ANALYSE D'IMPACT

C’est quoi un PIA ?

Le *Privacy Impact Assessment* (PIA) — en français, « évaluations de l’impact sur la vie privée » ou AIPD pour « analyses d'impact relatives à la protection des données » — est une méthode conçue et validée par le groupe de travail Article 29 sur la protection des données , le groupe des autorités de contrôle sur les données personnelles européennes (ex. : la CNIL, en France), pour réaliser des analyses d'impact requises par le Règlement général sur la protection des données concernant la protection des données personnelles, appliqué depuis le 25 mai 2018 dans toute l'Union européenne.

1.Contexte

Cette section vous permet d'obtenir une vision claire du(des) traitement(s) de données à caractère personnel considéré(s).

Objectif : obtenir une vision claire des traitements de données personnelles.

1.1 Vue d'ensemble

- **Présenter le traitement considéré, sa nature, sa portée, son contexte, ses finalités et ses enjeux de manière synthétique.**
- **Identifier le responsable du traitement et les éventuels sous-traitants.**
- **Recenser les référentiels applicables au traitement, utiles ou à respecter, notamment les codes de conduite approuvés (cf. art. 40 du [RGPD]) et certifications en matière de protection des données (cf. art. 42 du [RGPD]).**

1.2 Données, processus et supports

Délimiter et décrire le périmètre de manière détaillée :

- **les données personnelles concernées, leurs destinataires et durées de conservation ;**
- **une description des processus et des supports de données pour l'ensemble du cycle de vie des données (depuis leur collecte jusqu'à leur effacement).**

2.Principes fondamentaux

Cette section vous permet de bâtir le dispositif de conformité aux principes de protection de la vie privée.

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

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

Expliciter et justifier les choix effectués pour respecter les exigences suivantes :

- **1. finalité(s) : déterminée, explicite et légitime (cf. art. 5.1 (b) du [RGPD]) ;**

- 2. fondement : licéité du traitement, interdiction du détournement de finalité (cf. art. 6 du [RGPD])11 ;
- 3. minimisation des données : adéquates, pertinentes et limitées (cf. art. 5.1 (c) du [RGPD])12 ;
- 4. qualité des données : exactes et tenues à jour (cf. art. 5.1 (d) du [RGPD]) ;
- 5. durées de conservation : limitées (cf. art. 5.1 (e) du [RGPD]).

Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer la manière dont chaque point est prévu, explicité et justifié, conformément au RGPD.

Le cas échéant, revoir leur description ou proposer des mesures complémentaires.

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

Identifier ou déterminer, et décrire, les mesures retenues (existantes ou prévues) pour respecter les exigences suivantes (nécessitant d'expliquer comment il est prévu de les mettre en œuvre) :

- 1. information des personnes concernées (traitement loyal et transparent, cf. art. 12, 13 et 14 du [RGPD]) ;

- 2. recueil du consentement, le cas échéant13 : exprès, démontrable, retirable (cf. art. 7 et 8 du [RGPD]) ;

- 3. exercice des droits d'accès et à la portabilité (cf. art. 15 et 20 du [RGPD]);

- 4. exercice des droits de rectification et d'effacement (cf. art. 16 et 17 du [RGPD])

- 5. exercice des droits de limitation du traitement et d'opposition (cf. art. 18 et 21 du [RGPD]) ;

- 6. sous-traitance : identifiée et contractualisée (cf. art. 28 du [RGPD]) ;

- 7. transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne (cf. art. 44 à 49 du [RGPD]). Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément au [RGPD]. Le

cas échéant, revoir leur description ou proposer des mesures complémentaires.

3.Risques

Cette section vous permet d'apprécier les risques sur la vie privée, compte tenu des mesures existantes ou prévues

Objectif : obtenir une bonne connaissance des mesures contribuant à la sécurité.

3.1 Évaluation des mesures existantes ou prévues

Identifier ou déterminer les mesures existantes ou prévues (déjà engagées), qui peuvent être de trois natures différentes :

1. **mesures portant spécifiquement sur les données du traitement : chiffrement, anonymisation, cloisonnement, contrôle d'accès, traçabilité, etc. ;**

2. **mesures générales de sécurité du système dans lequel le traitement est mis en œuvre : sécurité de l'exploitation, sauvegardes, sécurité des matériels, etc. ;**

3. **mesures organisationnelles (gouvernance) : politique, gestion des projets, gestion des personnels, gestion des incidents et violations, relations avec les tiers, etc.**

Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément aux bonnes pratiques de sécurité.

Le cas échéant, préciser leur description ou proposer des mesures complémentaires.

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

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

Pour chaque événement redouté (un accès illégitime à des données, une modification non désirée de données, et une disparition de données) :

- **1. déterminer les impacts potentiels sur la vie privée des personnes concernées s'ils survenaient ;**

- **2. estimer sa gravité, notamment en fonction du caractère préjudiciable des impacts potentiels et, le cas échéant, des mesures susceptibles de les modifier ;**
- **3. identifier les menaces sur les supports des données qui pourraient mener à cet événement redouté et les sources de risques qui pourraient en être à l'origine ;**
- **4. estimer sa vraisemblance, notamment en fonction des vulnérabilités des supports de données, des capacités des sources de risques à les exploiter et des mesures susceptibles de les modifier.**

Déterminer si les risques ainsi identifiés peuvent être jugés acceptables compte tenu des mesures existantes ou prévues.

Dans la négative, proposer des mesures complémentaires et ré-estimer le niveau de chacun des risques en tenant compte de celles-ci, afin de déterminer les risques résiduels.

4.Validation

Généralement réalisée par le responsable de traitement, avec l'aide d'une personne en charge des aspects « Informatique et libertés ».

Objectif : décider d'accepter ou non le PIA au regard des résultats de l'étude.

4.1 Préparation des éléments utiles à la validation

Consolider et mettre en forme les résultats de l'étude :

- **1. élaborer une représentation visuelle des mesures choisies pour respecter les principes fondamentaux, en fonction de leur conformité au [RGPD] (ex : à améliorer, ou jugé comme conforme) ;**

- **2. élaborer une représentation visuelle des mesures choisies pour contribuer à la sécurité des données, en fonction de leur conformité aux bonnes pratiques de sécurité (ex : à améliorer, ou jugé comme conforme) ;**

- **3. élaborer une cartographie visuelle des risques résiduels en fonction de leur gravité et vraisemblance ;**

- 4. élaborer un plan d'action à partir des mesures complémentaires identifiées lors des étapes précédentes : pour chaque mesure, déterminer au moins le responsable de sa mise en œuvre, son coût (financier et/ou en termes de charge) et son échéance prévisionnelle.

Formaliser la prise en compte des parties prenantes :

- 1. le conseil de la personne en charge des aspects « Informatique et libertés », si elle a été désignée (cf. art. 35 (2) du [RGPD]) ;

- 2. l'avis des personnes concernées ou de leurs représentants, le cas échéant (cf. art. 35 (9) du [RGPD]).

4.2 Validation formelle

Décider de l'acceptabilité des mesures choisies, des risques résiduels et du plan d'action, de manière argumentée, au regard des enjeux préalablement identifiés et de l'avis des parties prenantes. Le PIA peut ainsi être :

- 1. validé ;
- 2. à améliorer (expliquer en quoi) ;
- 3. refusé

Le cas échéant, revoir les étapes précédentes pour que le PIA puisse être validé.