**Modèle de contrat de sous-traitance de traitement des données**

**Clause de non-responsabilité**

☞ Ce document sert de modèle de contrat de sous-traitance. Il ne constitue pas un conseil juridique et il doit être adapté aux circonstances concrètes de chaque cas. Toute garantie est exclue concernant le contenu. L’utilisation se fait aux risques et périls de l’utilisateur.

**CONTRAT DE SOUS-TRAITANCE de traitement des données**

entre

**[NOM, ADRESSE] (ci-après le « mandant »),**

et

**[NOM, ADRESSE] (ci-après le « sous-traitant »),**

collectivement « les parties ».

1. **Objet et durée du contrat**

Le sous-traitant fournit au mandant des services fiduciaires et comptables sur la base d’un contrat distinct.

Cet accord permet aux parties d’honorer leurs obligations en vertu de la législation applicable en matière de protection des données lorsque le sous-traitant traite des données personnelles pour le compte du mandant. Il concrétise les obligations des parties en matière de protection des données, qui découlent de la sous-traitance décrite dans le contrat distinct.

Les clauses du présent accord s’appliquent à toutes les activités liées au contrat distinct dans le cadre duquel le sous-traitant et ses salariés ou les personnes mandatées par le sous-traitant entrent en contact avec des données à caractère personnel provenant du mandant ou collectées pour le compte du mandant.

La durée du présent accord dépend de la durée du contrat distinct et l’accord peut uniquement être résilié conjointement au contrat, de manière ordinaire ou extraordinaire.

1. **Type de traitement et nature des données**

Le sous-traitant a accès aux données à caractère personnel pour le compte du mandant. Cela comprend les activités décrites dans le contrat distinct.

Dans ce contexte, les activités du sous-traitant peuvent comprendre, entre autres, les aspects suivants :

* Réception, traitement et envoi de données salariales
* Établissement et envoi de décomptes de salaire
* Gestion de données de base des salariés
* Établissement d’attestations et de déclarations à l’attention des autorités et assurances
* Accès à des données et traitement de celles-ci chez le mandant ou directement chez son client

Données personnelles nécessaires à l’exécution de ces activités :

* Données de base de personnes
* Données de base des salariés
* Données de communication
* Données contractuelles de base
* Données salariales
* Données de sécurité sociale et de santé
* Données de décompte et de paiement
* Autres données personnelles découlant éventuellement du contrat distinct

1. **Obligations du sous-traitant**
   1. Le sous-traitant et les personnes placées sous ses ordres qui ont accès aux données personnelles ne peuvent traiter (collecter, enregistrer, conserver, utiliser, modifier, communiquer, archiver, effacer ou détruire, etc.) les données que dans le cadre du mandat et des instructions du mandant, sauf cas exceptionnel, par exemple dans le cadre d’enquêtes menées par les autorités de poursuite pénale. Dans ce cas, le sous-traitant communique cette injonction légale au mandant, à moins que le droit concerné n’interdise une telle communication au motif d’un intérêt public important.

En cas de changement des personnes habilitées à donner des instructions ou d’empêchement de longue durée des personnes désignées, l’identité du successeur ou du représentant doit être communiquée au partenaire contractuel.

Si une instruction du mandant est contraire aux dispositions légales en vigueur, le sous-traitant en informe immédiatement le mandant.

