DPO Consulting
Your personal data protection officer

Fiche Pratique

Relation RT/ST, guide des clauses contractuelles

contact@dpo-consulting.com www.dpo-consulting.fr +33 (0)1 55 06 16 86

Relation RT/ST, guide des clauses contractuelles

Objectif de la fiche :

Donner des précisions sur la négociation des clauses sous-traitant
La sous-traitance implique que le prestataire agisse sur instructions détaillées et sous l'autorité du responsable de traitement.
L'article 28 du RGPD impose au Responsable de traitement d'encadrer contractuellement cette relation.

Qualification des parties

Il est important que le rôle de chaque partie au contrat soit défini clairement : qui est responsable de traitement et qui est sous-traitant ?

Description du traitement

Il s'agit de la présentation des aspects opérationnels du traitement. La description du traitement peut être réalisée dans une annexe. Les points principaux de cette annexe sont les suivants :

- Quelle est la **prestation** que le sous-traitant fournit au responsable de traitement ?
- Quelles sont les **opérations de traitements** réalisées ? (ex : collecte, utilisation, transfert, etc)
- Quelles sont les **finalités** du traitement ? (ex : mesurer l'audience du site, gérer l'organisation de la paie, etc)
- Quelles sont les **données personnelles** traitées ? (Adresse IP, nom/prénom, adresses mail, etc.)
- Quelles sont les **catégories de personnes concernées** par les traitements de données ? (ex : salariés, utilisateurs du site internet, clients, etc.)

Le respect des instructions par le sous-traitant

Le sous-traitant doit s'engager à n'agir que sur les instructions du responsable de traitement et **s'interdire d'utiliser les données à d'autres fins** que ce qui a été prévu au contrat.

En d'autres termes, il ne doit avoir **aucune utilisation des données pour son propre compte :** les données confiées ne sont utilisées que pour réaliser la prestation objet du contrat

Aide, conseil et assistance au responsable de traitement

• **Analyse d'Impact sur la Vie Privée (AIVP) :** le sous-traitant aide le responsable de traitement à réaliser les AIVP dont il a la charge. Cette assistance doit être gratuite et non payante.
• Le sous-traitant s'engage à alerter le responsable de traitement s'il estime que l'une de ses instructions constitue un manquement à l'une de ses obligations essentielles.

Information et consentement

Il appartient au responsable de traitement de :
• Recueillir le consentement des personnes dans les cas où il est nécessaire
• Fournir aux personnes concernées les informations obligatoires (art. 13 et 14 du RGPD)

Le contrat doit prévoir un transfert opérationnel de la collecte du consentement et de l'information des personnes au sous-traitant.

Si le sous-traitant collecte des données et communique au nom du responsable de traitement, il devra s'engager à **recueillir le consentement de façon conforme ET à fournir aux personnes les informations obligatoires** lors de chaque communication.

L'obligation de confidentialité

L'article 28 impose que le sous-traitant s'engage à soumettre son personnel à une obligation de confidentialité.

Gestion des demandes des personnes concernées

Le sous-traitant s'engage à aider et assister le responsable de traitement dans la gestion des demandes des personnes concernées.

↳ Le contrat doit définir les modalités de gestion des demandes :
Qui est chargé de répondre ?
Quels sont les délais d'action, et notamment de notification par le sous-traitant au responsable de traitement ?

Gestion des violations de données

Le sous-traitant doit s'engager à notifier au responsable de traitement toute violation de données personnelles dans les plus brefs délais.

↳ Prévoir un **délai de notification maximum** : en général « sans délai indu et au maximum 72h après la découverte de la violation ».

↳ Prévoir ce que devra contenir la notification (ex : description de la violation, conséquences probables, l'obligation d'investigation, la description des mesures prises pour y remédier).

Transferts hors Union Européenne

Le sous-traitant s'interdit de transférer des données personnelles hors UE sans mettre en place les garanties juridiques appropriées. Si le sous-traitant prévoit de mettre en place les garanties suffisantes.

↳ Répertorier les **transferts** réalisés en annexe

Sous-traitance ultérieure

Le sous-traitant ne recrute pas un autre sous-traitant sans autorisation du responsable de traitement. L'autorisation peut être générale ou spécifique.

- Autorisation spécifique :
  Chaque recours ou changement de sous-traitant doit être autorisé par le responsable de traitement. Le sous-traitant envoie un courrier au responsable de traitement et ne peut contracter qu'avec l'autorisation du responsable de traitement.

- Autorisation générale :
  Le responsable de traitement donne une autorisation générale et chaque changement ou recours à un nouveau sous-traitant doit faire l'objet d'une notification au responsable de traitement, qui dispose d'un certain délai pour émettre ses objections.

↳ Etablir la liste des sous-traitants ultérieurs en annexe.

Audit

Le sous-traitant doit mettre à disposition du responsable de traitement les informations nécessaires à démontrer le respect de ses obligations et pour permettre la réalisation d'audits

↳ Prévoir les modalités d'audit :
À quelle fréquence peuvent-ils être réalisés ? Avec quels délais de notification ?
Qui prend en charge les coûts, quelles seront les suites de l'audit en cas de non-conformité ? Etc.

Mesures de sécurité

Le sous-traitant doit assurer la sécurité, intégrité et confidentialité des données. les mesures de sécurité mises en place pour garantir ce niveau de sécurité peuvent être détaillées dans une annexe.

Fin du contrat

Au terme de la prestation, le sous-traitant doit s'engager à restituer et à détruire les données personnelles appartenant au responsable de traitement ou à les supprimer en fonction des instructions du responsable de traitement.

DPO Consulting
Your personal data protection officer

Contact commercial

Mail : contact@dpo-consulting.com
Tél : +33 (0)1 55 06 16 86

Nous contacter

Nous trouver

Découvrez nos bureaux,
un contact proche de chez vous !