GIDE

GIDE LOYRETTE NOUEL

Thème n° 5

Règlement Général sur la Protection des Données

Délégué à la protection des données (DPO) et Analyse d'impact (PIA)

16 mai 2018

Table des matières

DPO : Désignation – art. 37-1

Désignation obligatoire dans 3 hypothèses :

a)

- le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;

b)

- **les activités de base** du RT ou du ST consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique **à grande échelle** des personnes concernées ; ou

c)

- **les activités de base** du RT ou du ST consistent en un traitement **à grande échelle** de catégories particulières de données visées à l'article 9 et de DP relatives à des condamnations pénales et à des infractions visées à l'article 10.

DPO : Désignation – art. 37-1b) et c)

Notion « activités de base » du RT/ST

Considérant 97 : « les activités de base d'un RT ont trait à ses activités principales et ne concernent pas le traitement des données personnelles en tant qu'activité auxiliaire. »

Exemple des Guidelines

Banque

Activité de base : traitement des données bancaires de ses clients

Activité auxiliaire : traitement des données RH de ses salariés

DPO : Désignation – art. 37-1b) et c)

Notion de traitement à grande échelle

Recommandation du G29

- Nombre de personnes concernées
- Volume et étendue des données traitées
- Durée des activités de traitement
- Etendue géographique de l'activité de traitement

DPO : Désignation – art. 37

DPO du Sous-Traitant

Le ST, s'il remplit les conditions de l'article 37, doit nommer un DPO

Le DPO du ST supervise également les activités de traitement lorsque le ST agit en qualité de RT

- Traitements RH, fichier clients …

DPO : Désignation – art. 37

DPO au sein d'un groupe / DPO externalisé

37-2

- Un groupe d'entreprises peut désigner un seul DPO à condition qu'un DPO soit facilement joignable à partir de chaque lieu d'établissement.

37-6 Guidelines

- DPO externalisé sur la base d'**un contrat de service**. Si équipe DPO, prévoir des dispositions spécifiques.

DPO : Désignation – art. 37-5

Qualités professionnelles

37-5

- Le DPO est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir ses missions

Guidelines

- Il est nécessaire que les DPO disposent en particulier d'une expertise dans le domaine des législations et pratiques nationales et européennes en matière de protection des données, ainsi que d'une connaissance approfondie du RGPD

DPO : Fonction – art. 38-2

Moyens fournis par le RT/ST

RT/ST veillent à ce que le DPO soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données personnelles

RT/ST aident le DPO à exercer ses missions

en fournissant les ressources nécessaires pour exercer ces missions,

ainsi que l'accès aux données personnelles et aux opérations de traitement

et en lui permettant d'entretenir ses connaissances spécialisées.

DPO : Fonction – art. 38

Point de contact / secret professionnel

38-4

- **Les personnes concernées peuvent prendre contact avec le DPO au sujet de toutes les questions relatives au traitement de leurs DP et à l'exercice des droits que leur confère le RGPD**

38-5

- **Le DPO est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions**

DPO : Fonction – art. 38-6

Conflit d'intérêts - Guidelines

DPO ne peut exercer au sein de l'entreprise une fonction qui l'amène à déterminer les finalités et les moyens de traitements

- Analyse au cas par cas nécessaire / établissement de règles internes pour éviter les situations de conflit d'intérêts

Fonctions incompatibles selon le G29 :

- Fonction d'encadrement supérieur : DG, directeur opérationnel, directeur financier, DRH, directeur du service informatique
- Autres membres de ces directions : si déterminent les finalités et moyens de traitements
- Fonction impliquant la défense en justice du RT/ST

DPO : Fonction – art. 38-3

L'indépendance

Le RT/ST veillent à ce que le DPO ne reçoive aucune instruction en ce qui concerne l'exercice des missions.

Le DPO ne peut être relevé de ses fonctions ou pénalisé par le RT/ST pour l'exercice de ses missions.

- Ex: si DPO conseille un PIA et que le RT n'est pas d'accord, le DPO ne peut être sanctionné.
- Sont considérées comme sanctions par le G29 : absence de promotion, refus d'octroi d'avantages dont bénéficient d'autres salariés. Une simple menace suffit.

Le DPO fait directement rapport au niveau le plus élevé de la direction du RT/ST.

