Obligations et responsabilités du sous-traitant au regard du RGPD

Définition du sous-traitant : il s'agit de la personne physique ou morale, l'autorité publique, le service ou un autre organisme, qui traite des données pour le compte du responsable de traitement (le client).

1 - Régime actuel selon la loi Informatique et Libertés (avant RGPD) :

Le responsable de traitement (votre client) est tenu 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. Ainsi, en qualité de sous-traitant, il ne doit agir que sur instructions du responsable du traitement et doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité des données.

En pratique, les parties prévoient (généralement mais pas toujours) par contrat le périmètre d'intervention et les obligations de chacun. Certains clients fournissent leurs exigences en matière de sécurité et exigent du sous-traitant la fourniture d'une politique de sécurité, la possibilité d'effectuer des audits, etc.

2 – Nouvelles obligations avec le RGPD :

Le sous-traitant ne doit agir que sur instruction du responsable du traitement. Il n'y a donc pas de grande révolution par rapport au régime précédent sur ce sujet.

Le sous-traitant doit présenter des garanties suffisantes et des mesures techniques et organisationnelles, notamment sur le terrain de la sécurité.

A titre d'exemple, le RGPD propose au sous-traitant d'adopter des codes de bonne conduite, de mettre en place un processus de certification, d'utiliser des outils de pseudonymisation ou de chiffrement de données robustes, proposer systématiquement des plans de sauvegarde, de réversibilité, etc. à ses clients.

La désignation d'un DPO pour le sous-traitant est, à ce titre, incontournable. L'obtention d'une certification par la CNIL est vivement conseillée.

S'il outrepasse ou ne respecte pas ces obligations ou les instructions du responsable du traitement, le sous-traitant sera susceptible d'engager sa propre responsabilité (ou conjointement avec le responsable de traitement) et être condamné au versement de dommages et intérêts par exemple.

Le RGPD exige du sous-traitant des engagements contractuels forts. Il devra par exemple s'engager par écrit à n'agir que sur instructions documentées du client, informer régulièrement son client, garantir la confidentialité et la sécurité des données, justifier des mesures organisationnelles et techniques prises, le cas échéant supprimer ou détruire les données, etc.

Il devra conclure des contrats prévoyant la nature, la durée l'objet, la finalité du traitement, le type de données, les catégories de personnes concernées, les obligations et droits du responsable du traitement.

Il ne pourra pas recruter un autre sous-traitant sans l'accord du responsable du traitement. Il met en œuvre des contrats avec ce sous-traitant conformes au RGPD.

Il ne pourra effectuer des transferts de données que sur instructions du responsable du traitement.

Il doit aider le responsable du traitement à se conformer au RGPD.

Il indique au responsable du traitement si ses instructions constituent une violation du RGPD.

Il met à la disposition du responsable du traitement les informations et la documentation en cas d'audit ou de contrôle de la CNIL.

Il agit pour faire en sorte que les personnes concernées voient leurs droits respectés (droit de modification, droit à l'oubli, droit de minimisation…).