# Que doit contenir un contrat avec un sous-traitant de données personnelles ?

## Réponse courte

Un contrat de sous-traitance conforme à l'**article 28 du RGPD** doit contenir un ensemble de **clauses obligatoires** précisant l'**objet**, la **durée**, la **nature** et la **finalité** du traitement, le **type de données** concernées, les **catégories de personnes** concernées et les **obligations et droits** du responsable de traitement.

Il doit également imposer au sous-traitant de ne traiter les données que sur **instructions documentées** du responsable, de garantir la **confidentialité** de son personnel, de mettre en place des **mesures de sécurité** appropriées, d'**encadrer** toute sous-traitance ultérieure, d'**assister** le responsable dans l'exercice des droits des personnes, de **notifier** toute violation, et de **restituer ou supprimer** les données à la fin du contrat. Les **audits** doivent être prévus et le prestataire doit mettre à disposition les informations nécessaires pour démontrer la conformité.

## Définition

Le **contrat de sous-traitance** ou **accord de traitement des données** (DPA, Data Processing Agreement) est l'instrument juridique qui formalise la relation entre le responsable de traitement et son sous-traitant au sens du RGPD. Il conditionne la licéité de la sous-traitance et engage la responsabilité des deux parties.

## Questions fréquentes

### Le sous-traitant doit-il notifier toute violation à l'employeur ?

Oui, le contrat doit prévoir une procédure de notification rapide des violations avec un délai maximal (généralement 24 à 48 heures), plus court que les 72 heures imposées au responsable par l'article 33 du RGPD vis-à-vis de la CNPD.

### Les clauses contractuelles types peuvent-elles être utilisées ?

Oui, les clauses contractuelles types publiées par la Commission européenne (décision 2021/915) offrent une base sûre. Elles peuvent être complétées pour tenir compte des spécificités de la prestation et des exigences sectorielles luxembourgeoises.

### Qu'est-ce qu'un DPA en RGPD ?

Le DPA (Data Processing Agreement) ou accord de traitement des données est l'instrument juridique formalisant la relation entre responsable de traitement et sous-traitant. Il conditionne la licéité de la sous-traitance et engage la responsabilité des deux parties.

### Que doit contenir un contrat avec un sous-traitant de données ?

Le contrat doit préciser l'objet, la durée, la nature et la finalité du traitement, le type de données concernées, les catégories de personnes concernées et les obligations et droits du responsable de traitement, conformément à l'article 28.3 du RGPD.

### Que prévoir pour la fin du contrat de sous-traitance ?

Le contrat doit prévoir la restitution ou la suppression certifiée des données à la fin du contrat, avec attestation écrite. Cette obligation découle de l'article 28.3.g du RGPD et garantit la conformité au principe de limitation.

**Quel droit d'audit prévoir dans le contrat de sous-traitance ?**

Le contrat doit prévoir un droit de contrôle du responsable, permettant des audits périodiques. Le sous-traitant doit mettre à disposition les informations nécessaires pour démontrer la conformité, conformément à l'article 28.3.h du RGPD.

**Quelles obligations sécurité doit imposer le contrat de sous-traitance ?**

Le contrat doit imposer la mise en place de mesures techniques et organisationnelles appropriées (article 32 RGPD), comme le chiffrement, la gestion des accès et la traçabilité. Une annexe technique précise les mesures attendues.

## Conditions d’exercice

Le contenu obligatoire est strictement défini par l'article 28.3 du RGPD et doit figurer dans le contrat.

| Clause obligatoire | Détail |
|---|---|
| **Objet du traitement** | Description précise des opérations confiées |
| **Durée** | Période du traitement et du contrat |
| **Nature et finalité** | Objectifs poursuivis par le traitement |
| **Catégories de données** | Types de données traitées (identité, paie, santé) |
| **Catégories de personnes** | Salariés, candidats, clients |
| **Obligations et droits** | Engagements réciproques des parties |
| **Instructions documentées** | Le sous-traitant agit sur demande écrite |
| **Confidentialité** | Engagement du personnel du sous-traitant |
| **Sécurité** | Mesures techniques et organisationnelles (art. 32) |
| **Sous-traitance ultérieure** | Autorisation préalable écrite |
| **Assistance** | Aide pour les droits et obligations |
| **Notification violations** | Information rapide du responsable |
| **Restitution/suppression** | Fin de contrat et traitement des données |
| **Audits** | Droit de contrôle du responsable |

## Modalités pratiques

Le contrat peut prendre la forme d'un document distinct ou d'un avenant au contrat commercial principal.

| Élément | Détail |
|---|---|
| **Format** | Contrat principal, avenant ou annexe dédiée |
| **Signature** | Représentants légaux des deux parties |
| **Annexes techniques** | Description des mesures de sécurité, liste des sous-traitants |
| **Procédures d'incident** | Modalités de notification et de coopération |
| **Indicateurs** | Durée de notification, délais d'assistance |
| **Révision** | Clause de mise à jour en cas d'évolution réglementaire |
| **Clauses types** | Utilisation possible des clauses de la Commission européenne |

## Pratiques et recommandations

**Utiliser** un modèle de contrat type validé par le DPO et le service juridique, intégrant l'ensemble des clauses obligatoires de l'article 28 RGPD.

**Exiger** la signature du contrat **avant** tout transfert effectif de données au sous-traitant, pour éviter toute période de non-conformité.

**Annexer** une description précise des mesures de sécurité attendues, notamment le chiffrement, la gestion des accès et la traçabilité.

**Prévoir** contractuellement une procédure de notification des violations avec un délai maximal (généralement 24 à 48 heures), plus court que les 72 heures imposées au responsable.

**Auditer** régulièrement le respect des engagements contractuels et documenter les constats pour démontrer la diligence de l'employeur.

## Cadre juridique

Le cadre juridique repose sur le RGPD et les lignes directrices européennes.

| Référence | Objet |
|---|---|
| **Art. 28 RGPD** | Obligations du responsable et du sous-traitant |
| **Art. 28.3 RGPD** | Clauses obligatoires du contrat |
| **Art. 29 RGPD** | Traitement sur instructions documentées |
| **Art. 32 RGPD** | Sécurité du traitement |
| **Art. 33 RGPD** | Notification des violations |
| **Loi du 1er août 2018** | Régime général au Luxembourg |
| **Clauses contractuelles types** | Décision 2021/915 de la Commission européenne |

Un contrat incomplet ou absent constitue une violation du RGPD sanctionnée par la **CNPD**. Les clauses contractuelles types publiées par la Commission européenne offrent une base sûre mais peuvent être complétées pour tenir compte des spécificités de la prestation.