

Fiche pratique

Identifier et encadrer ses sous-traitants

Le : ...

Objectif de la fiche

Cette fiche a pour but d'aider les CPTS à :

- identifier leurs sous-traitants au sens du RGPD,
- vérifier qu'ils offrent des garanties suffisantes de sécurité et de conformité,
- et formaliser la relation contractuelle conformément à l'article 28 du RGPD.

Elle ne remplace pas le registre du sous-traitant (qu'il doit tenir lui-même), mais aide la CPTS à documenter sa responsabilité de *responsable de traitement*.

1. Rappel des principes du RGPD

La CPTS est responsable de traitement pour les données qu'elle collecte et gère (adhérents, salariés, partenaires, patients...). Lorsqu'elle confie certaines opérations à un prestataire (hébergement, paie, site web, etc.), ce prestataire devient sous-traitant au sens du RGPD.

Article 28 du RGPD : "Le responsable du traitement ne fait appel qu'à des sous-traitants qui présentent des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées."

2. Identifier un sous-traitant

Un sous-traitant est une personne ou une structure (entreprise, association, indépendant) qui traite des données personnelles pour le compte et sur instructions de la CPTS.

Exemples de sous-traitants courants :

Sous traitant ou responsable de traitement	Type de service	Données traitées
GE ASOE	Gestion RH / paie	Données salariés, RIB, contrats

Sous traitant ou responsable de traitement	Type de service	Données traitées
OVH, IONOS...	Hébergement site web	Données de contact / cookies
Prestataire web	Maintenance, formulaires en ligne	Données visiteurs du site
Expert-comptable	Comptabilité, indemnités, RIB	Données financières
Plateforme santé (ex. Diapason, e-parcours)	Coordination des parcours	Données de santé
HelloAsso, Framafoms	Inscription à des événements	Nom, prénom, email
Office 365, Google Workspace	Outils collaboratifs	Données internes, emails

Attention : un partenaire (ex. ARS, URPS, MSP, association) n'est pas forcément un sous-traitant, il peut être responsable de traitement indépendant ou, dans certains cas, co-responsable.

Question réflexe : Est-ce que le prestataire agit sur instruction de la CPTS ou pour ses propres besoins ?

3. Vérifier la conformité d'un sous-traitant

Avant de contractualiser, la CPTS doit s'assurer que le sous-traitant est conforme au RGPD. Voici les vérifications à effectuer ou à demander :

Éléments à vérifier	Pourquoi c'est important	Comment vérifier
Politique RGPD / mentions légales	Montre que le prestataire connaît ses obligations	Consulter son site ou demander son document interne
Localisation des serveurs	Garantit que les données restent dans l'UE ou dans un pays adéquat	Poser la question ou demander une attestation
Contrat ou clause RGPD	Obligation de l'article 28 RGPD	Vérifier la présence de clauses de sécurité et confidentialité
Mesures de sécurité techniques	Garantit la protection des données traitées	Demander un descriptif ou un engagement de sécurité

Éléments à vérifier	Pourquoi c'est important	Comment vérifier
Certification (HDS, ISO 27001...)	Preuve de conformité reconnue	Vérifier le certificat ou la référence CNIL
Gestion des incidents	Permet la notification rapide en cas de fuite	Demander la procédure ou la clause correspondante
Sous-traitance ultérieure	Savoir si le prestataire fait appel à d'autres sous-traitants	Vérifier dans le contrat

Bon réflexe : Conserver les échanges ou les documents de vérification dans un dossier "RGPD / Sous-traitants".

4. Formaliser la relation contractuelle

Chaque sous-traitant doit être encadré par un contrat ou une clause spécifique (article 28 du RGPD). Cette clause doit préciser au minimum :

- l'objet et la durée du traitement confié,
- la nature et la finalité du traitement,
- le type de données et les catégories de personnes concernées,
- les obligations du sous-traitant (confidentialité, sécurité, assistance, suppression des données),
- la possibilité d'audit ou de vérification,
- et l'interdiction de sous-traiter sans accord écrit de la CPTS.

Le contrat doit également prévoir les modalités de restitution ou de suppression des données en fin de prestation.

5. Tenir une liste interne des sous-traitants

La CPTS doit tenir à jour un **tableau de suivi** recensant ses sous-traitants. Ce document permet de :

- suivre les contrats signés,
- planifier les vérifications annuelles,
- prouver la conformité en cas de contrôle.

Exemple de tableau de suivi :

Sous-traitant / Prestataire	Service fourni	Données traitées	Hébergement / Localisation	Contrat RGPD signé	Dernière vérification	Commentaires
GE ASOE	Gestion RH et paie	Données salariés	France	Oui	2025	Convention signée
OVH	Hébergement du site web	Données visiteurs	France / UE	Oui	2025	Sécurité conforme
HelloAsso	Inscriptions événement	Données participants	France	À vérifier	-	Conditions RGPD disponibles
Expert-comptable	Comptabilité	Données financières	France	Oui	2025	Clause RGPD dans le contrat

6. Bonnes pratiques

- Mettre à jour la liste au moins une fois par an ou à chaque nouveau contrat.
- Conserver dans un dossier unique les contrats + clauses RGPD signés.
- Intégrer le suivi des sous-traitants dans la revue annuelle RGPD.
- En cas de doute, privilégier des prestataires basés dans l'Union Européenne.
- Si le sous-traitant subit une violation de données, il doit en informer la CPTS sans délai,
- Sensibiliser les équipes à ne pas utiliser d'outils non validés (ex : outils gratuits en ligne).

7. Cas fréquents à analyser

- Expert-comptable → généralement sous-traitant
- Hébergeur → sous-traitant
- Outil métier santé → sous-traitant
- Groupement d'employeurs → souvent responsable de traitement indépendant
- Partenaires (ARS, MSP...) → responsables de traitement indépendants

En résumé

Étape	Objectif
1. Identifier	Lister les prestataires qui traitent des données personnelles pour la CPTS
2. Vérifier	S'assurer qu'ils offrent des garanties suffisantes (sécurité, RGPD, hébergement UE)
3. Contractualiser	Signer une clause ou un contrat RGPD conforme à l'article 28
4. Suivre	Tenir à jour un tableau de suivi et archiver les contrats