Délibération n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD)

11/10/2018

« Le règlement général sur la protection des données (RGPD) promeut le principe de responsabilisation des organismes, dont la mise en œuvre concrète repose notamment sur la réalisation d'analyses d'impact relatives à la protection des données (AIPD ou Privacy Impact Assessment - PIA) pour les traitements susceptibles d'engendrer un risque élevé pour les droits et les libertés des personnes.
En propos liminaires, la Commission nationale de l'informatique et des libertés rappelle l'importance des AIPD qui, au-delà de leur caractère obligatoire dans certaines hypothèses et des sanctions encourues en cas de méconnaissance de cette obligation, permettent à chaque responsable de traitement concerné d'identifier les garanties nécessaires afin d'assurer et de démontrer la conformité du traitement qu'il envisage de mettre en œuvre au regard des exigences du RGPD. Les AIPD sont avant tout l'occasion de mener une réflexion interne, spécifique à chaque traitement, de nature à garantir de manière opérationnelle le respect des principes relatifs à la protection des données et de pouvoir, le cas échéant, le démontrer.
La commission a donc souhaité accompagner les responsables de traitement dans cette démarche essentielle en leur proposant différents outils tels que des guides méthodologiques ainsi qu'un logiciel d'aide à la rédaction des AIPD, disponibles sur son site.
En complément de celles adoptées le 4 octobre 2017 au niveau européen par le groupe de travail « article 29 » (G29), et reprises à son compte par le Comité européen à la protection des données (CEPD) le 25 mai 2018, la commission a également estimé utile d'adopter des lignes directrices afin de préciser le périmètre de l'obligation d'effectuer une AIPD, les conditions de réalisation de celle-ci et, enfin, les cas dans lesquels une AIPD doit lui être transmise.
Les responsables de traitement concernés par la réalisation d'une AIPD pourront également se reporter aux référentiels sectoriels que la commission a adoptés afin, d'une part, d'évaluer la nécessité et la proportionnalité des opérations de traitement envisagées ou mises en œuvre et, d'autre part, d'identifier les garanties devant être apportées pour protéger les droits et libertés des personnes dont les données seront traitées. Ces référentiels pourront éclairer utilement les responsables de traitement sur les attentes de la commission.
La commission pourra par ailleurs, dans certains cas, donner à ces référentiels un effet juridique, en exonérant de la réalisation d'AIPD les responsables de traitement qui s'y conformeraient strictement. Chaque référentiel précisera les effets qui lui sont attachés (référentiel servant de simple aide à la rédaction des AIPD ; référentiel permettant d'être exonéré de la réalisation d'une AIPD). »