

Fiche conseil. 11

Qu'est-ce qu'un sous-traitant ?

Le sous-traitant est la personne physique ou morale (entreprise ou organisme public) qui traite des données pour le compte et sur instruction d'un autre organisme « le responsable de traitement », dans le cadre d'un service ou d'une prestation.

Que dit le RGPD ?

- Principes fondamentaux du RGPD : intégrité, confidentialité, transparence et loyauté.
- [Article 28 du RGPD](#) : définit les obligations du sous-traitant

Applicable depuis le 25 mai 2018, le RGPD impose des obligations spécifiques aux sous-traitants dont la responsabilité sera susceptible d'être engagée en cas de manquement.

Ces obligations concernent tous les organismes qui traitent des données personnelles pour le compte d'un autre organisme, dans le cadre d'un service ou d'une prestation.

Les sous-traitants sont tenus de respecter des obligations spécifiques en matière de sécurité, de confidentialité et de documentation de leur activité. Ils doivent prendre en compte la protection des données dès la conception du service ou du produit et par défaut et mettre en place des mesures permettant de garantir une protection optimale des données.

Bonnes pratiques si votre structure est sous-traitante

- Établir un contrat clair avec votre client ;
- Traiter les données à caractère personnel que sur instruction documentée du responsable du traitement ;
- Documenter l'activité de sous-traitance (registre des activités), le cas échéant ;
- Proposer des outils respectueux des données personnelles (garanties suffisantes) ;
- Aider le responsable de traitement, dans la mesure du possible, à s'acquitter de ses obligations (notamment, sans s'y limiter : assurer la sécurité du traitement ; donner suite aux demandes d'exercice des droits des personnes concernées ; notifier à l'autorité de contrôle et communiquer aux personnes concernées une violation de données à caractère personnel ; réaliser une analyse d'impact relative à la protection des données et une consultation préalable de la CNIL) ;
- Garantir la sécurité des données collectées.

Bonnes pratiques si votre structure est responsable de traitement

- Établir un contrat clair avec votre sous-traitant (article 28 du RGPD) ;
- Auditer le sous-traitant ;
- Garantir la sécurité des données collectées.