DPO : Missions – art. 39

a)

- Informer/conseiller RT/ST ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du RGPD et des autres règles en matière de protection des données

b)

- Contrôler le respect du RGPD, et des autres règles en matière de protection des données et des règles internes du RT/ST
  - y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant

DPO : Missions – art. 39

c)

- Dispenser des conseils sur demande en ce qui concerne l'analyse d'impact et vérifier l'exécution de celle-ci

d) et e)

- Coopérer avec l'autorité de contrôle ; faire office de point de contact pour l'autorité de contrôle sur les questions relatives aux traitements

Quelques recommandations sur le DPO

- Attention, nommer un DPO de manière facultative entraîne l'obligation de respecter toutes les dispositions relatives au DPO
- Rédaction d'une lettre de mission pour le DPO : **Exemple de lettre de mission d'un Délégué à la protection des données**
- Exigence de la CNIL : désignation du DPO sur le site de la CNIL par toutes les sociétés du groupe : Formulaire de désignation DPO
- Le DPO peut se voir confier la tenue du registre sous la responsabilité du RT/ST
- Possibilité d'utiliser des coordonnées génériques pour le DPO (ex : privacy@societe.com) même si des coordonnées nominatives doivent être transmises à la CNIL

PIA – art.35-3

Dans quels cas un PIA est-il obligatoire ?

a) l'évaluation systématique et approfondie d'aspects personnels concernant des PP, 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 PP 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, ou de DP 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.

PIA

Autres cas potentiels

Guidelines G29

- Croisement ou combinaison d'ensemble de données

Considérant 75

- Traitement portant sur des données relatives aux personnes vulnérables en particulier les enfants

Article 25 de la loi de 1978

- Traitements automatisés comportant des appréciations sur les difficultés sociales des personnes

PIA

Traitement pour lequel un PIA n'est pas requis

- N'est pas susceptible d'engendrer un risque élevé
- Est similaire et présente des risques similaires à un traitement pour lequel un PIA a déjà été effectué
- Est compris dans une liste d'exemptions publiée par l'Autorité
- Est fondé sur une obligation légale et un PIA a déjà été effectué lors de l'adoption de la base juridique en question

PIA

Les acteurs du PIA

35-1

- **Le responsable du traitement effectue le PIA**

35-2

- **Le RT demande conseil au DPO**

28-3 f) C.95

- **Le ST devra aider le RT si nécessaire et sur demande à assurer le respect des obligations découlant d'un PIA**

35-9

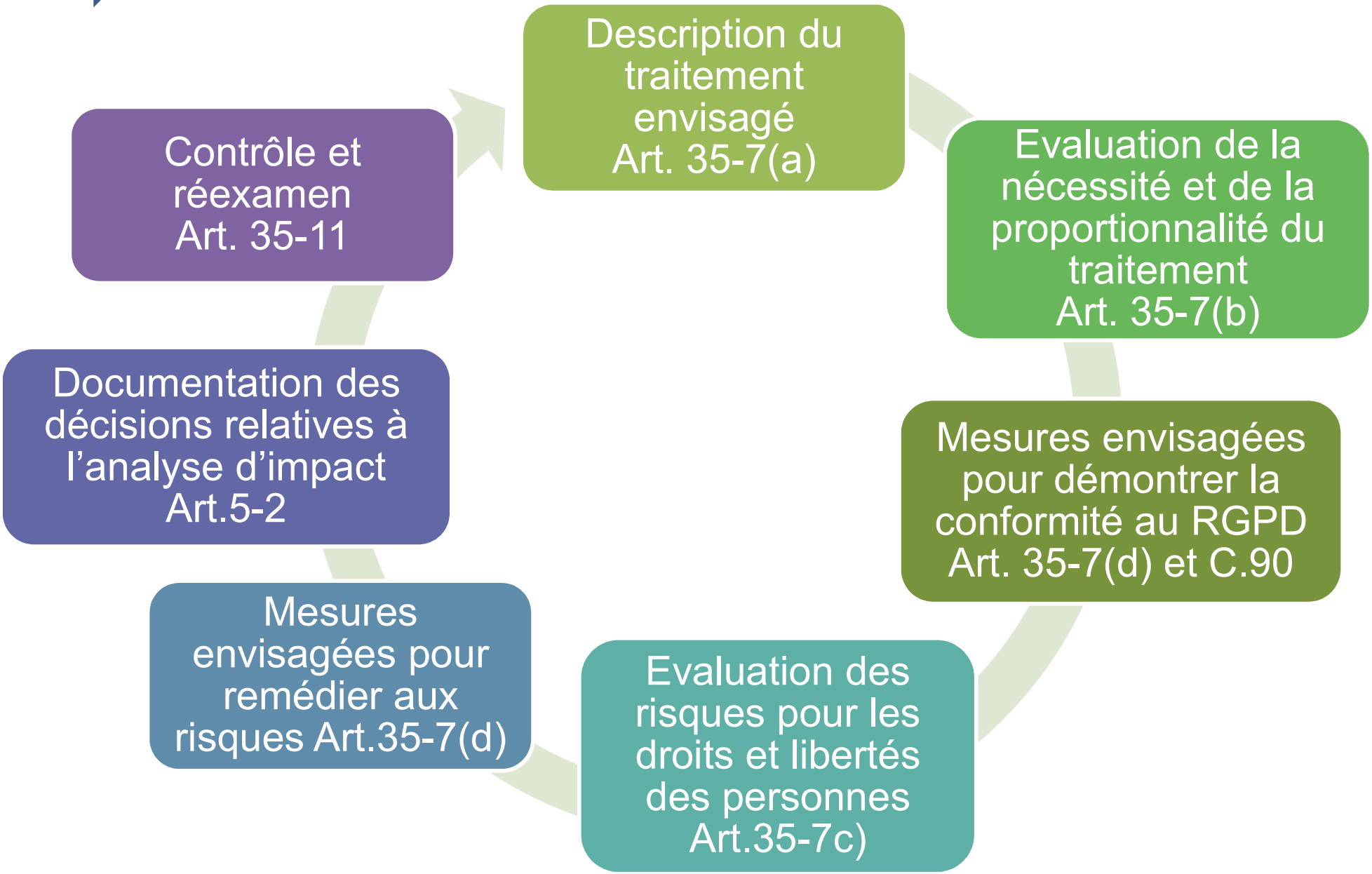
- **Le cas échéant, le RT demande l'avis des personnes concernées**

