INSTITUT DES CONSTRUCTEURS ET DES PROMOTEURS

Information PRO n°8 – le 12 mars 2018

RGPD : Règlement Général sur la Protection des Données

Le *RGPD* (ou GDPR) est le Règlement Général sur la Protection des Données, une nouvelle réglementation européenne qui entrera en vigueur le 25 mai 2018. Cette nouvelle loi a différents objectifs : Renforcer les droits des personnes / Responsabiliser les acteurs traitant des données / Crédibiliser la régulation.
L'entrée en vigueur du RGPD va affecter le fonctionnement des entreprises, si ce n'est déjà fait. En effet, avec ce nouveau règlement, les entreprises devront investir du temps et de l'argent dans la mise en place de divers mécanismes pour optimiser la protection des données personnelles qu'elles traitent.

L'une des plus grandes nouveautés apportées par le RGPD est l'obligation pour les entreprises de mener une analyse d'impact sur la protection des données (DPIA-Data Protection Impact Assessment) sur les traitements susceptibles de présenter un risque élevé pour les droits et libertés des personnes concernées.

L'analyse d'impact (DPIA) est l'une des notions les plus importantes du RGPD. C'est un outil important pour responsabiliser les organismes. Et pour cause, le DPIA peut grandement aider dans la mise en place des traitements de données plus respectueux de la vie privée. Pour les autorités de contrôle, elle sert à déterminer si un traitement est bien conforme au nouveau règlement sur la protection des données.
Le DPIA est obligatoire pour les traitements susceptibles d'engendrer des risques élevés pour la vie privée. Une fois que l'on a bien identifié le type de traitement, on pourra mener un DPIA.
L'analyse d'impact repose sur 2 grands piliers :
-Faire un rapprochement entre les principes fondamentaux du RGPD et les traitements effectués : finalités du traitement, durée de conservation des données, devoir d'information…
-Analyse des risques portant sur la sécurité des données (condition d'accès, disparition de données, impact sur la vie privée…), pour faciliter la mise en place de mesures techniques efficaces pour protéger les données.
Comment bien mener un DPIA ?
Le RGPD ne donne pas une méthode précise pour mener un DPIA. Mais si l'on s'en tient à l'esprit du règlement, un DPIA devrait au moins contenir :
-Une description des opérations de traitements (finalités, intérêt…) ;
-Une analyse de la nécessité et de la proportionnalité des opérations de traitements par rapport aux finalités ;
-Une analyse des risques sur les droits et libertés des cibles du traitement ;
-Une description des mesures de protection envisagées (mécanismes de sécurité et garanties de protection des données manipulées) ;

Les sanctions
En cas de manquement aux obligations relatives à l'analyse d'impact, des sanctions assez sévères sont prévues par le RGPD : une amende pouvant atteindre les 10 000 000 d'euros ou

les 2% du chiffre d'affaires de l'année précédente. Ce sera le montant le plus élevé qui sera retenu.

La CNIL a conçu un guide très précis et très pratique sur cette obligation nouvelle. Ce guide est en fichier joint à cette information PRO.