

Fic 2016 : Etude d'impacts sur la vie privée : suivez la méthode de la CNIL

	Fic 2016 : Etude d'impacts sur la vie privée : Suivre la méthode de la CNIL
---	--

La CNIL publie sa méthode pour mener des PIA (Privacy Impact Assessment) pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits.

De l'application de bonnes pratiques de sécurité à une véritable mise en conformité

La Loi informatique et libertés (article 34), impose aux responsables de traitement de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données ».

Chaque responsable doit donc identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire.

Pour aider les TPE et PME dans cette étude, la CNIL a publié en 2010 un premier guide sécurité. Celui-ci présente sous forme de fiches thématiques les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement des données personnelles.

En juin 2012, la CNIL publiait un autre guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Il aidait les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.

Une méthode plus rapide, plus facile à appliquer et plus outillée

Ce guide a été révisé afin d'être plus en phase avec le projet de règlement européen sur la protection des données et les réflexions du G29 sur l'approche par les risques. Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs.

La CNIL propose ainsi une méthode encore plus efficace, qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la CNIL.

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :

les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;

la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.

Pour mettre en œuvre ces deux piliers, la démarche comprend 4 étapes :

- Étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
- Étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
- Étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
- Validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.

L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

Denis JACOPINI EST FORMATEUR EN ETUDE D'IMPACT SUR LA VIE PRIVÉE



Réagissez à cet article

Source : *Etude d'impacts sur la vie privée : suivez la méthode de la CNIL – CNIL – Commission nationale de l'informatique et des libertés*