|  |
| --- |
| **Le RGPD en 10 étapes**Étape 7 – Établissez des contrats de sous‑traitance  |

## **Le RGPD en 10 étapes**

## **Étape 7 – Établissez des contrats de sous-traitance**

### Introduction

Un sous-traitant est une personne physique ou morale, une autorité publique ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Le responsable du traitement peut toujours choisir de traiter les données en interne, ce que nous appelons la « gestion interne », ou de sous-traiter une partie du traitement à une partie externe. Dans ce dernier cas, il fait appel à un « sous-traitant ».

Parmi les exemples types de sous-traitants, citons les secrétariats sociaux (pour le calcul des salaires), les entreprises informatiques (pour l’installation et la maintenance des logiciels, et éventuellement pour la sécurisation du traitement) et les confrères qui effectuent certaines prestations en « sous-traitance » pour votre cabinet et sont dès lors amenés à traiter des données à caractère personnel. Si vous conservez vos données dans un « cloud », le gestionnaire du cloud est considéré comme un sous-traitant.

### Quel sous-traitant ?

Vous avez 2 obligations en ce qui concerne les sous-traitants :

* Vous devez choisir un sous-traitant approprié
* Vous devez établir un contrat de sous-traitance

#### Sous-traitant approprié

Cette obligation vous impose de ne faire appel qu’à des sous-traitants présentant des garanties suffisantes en termes de sécurisation des données, de respect du RGPD et de protection des droits de la personne concernée.

Le principe est simple. Tant que vous vous occupez du traitement, vous pouvez et devez-vous assurer que celui-ci est conforme au RGPD. Dès que vous sous-traitez une partie du traitement à des tiers, tout se complique.

Vous devez tout d’abord et avant tout vérifier si le sous-traitant auquel vous souhaitez faire appel met suffisamment de mesures en œuvre pour respecter le RGPD. Il ne suffit bien entendu pas de le lui demander et de se satisfaire d’une réponse positive comme « Oui, nous prenons suffisamment de mesures ». Vous devez avoir une idée minimale des mesures que le sous-traitant met en œuvre, comme le fait de limiter l’accès aux données à caractère personnel aux personnes autorisées, la mise en place de mesures relatives aux données sensibles, etc.

Si votre enquête ne vous permet pas de qualifier le sous-traitant d’ « approprié », vous ne pouvez pas l’engager et devez en principe en choisir un autre.

#### Conclure un contrat de sous-traitance

Dans un second temps, vous devez conclure un « contrat de sous-traitance » avec votre sous-traitant. Ce contrat consiste en une description générale des activités de traitement que vous confiez au sous-traitant.

En général, ce contrat doit avant tout définir l’objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, ainsi que les obligations et les droits du responsable du traitement. Ensuite, le contrat énumère également les obligations du sous-traitant (protection des données, coopération en cas de plaintes éventuelles, etc.).

Vous pourriez vous demander comment parvenir à faire signer par de grands acteurs, internationaux ou non, un contrat établi par vos soins. Or vous y êtes en principe obligé. Dans la plupart des cas, cependant, ces entreprises imposent elles-mêmes ce type de contrat. Dans le cas contraire, il est tout de même préférable que vous le leur demandiez. Et si elles n’accèdent pas à votre demande, vous pourrez tout au moins prouver que vous avez essayé.

Si vous recevez un modèle à signer, vous pouvez le comparer au modèle ci-joint ou vous pouvez vous référer à une [check-list](https://whitewire.be/wp-content/uploads/2017/02/20170411_verwerkersovereenkomst_checklist.xlsx) telle que celle développée par White Wire (uniquement en néerlandais pour l’instant).

**Check-list**

|  |
| --- |
| * **Je dispose d’une liste des sous-traitants avec lesquels je travaille.**
* **J’ai vérifié s’ils mettaient en œuvre les mesures nécessaires pour respecter le RGPD.**
* **J’ai conclu un contrat de sous-traitance avec chacun d’entre eux.**
 |

###

### Modèle de contrat de sous-traitance

|  |
| --- |
| ENTRE...................................................................................................................................................................dont le siège est sis à .....................................................................................................................................inscrite au registre des personnes morales de ……………..……, section …………………………………………….sous le numéro d’entreprise …….……………………………………………………………………….………………………………légalement représentée par ........................................................................................................….,ci-après dénommée le « responsable du traitement »,ET...................................................................................................................................................................dont le siège est sis à .....................................................................................................................................inscrite au registre des personnes morales de ……………..……, section …………………………………………….sous le numéro d’entreprise .…….……………………………………………………………………….……………………………..légalement représentée par ............................................................................................................,ci-après dénommée le « sous-traitant ».Ci-après dénommées séparément la « partie » et conjointement les « parties »,ATTENDU QUE :1. Le responsable du traitement est actif dans le secteur de ..................................................................................................................…………………………………

......................................................................................................................................................1. Le sous-traitant est actif dans le secteur de/en qualité de .......................................................................................................
2. Le responsable du traitement souhaite sous-traiter et confier certaines activités au sous-traitant. Ces activités exigent/nécessitent le traitement de données à caractère personnel, ce qui fait que, dans le cadre de sa prestation de services, le sous-traitant sera également amené à traiter des données à caractère personnel pour le compte du responsable du traitement.

