Les obligations du sous-traitant

Qu’est-ce qu’un sous-traitant ?

Le sous-traitant traite des données personnelles pour le compte, sur instruction et sous l’autorité d’un responsable de traitement.

L’activité du sous-traitant peut porter sur une tâche précisément définie comme l’envoi de courrier ou plus étendue comme la gestion de la paie des salariés.

Qui est le sous-traitant ?

Est sous-traitant toute entreprise qui effectue le traitement de données personnelles comme une prestation ou un service pour un autre organisme. Ainsi, les sous-traitants sont aussi concernés par des obligations du RGPD.

On retrouve comme entreprise pouvant être sous-traitante :

- les prestataires de services informatiques (hébergement, maintenance,…),
- Les intégrateurs de logiciels (déploiement de PGI,...),
- Les sociétés de sécurité informatique,
- Les ESN (entreprises de service du numérique) ayant accès aux données traitées,
- Les agences de marketing ou de communication qui traitent les données personnelles du public de leurs clients

Quelles sont ses obligations ?

Le sous-traitant est co-responsable avec le responsable de traitement. Ils sont tous les deux soumis à des obligations du RGPD, qui sont complémentaires.

Le sous-traitant a *obligation d’assistance*. Il doit aider le responsable de traitement dans la pratique des obligations du RGPD.

Ainsi, le sous-traitant participe à l’étude d’impact (l’évaluation des risques des violations possibles des données personnelles), à la notification de violation de données (la CNIL devant être notifiée par le responsable de traitement quand des données personnelles détenues par une entreprise sont violées), aux audits de sécurité et à la sécurisation des données et de leur traitement.
Comme le responsable de traitement, le sous-traitant doit tenir un registre des traitements effectués pour le compte du client, et dans certains cas, doit aussi désigner un DPD (délégué à

la protection des données). Le sous-traitant doit aussi notifier le responsable de traitement des violations des données personnelles. Enfin, le sous-traitant est soumis à une clause de confidentialité. La protection des données est à prendre en compte par défaut (privacy by default) et dès la conception du produit ou du service (privacy by design).

Enfin, le sous-traitant est bien entendu tenu de répondre à un client faisant valoir ses droits.