CABRI

IT - CONSULTANCE
INVESTISSEMENTS

RGPD
valider un sous-traitant

Contrat RGPD

Un contrat définissant les caractéristiques du traitement ainsi que les différentes obligations des parties en matière de protection des données doit être établi entre elles (article 28 du RGPD). Ce contrat devra mentionner que le prestataire, en tant que sous-traitant :

- ne traite les données à caractère personnel que sur instruction du responsable de traitement ;
- veille à la signature d'engagements de confidentialité par le personnel ;
- prend toutes les mesures de sécurité requises au regard des objectifs de sécurité qui lui sont fixés par le responsable de traitement ;
- ne recrute pas de sous-traitant sans autorisation écrite préalable du responsable de traitement ;
- coopère avec le responsable de traitement pour le respect de ses obligations, notamment lorsque des patients/clients ont des demandes concernant leurs données ;
- supprime ou renvoie au responsable de traitement l'ensemble des données à caractère personnel à l'issue des prestations ;
- met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations pour permettre la réalisation d'audits.

Registre des traitements

Le sous-traitant doit tenir un registre des activités de traitement.

Notification et information

Le sous-traitant doit, en cas d'incident lié aux données qu'il gère pour le compte du responsable de traitement (faille de sécurité, piratage, perte, etc.) l'en informer dans les meilleurs délais, afin que ce dernier puisse respecter ses propres obligations de gestion et de notification de l'incident. Le contrat signé entre le responsable de traitement et son sous-traitant devrait prévoir les modalités de notification du sous-traitant au responsable de traitement