PIA

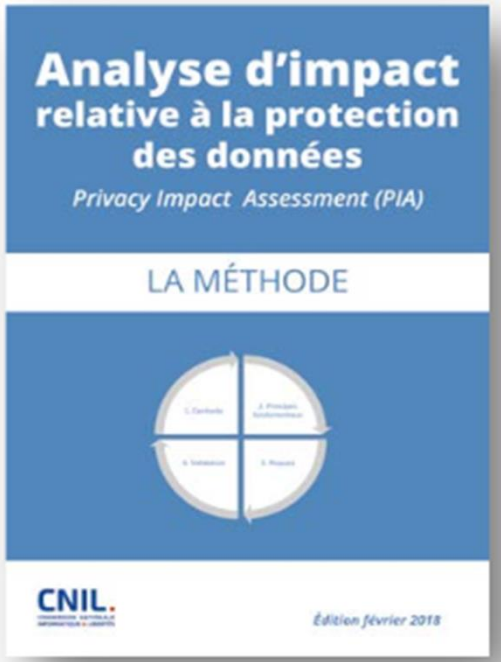
Modalités de la réalisation du PIA – Guidelines G29 et CNIL

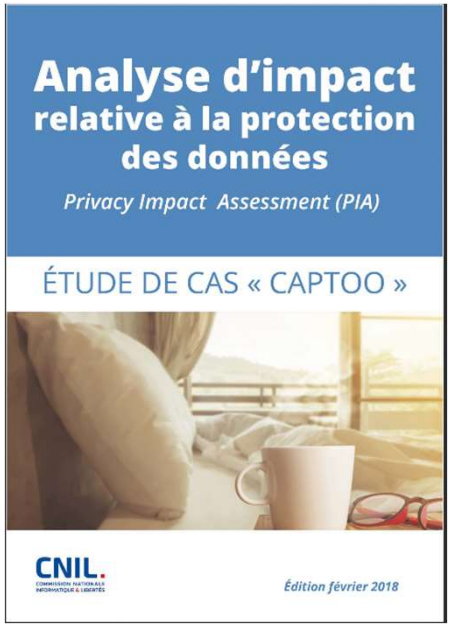
- Le PIA doit être réalisé préalablement à la mise en œuvre du traitement le plus tôt possible
- Le PIA devra faire l'objet de mises à jour et le RT devra mettre en place un mécanisme de suivi pour gérer dans le temps les revues et mises à jour des PIA déjà réalisés
- Pas de PIA requise pour les traitements qui ont déjà fait l'objet d'une formalité auprès de la CNIL avant le 25 mai 2018

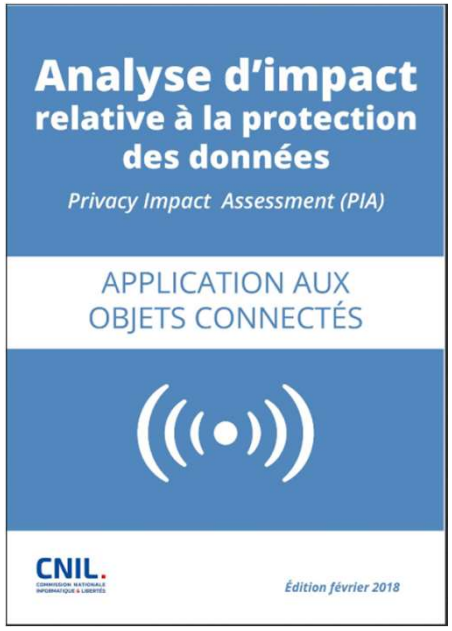
Comment mettre en place un PIA



Ressources CNIL







Logiciel de la CNIL

GIDE

GIDE LOYRETTE NOUEL

Merci pour votre attention

Questions / Réponses

Thierry Dor
dor@gide.com

François Vergne
f.vergne@gide.com

Gide Loyrette Nouel A.A.R.P.I.
22 cours Albert Ier
75008 Paris
tél. +33 (0)1 40 75 60 00
info@gide.com - gide.com