

3. Avoir un contrat avec chaque sous-traitant

Quelles obligations par rapport à mes sous-traitants ?



Il vous arrive de confier un service ou une opération, que vous n'effectuez pas vous-même, à une autre personne (exemple : un fournisseur de service DMI). Ce dernier devient alors votre « sous-traitant ».

➡ Chaque sous-traitant traite des données à caractère personnel pour votre compte et sous vos instructions. Ce qui signifie qu'un sous-traitant va effectuer des opérations **sous votre propre responsabilité et sous votre contrôle**. Ce dernier est soumis au Règlement Général de Protection de Données (RGPD) tout comme vous.

Quelques exemples de sous-traitants :

- Votre informaticien
- Votre fournisseur DMI
- Réseau Santé Bruxellois
- Sociétés de facturation (comptable)
- Etc.

ATTENTION : toute personne qui ne traite pas de données à caractère personnel n'est pas considéré comme étant votre sous-traitant (exemple : Fournisseur Gaz/Électricité)

Les obligations

Vous êtes soumis au Règlement Général de Protection de Données (RGPD) en tant que responsable du traitement des données à caractère personnel. Cependant, vos sous-traitants sont également soumis au RGPD.

Le RGPD exige plusieurs obligations dans votre relation avec vos sous-traitants :

- Vous êtes tenu de **choisir un sous-traitant qui garantit le respect du RGPD**
- Vous êtes dans l'obligation d'**établir un contrat par écrit avec vos différents sous-traitants**, mentionnant notamment toutes les clauses exigées par le RGPD ou importantes pour vous.
 - Clauses imposées par le RGPD (non exhaustives [-Art.28 du RGPD-](#)) :
 - Le sous-traitant traitera les données uniquement sous vos instructions
 - En cas de sous-traitance de second rang : il est conseillé de prévoir une autorisation de votre part
 - Droit d'audit dans votre chef
 - Notification d'une violation de données dans les plus brefs délais de la connaissance (Conseil : 24 heures calendaires)
 - Destruction et/ou retour des données à la fin du contrat

-
- Vous devez vous assurer de la **légalité de transfert de données hors de l'Union Européenne**
 - Vous devez également **reprendre l'identité de votre sous-traitant dans votre Registre d'activités de traitement**

Concrètement



Choisissez des sous-traitants garantissant le respect du RGPD et qui répondent à vos besoins / domaine d'activité



Reprenez les clauses reprises par l'Art.28 du RGPD



Optez pour des garanties en termes de mesures de sécurité, répondant au RGPD



Analysez minutieusement vos contrats avec vos sous-traitants en cours



Etablissez un contrat écrit avec des instructions claires et concises de ce que vous attendez de vos sous-traitants (contrat spécifique par sous-traitant)



Indiquez dans votre registre d'activités de traitements tous vos sous-traitants



Soyez attentif à la légalité de transfert de données hors l'Espace Économique Européen



Interdisez l'accès aux sous-traitants obsolètes (exemple : changement de logiciel/ sous-traitant, d'adresse ou de cabinet, etc.
Retirer les accès inutiles)