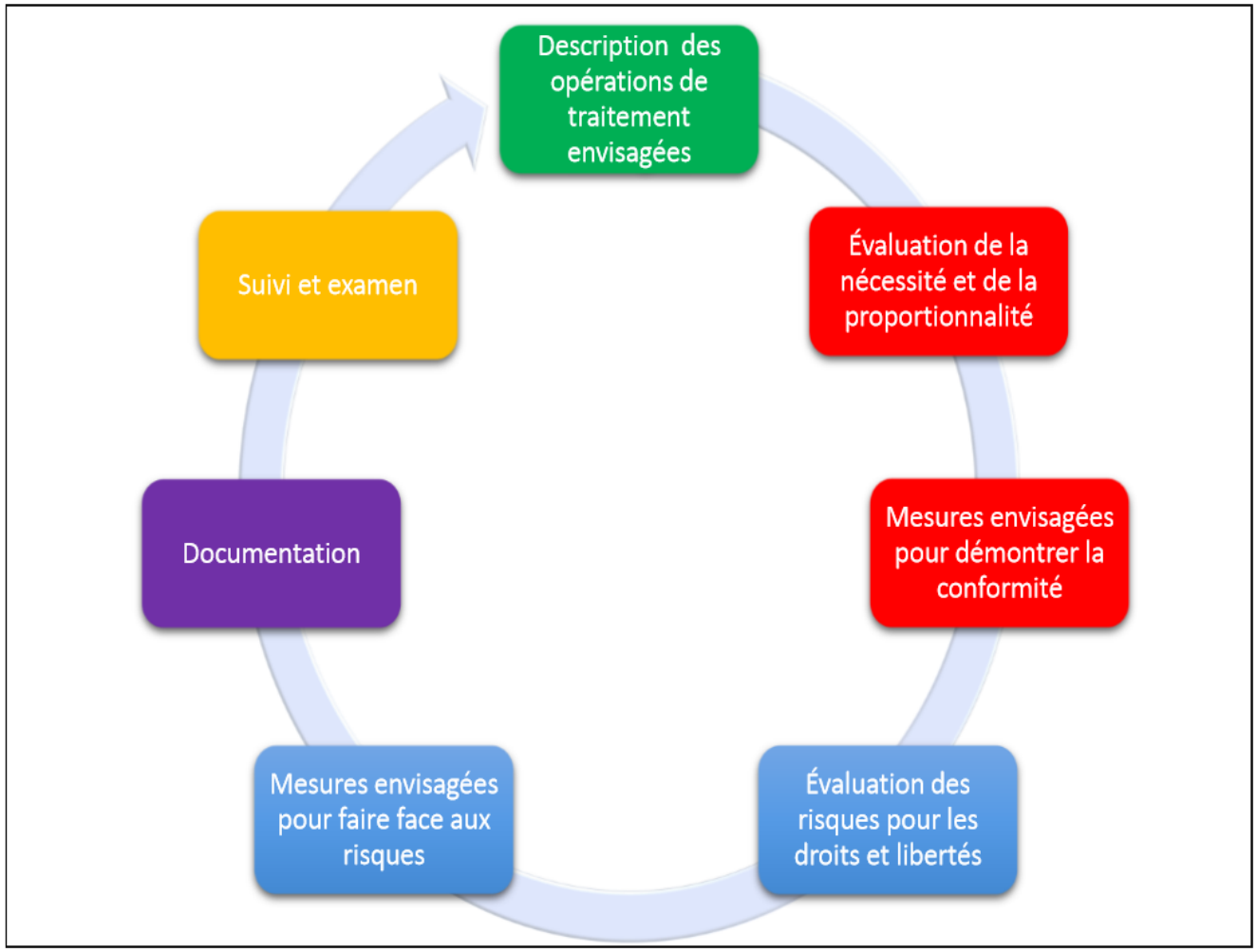
- Evaluation des mesures **techniques** *(chiffrement, anonymisation, accès, traçabilité, archivage, papier, sécurité informatique)* et **organisationnelles** *(rôles, personnels, gestion des incidents et violation, …)*
- Appréciation des risques d'**atteinte potentielle à la vie privée : accès illégitimes, modification non désirées, disparation de données** *(impact, menace, source, mesures pour traiter les risques, évaluation de la gravité/vraisemblance des risques, et mesures correctrices pour réduire gravité et/ou vraisemblance)*

4 – Validation du PIA

- synthèse évaluation des mesures et des risques (● ● ● ●), cartographie des risques (gravité/vraisemblance) et plan d'action
- Validation formelle (avis du DPO)

