Ce qu'il faut savoir sur l’analyse d’impact relative à la protection des données (DPIA) . (document CNIL)

18 octobre 2017

L’article 35 du RGPD prévoit la conduite d’une analyse d’impact sur la protection des données (DPIA - Data Protection Impact Assessment), lorsqu‘un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

- Qu’est-ce qu’une analyse d’impact relative à la protection des données (DPIA) ?

L’analyse d’impact (DPIA) est un outil important pour la responsabilisation des organismes : elle les aide non seulement à construire des traitements de données respectueux de la vie privée, mais aussi à démontrer leur conformité au Règlement général sur la protection des données (RGPD). Elle est obligatoire pour les traitements susceptibles d’engendrer des risques élevés.

Une fois la description du traitement réalisée, le DPIA 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 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 ;
- **l’étude, de nature plus technique, des risques sur la sécurité des données** (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 protéger les données.

On note qu’analyse d’impact relative à la protection des données, DPIA (*Data Protection Impact Assessment*, terme retenu dans le RGPD) et PIA (*Privacy Impact Assessment*, terme plus commun utilisé dans d’autres régions du monde) sont synonymes.

- Qu’est-ce qu’un risque sur la vie privée ?

Un « risque sur la vie privée » est un 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.

Par exemple, un salarié soudoyé par un concurrent pourrait lui envoyer le fichier des adresses email des clients par courrier électronique. Si cela se produisait, les clients pourraient ensuite être sollicités et avoir un sentiment d'atteinte à la vie privée, des ennuis personnels ou professionnels, *etc*. Du point de vue « informatique et libertés », ce risque pourrait être estimé comme peu grave (conséquences peu importantes) et très vraisemblable (dans la mesure où ce scénario s'est déjà produit) par l'entreprise.

- Une analyse d'impact peut-elle porter sur un ou plusieurs traitements ?

Oui : Un DPIA peut concerner un seul traitement ou un ensemble de traitements similaires.

Par exemple :

- des collectivités qui mettent chacune en place un système de vidéosurveillance similaire pourraient effectuer une seule analyse qui porterait sur ce système bien que celui-ci soit ultérieurement mis en œuvre par des responsables de traitements distincts ;
- un opérateur ferroviaire (responsable de traitement unique) pourrait effectuer une seule analyse d'impact sur le dispositif de la surveillance vidéo déployé dans plusieurs gares.

En tant que bonne pratique, un DPIA peut également être mené par le fournisseur d'un produit matériel ou logiciel, pour évaluer l'impact sur la protection des données de son produit. Les différents responsables de traitement qui utilisent ensuite ce produit doivent mener leurs propres DPIA mais, le cas échéant, ceux-ci peuvent être alimentés par le DPIA du fournisseur du produit.

- uand est-ce qu'une analyse d'impact n'est pas obligatoire ?

Un DPIA n'est pas nécessaire dans les cas suivants :

- quand le traitement ne présente pas de risque élevé pour les droits et libertés des personnes concernées ;
- lorsque la nature, la portée, le contexte et les finalités du traitement envisagé sont très similaires à un traitement pour lequel un DPIA a déjà été mené ;
- quand le traitement répond à une obligation légale ou est nécessaire à l'exercice d'une mission de service public (art 6.1.c 6.1.e), sous réserve que les conditions suivantes soient remplies :

a) qu'il ait une base juridique dans le droit de l'UE ou le droit de l'État membre ;

b) que ce droit règlemente cette opération de traitement ;

c) et qu'un PIA ait déjà été menée lors de l'adoption de cette base juridique ;

- quand le traitement correspond à une exception déterminée par la CNIL conformément à l'article 35(5). La CNIL adoptera courant 2018 la liste de ces exceptions.

- Quand est-ce qu'une analyse d'impact est obligatoire ?

Un DPIA doit obligatoirement être mené quand le traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées* ».

Ainsi, généralement, les traitements qui remplissent au moins **deux des critères suivants** doivent faire l'objet d'une analyse d'impact :

- 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 ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, *etc*.) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

Exemple : une entreprise met en place un contrôle de l'activité de ses salariés, ce traitement remplit le critère de la surveillance systématique et celui des données concernant des personnes vulnérables donc la réalisation d'un DPIA sera nécessaire.

- À quel moment faut-il mener une analyse d'impact ?

Le DPIA doit être mené avant la mise en œuvre du traitement. Il doit être démarré le plus en amont possible et sera mise à jour tout au long du cycle de vie du traitement.

Il est également recommandé de revoir un DPIA de manière régulière pour s'assurer que le niveau de risque reste acceptable.

- Qui intervient dans la réalisation d'une analyse d'impact ?

Le **responsable de traitement** est tenu par l'obligation de s'assurer de la conformité de son traitement au RGPD.

S'il a désigné un **délégué à la protection des données**, il lui demande conseil et le charge de vérifier l'exécution du DPIA.

Si un **sous-traitant** intervient dans le traitement, il doit fournir son aide et les informations nécessaires à la réalisation du DPIA.

Le responsable de traitement devrait également demander l'avis **des personnes concernées** (par le biais d'une enquête, d'un sondage, d'une question formelle aux représentants du personnel), ou le justifier sinon.

Idéalement, les métiers (maîtrise d'ouvrage), les équipes chargées de la mise en œuvre (maîtrise d'œuvre), et la personne chargée de la sécurité des systèmes d'information devraient également participer au processus de réalisation du DPIA et à sa validation.

- Comment fait-on une analyse d'impact, existe-t-il une méthode pour faire une analyse d'impact?

Un DPIA contient à minima :

- une **description** systématique des **opérations de traitement** envisagées et les **finalités** du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;
- une **évaluation de la nécessité** et de la **proportionnalité** des opérations de traitement au regard des finalités;
- une **évaluation des risques** sur les droits et libertés des personnes concernées et ;
- 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 règlement.

Pour ce faire, **plusieurs méthodes sont utilisables**. Le responsable de traitement est libre de choisir sa méthode. Mais quelle que soit la méthode, celle-ci devrait respecter les critères définis dans l'annexe 2 des lignes directrices du G29.

Les guides DPIA de la CNIL (en cours de révision) décrivent la méthode suivante :

1. **délimiter et décrire le contexte** du (des) traitement(s) considéré(s) ;
2. **analyser les mesures** garantissant le respect des principes fondamentaux : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées ;
3. **apprécier les risques** sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités ;
4. **formaliser la validation** du PIA au regard des éléments précédents ou bien décider de réviser les étapes précédentes.

- Faut-il publier ou communiquer l'analyse d'impact ?

Il n'y a aucune obligation de publication. Toutefois, le DPIA peut aboutir à la production d'un rapport ou d'un résumé, pouvant être partagé, publié, communiqué. Cette bonne pratique contribue à améliorer la confiance entre les parties prenantes.

En outre, le DPIA doit être communiqué à la CNIL, dans son intégralité, en cas de consultation préalable (cf. article 36).

- Quand faut-il transmettre son analyse d'impact à la CNIL ?

Le DPIA doit être transmis à la CNIL dans les cas suivants :

- s'il apparait que le niveau de **risque résiduel** reste élevé (cas où la CNIL doit être consultée) ;
- quand la législation nationale d'un État membre l'exige ;
- en cas de contrôle par la CNIL.

- Quel est le montant des sanctions prévues par le règlement en cas de manquements aux dispositions relatives aux analyses d'impact ?

Le montant des amendes peut s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (art. 83(4)(a)).