L’objet, la durée, la nature et les finalités du traitement, ainsi que le type de données à caractère personnel et les catégories de personnes concernées sont décrits en détail à l’Annexe 1 du présent contrat.1. Dans le cadre de l’application du présent contrat, le terme « données à caractère personnel » signifie les données protégées en vertu des dispositions du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (« RGPD »), et de la législation et réglementation transposant ce règlement.
2. Les parties souhaitent conclure un contrat fixant les règles et les conditions de sous-traitance (d’une partie) du traitement, dans le but de protéger les données à caractère personnel concernées.

IL EST CONVENU CE QUI SUIT :*Article 1 – Obligations du sous-traitant* * 1. Le sous-traitant ne traite les données à caractère personnel que pour le compte du responsable du traitement et sur la base de ses instructions documentées et du présent contrat.

Si le sous-traitant n’est pas en mesure de le faire et a des raisons de croire que la législation qui lui est applicable l’empêche de suivre les instructions du responsable du traitement et de remplir ses obligations en vertu du présent contrat, il en informe le responsable du traitement avant de procéder au traitement des données. Dans ce cas, le responsable du traitement a le droit de suspendre l’accès aux données ou leur communication et/ou de résilier le contrat.* 1. Le sous-traitant confirme que, compte tenu de l’état de la technique, des coûts de mise en œuvre ainsi que de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, il a mis et continue à mettre en œuvre des mesures de sécurité techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Ces mesures sont détaillées à l’Annexe 2 du présent contrat.

Il s’engage notamment à protéger les données à caractère personnel contre la destruction, la perte, l’altération, la divulgation non autorisée ou l’accès non autorisé, de manière accidentelle ou illicite.* 1. Le sous-traitant veille à ce que les personnes à son service autorisées à traiter les données à caractère personnel s’engagent à respecter la confidentialité de ces données.
	2. Le sous-traitant garantit qu’il tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s’acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d’exercer leurs droits prévus au chapitre III du Règlement général sur la protection des données.

À cet égard, le sous-traitant est tenu d’informer immédiatement le responsable du traitement de toute demande émanant directement d’une personne concernée, sans répondre à cette demande, sauf si le responsable du traitement y a consenti ou lui a demandé de le faire.* 1. Le sous-traitant garantit que, compte tenu de la nature du traitement et des informations à sa disposition, il aide le responsable du traitement à garantir le respect des obligations en matière de sécurité des données à caractère personnel prévues aux articles 32 à 34 du RGPD, d’analyse d’impact relative à la protection des données prévues à l’article 35 du RGPD et de consultation préalable prévues à l’article 36 du RGPD.
	2. Le sous-traitant garantit qu’il ne transfère, ne met à disposition ou ne donne accès à aucune donnée à caractère personnel à des pays ou des organisations internationales en dehors de l’Espace économique européen, à moins qu’il en ait reçu l’instruction du responsable du traitement.
	3. Le sous-traitant ne conserve pas les données à caractère personnel plus longtemps que la durée nécessaire à l’exécution du présent contrat. Au terme de la prestation de services relatifs au traitement, le sous-traitant supprime les données à caractère personnel ou les renvoie au responsable du traitement, selon le choix du responsable du traitement.

De même, le sous-traitant détruit toute copie existante des données à caractère personnel. À la demande du responsable du traitement, le sous-traitant confirme la suppression de toutes les copies de données à caractère personnel. Si la législation ou la réglementation en vigueur exige la conservation des données à caractère personnel, le sous-traitant en informe le responsable du traitement, à moins que la législation ou la réglementation le lui interdise. * 1. Le sous-traitant confirme expressément qu’il ne divulguera aucune donnée à caractère personnel ou toute autre information en découlant à des tiers, qu’il n’utilisera et/ou ne traitera à aucun moment les données à caractère personnel pour des besoins ou finalités propres et qu’il ne copiera pas les données à caractère personnel (à moins que ce soit strictement nécessaire dans le cadre de l’exécution du présent contrat).

*Article 2 – Pas de transfert des droits ou de sous-traitance ultérieure** 1. Le sous-traitant n’a pas le droit d’octroyer un droit et/ou d’imposer une obligation, ni de les transférer à un tiers en vertu du présent contrat, sans l’autorisation écrite préalable du responsable du traitement.
	2. Le sous-traitant ne recrute aucun autre sous-traitant (via un contrat de sous-traitance ultérieure) pour exécuter une partie quelconque du présent contrat sans l’autorisation écrite préalable du responsable du traitement.
	3. L’autorisation écrite du responsable du traitement visée aux points 5.1 et 5.2 est

SOIT fournie à titre général. Cela implique que le sous-traitant informe le responsable du traitement de tout changement prévu concernant l’ajout ou le remplacement d’autres sous-traitants. Le responsable du traitement peut alors émettre des objections à l’encontre de ces changements SOIT fournie à titre exceptionnel. Cela implique que le sous-traitant doit obtenir l’autorisation écrite expresse du responsable du traitement pour tout changement prévu concernant l’ajout ou le remplacement d’autres sous-traitants.* 1. La conclusion d’un quelconque contrat de sous-traitance ultérieure pour l’exécution d’une partie du présent contrat n’exempte en aucun cas le sous-traitant du respect de ses obligations en vertu du présent contrat. Les services relatifs au traitement fournis par le sous-traitant ultérieur doivent être réalisés conformément aux dispositions du présent contrat. Sur simple demande, le sous-traitant remet immédiatement au responsable du traitement une copie des éventuels contrats de sous-traitance ultérieure, le cas échéant à l’exception des accords financiers conclus entre le sous-traitant et le sous-traitant ultérieur.