3 -Ce que doit contenir un PIA – cycle d'amélioration

PIA ➔ cycle d'amélioration / risque résiduel



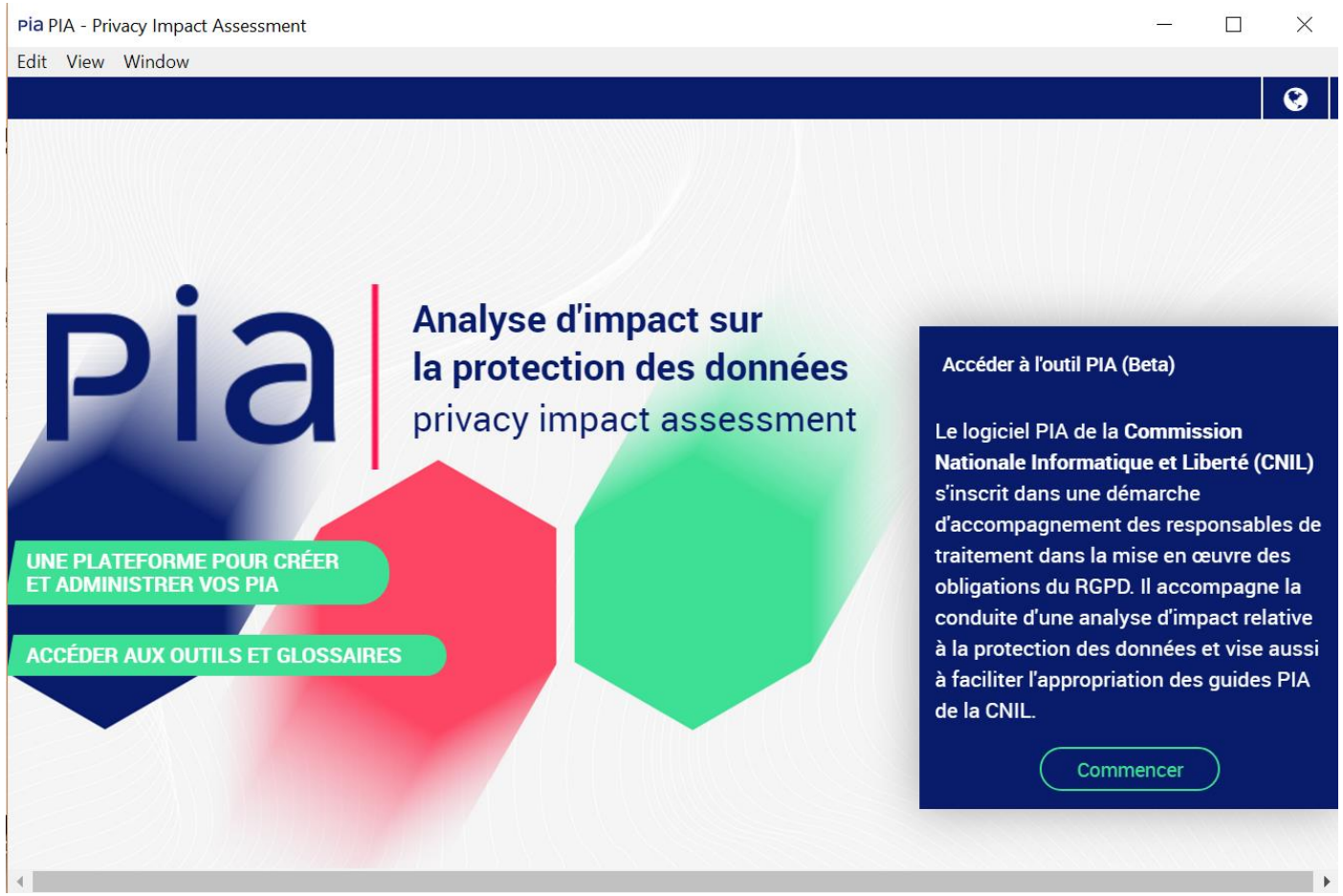
Avis WP248 du G29

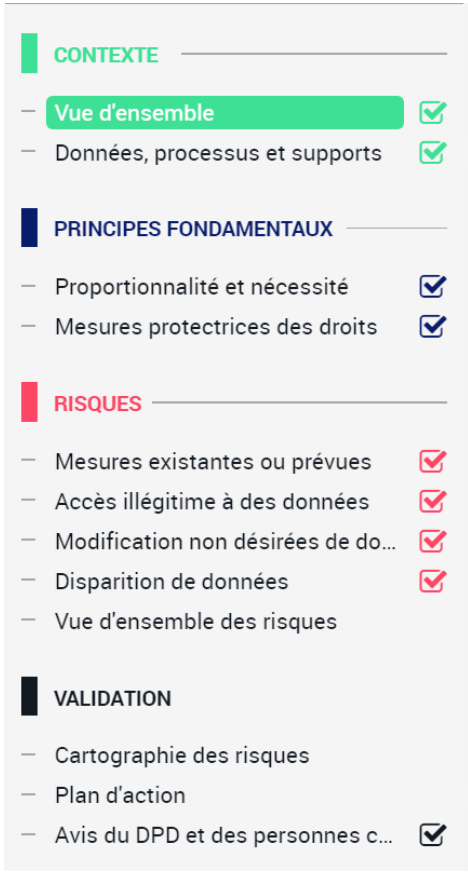
4 - Ressources – guides de la CNIL

Guides de la CNIL : *https://www.cnil.fr/fr/PIA-privacy-impact-assessment*

4 - Ressources – Logiciel de la CNIL

Logiciel open source : *https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil*





4 - Ressources – Logiciels de gestion de la conformité

Il existe de nombreux logiciels de gestion de la conformité couvrant :

- Le Registre des traitements
- Le PIA
- La traçabilité du consentement
- Le suivi des notifications des failles de sécurité
- Etc …

5 – PIA & Privacy by design

Le PIA, élément clé de la « **privacy by design** » est un outil essentiel pour minimiser les risques de vie privée et bâtir la confiance :

- identification des problèmes potentiels à un stade précoce
  → *corrections souvent plus simples et moins coûteuses*
- sensibilisation accrue à la protection de la vie privée et des données au sein d'une organisation
- se donner les moyens de respecter les obligations légales et de suivre la mise en œuvre des traitements

- limitation des actions intrusives dans la vie privée qui ont un impact négatif sur les individus

6 – PIA & Expertise

Dans les cas d'**atteintes aux données personnelles**, telles que :

- faille de sécurité,
- fuite de données
- détournement de finalités
- etc, …

Le PIA constitue un **référentiel de conformité** à prendre en compte par l'expert, en complément de ses investigations techniques, pour appréhender :

- le niveau de sécurité défini, prévu et convenu
- le niveau de sécurité atteint
- et constater les écarts

Merci