*Article 3 – Audit*Le sous-traitant s’engage expressément à se soumettre et à coopérer à tout audit, contrôle ou enquête, mené directement ou indirectement par une personne ou organisation autorisée à cette fin à la demande du responsable du traitement pour vérifier si le sous-traitant respecte ses obligations.Dans ce cas, le sous-traitant fournit notamment, à la demande du responsable du traitement, toutes les informations nécessaires pour prouver qu’il respecte les obligations liées à l’intervention d’un sous-traitant, comme prévu à l’article 28 du RGPD. Il s’agit notamment des informations relatives aux activités de traitement des données à caractère personnel et aux mesures de sécurité mises en œuvre. Dans ce cadre, le sous-traitant s’engage également à permettre au responsable du traitement d’accéder à ses installations/infrastructures de traitement des données pour qu’il puisse vérifier le respect du présent contrat.*Article 4 – Responsabilité** 1. Le sous-traitant respecte la législation et la réglementation en vigueur en matière de protection des données à caractère personnel. À cet égard, le sous-traitant ne sera tenu pour responsable du dommage causé par le traitement que (1) s’il n’a pas respecté les obligations prévues par le RGPD qui incombent spécifiquement aux sous-traitants ou (2) s’il a agi en dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.
	2. Le sous-traitant décharge le responsable du traitement de toute action en justice intentée par un tiers au motif d’une violation de la réglementation en vigueur et/ou du présent contrat dont le sous-traitant porte la responsabilité.
	3. Le sous-traitant assure dûment sa responsabilité. Sur demande, il présente la police au responsable du traitement.

*Article 5 – Durée** 1. Le présent contrat entre en vigueur le ....... (date) et reste applicable [pendant une durée indéterminée] OU [jusqu’au [date]], sauf résiliation en vertu de l’article 1.1 ou de toute autre disposition du contrat.
	2. [en cas de durée indéterminée] Chaque partie peut résilier le présent contrat en envoyant une notification écrite à l’autre partie. Il doit à cet effet être tenu compte d’un délai de préavis de 30 jours minimum. Le délai de préavis prend effet le premier jour du mois qui suit celui de l’envoi de la notification.
	3. Le responsable du traitement peut immédiatement résilier le présent contrat, sans s’adresser à un tribunal, en envoyant une notification de résiliation écrite au sous-traitant si :
	4. le sous-traitant viole le présent contrat et que la violation est irrémédiable ;
	5. le sous-traitant viole le présent contrat et que la violation n’est pas irrémédiable, mais qu’il ne parvient pas à y remédier dans les [30 jours] suivant la réception d’une mise en demeure écrite l’invitant à remédier à la violation.
	6. le sous-traitant est déclaré en faillite, en liquidation ou en dissolution.

*Article 6 – Divers** 1. Le présent contrat constitue l’intégralité de l’accord entre les parties et n’impose en aucun cas de mettre des données à caractère personnel à la disposition du sous-traitant.
	2. Si une ou plusieurs dispositions du présent contrat sont déclarées nulles ou irréalisables, les parties s’engagent à remplacer la ou les dispositions en question par une ou plusieurs dispositions valables et réalisables s’approchant le plus possible des objectifs économiques, commerciaux ou autres de la ou des dispositions déclarées nulles ou irréalisables. Les autres dispositions du présent contrat demeurent pleinement en vigueur.
	3. Le simple fait qu’une partie n’insiste pas sur le respect strict d’une disposition du contrat ou ne l’applique pas ne peut en aucun cas être interprété comme une renonciation ou un abandon des droits de cette partie, sauf confirmation écrite.

*Article 7 – Droit applicable et litiges*Le présent contrat est régi par le droit belge. [Tout litige entre les parties sera soumis au tribunal de l’arrondissement dans lequel se situe le siège du responsable du traitement.]OU[Tout litige découlant de ou se rapportant au présent contrat sera définitivement réglé conformément au règlement d’arbitrage du CEPANI par un ou plusieurs arbitres désignés en vertu de ce règlement.]Fait à ..........................., le ............................, en deux exemplaires originaux, dont chaque partie reconnaît en avoir reçu un.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Pour le responsable du traitement Pour le sous-traitantNom :..................................... Nom :......................................Fonction : .................................. Fonction : ...................................Annexe 1 : Objet du contratAnnexe 2 : Mesures de sécurité |