* 1. Le sous-traitant utilise les données confiées pour le traitement exclusivement aux fins convenues et non à des fins personnelles. Il ne fait pas de copie ou duplicata des données à l’insu du mandant, sauf s’il s’agit de copies de sauvegarde.
  2. Le sous-traitant n’est pas autorisé à supprimer de son propre chef ou à détruire d’une autre manière les données traitées dans le cadre du mandat. Toute suppression ou destruction des données ne peut être effectuée que sur la base d’instructions écrites du mandant, à moins qu’il n’existe une raison légale exigeant une telle mesure.
  3. Le mandant autorise par la présente le traitement de données en dehors du site de l’entreprise du sous-traitant, par exemple dans le bureau au domicile de membres du personnel. Si le traitement des données a lieu dans un logement privé, des mesures de sécurité appropriées doivent être contractuellement garanties.
  4. Le sous-traitant s’engage à traiter de manière confidentielle toutes les données personnelles dont il a connaissance dans le cadre du présent contrat de sous-traitance. Cette obligation subsiste même après la fin du présent contrat. Le sous-traitant veillera à ce que toutes les personnes ayant accès aux données personnelles ou chargées de leur traitement soient informées de l’obligation de confidentialité et soient contractuellement liées en conséquence.
  5. Le sous-traitant est tenu de signaler sans délai au mandant les éventuelles violations de la protection des données ou irrégularités et de lui communiquer tous les détails pertinents de la violation, y compris la nature de la violation, les données personnelles concernées, les possibles conséquences ainsi que les mesures prises ou prévues pour endiguer l’incident et minimiser les éventuelles conséquences négatives.
  6. Sur demande du mandant, le sous-traitant est tenu de rectifier les données si elles sont inexactes ou incomplètes. Si une personne concernée fait directement valoir ses droits auprès du sous-traitant, notamment son droit d’accès, de renseignement ou de transfert des données, son droit d’opposition ou son droit de rectification, d’effacement ou de destruction des données, le sous-traitant ne statue pas de manière autonome, mais renvoie immédiatement la personne concernée vers le mandant et attend ses instructions.
  7. Le sous-traitant ne peut fournir à des tiers ou aux personnes concernées des renseignements relatifs à des données personnelles découlant du contrat qu’après avoir reçu des instructions ou le consentement du mandant.
  8. Après l’achèvement des travaux contractuels, le sous-traitant s’engage à effacer ou détruire tous les documents et résultats d’utilisation qui ont été produits dans le cadre du présent contrat de sous-traitance, dans le respect de la législation sur la protection des données, ainsi qu’à restituer au mandant l’ensemble des documents, données et supports de données qui lui ont été remis dans le cadre du contrat distinct. L’effacement ou la destruction intervient dès lors qu’aucun motif légal s’y oppose. Il convient de noter que le sous-traitant peut être légalement tenu de conserver certaines données pendant une période définie. Toutefois, à l’expiration de ce délai, les données concernées sont également effacées ou détruites conformément à la législation sur la protection des données.
  9. Le sous-traitant confirme qu’il connaît les prescriptions en vigueur en matière de protection des données et qu’il s’engage à la respecter intégralement.

1. **Mesures techniques et organisationnelles**
   1. Le sous-traitant s’engage à prendre des mesures techniques et organisationnelles appropriées afin de garantir la sécurité des données personnelles.
   2. Le sous-traitant prend des mesures techniques appropriées pour protéger les données personnelles contre tout accès non autorisé, toute perte ou toute destruction. Cela comprend l’utilisation de pare-feux, de technologies de cryptage, de contrôles d’accès et d’autres mesures de sécurité appropriées.
   3. En outre, le sous-traitant met en œuvre des mesures organisationnelles internes appropriées afin de garantir que seul le personnel autorisé ait accès aux données personnelles. Il s’agit notamment de former le personnel aux règles de protection des données et de mettre en place des restrictions d’accès.
   4. Ces mesures techniques et organisationnelles sont régulièrement contrôlées et, si nécessaire, mises à jour afin de répondre aux normes technologiques actuelles et aux dispositions en vigueur en matière de protection des données.
   5. Le mandant a le droit, après concertation avec le mandataire, de procéder à des contrôles ou de les faire effectuer par des auditeurs indépendants à désigner au cas par cas. Il a le droit de s’assurer du respect du présent accord par le mandataire dans le cadre de ses activités en procédant à des contrôles aléatoires, qui doivent généralement être annoncés en temps voulu.
   6. Il appartient au mandataire de garantir que le mandant puisse s’assurer du respect des obligations du mandataire selon la LPD. Le mandataire s’engage à fournir les informations nécessaires au mandant, à sa demande, et notamment à prouver la mise en œuvre des mesures techniques et organisationnelles.

La preuve de telles mesures, qui ne concernent pas uniquement le mandat concret, peut être apportée par

le respect de règles de conduite approuvées selon la LPD ;

la certification selon la LPD ;

des attestations, rapports ou extraits de rapports récents d’instances indépendantes (p. ex. experts-comptables, réviseurs, conseillers en protection des données, service de sécurité informatique, auditeurs chargés de la protection des données, auditeurs qualité) ;

une certification appropriée par un audit de sécurité informatique ou de protection des données (p. ex. selon la norme ISO 27001, ISO 27701, GoodPriv@cy, etc.)

Le mandataire peut faire valoir un droit à rémunération pour avoir permis au mandant de procéder à des contrôles.

1. **Lieu de traitement des données**
   1. Le traitement des données a lieu exclusivement en Suisse ou dans un pays tiers qui remplit les conditions légales en matière de protection des données.
   2. Si le traitement des données a lieu à l’étranger ou si des données sont transférées à l’étranger, il convient de s’assurer au préalable que les exigences légales en matière de protection des données sont respectées :

L’externalisation à un sous-sous-traitant dans un État membre de l’Union européenne (UE) ou de l’Espace économique européen (EEE) ou dans un pays qui, selon la LPD en vigueur, offre un niveau adéquat de protection des données, est autorisée à condition qu’un accord contractuel soit conclu selon la LPD (contrat de sous-traitance).

L’externalisation à un sous-sous-traitant dans un pays qui n’offre pas un niveau adéquat de protection des données est autorisée à condition que le mandataire et le sous-sous-traitant concluent un accord contractuel selon la LPD (contrat de sous-traitance) et que les conditions particulières de la LPD soient satisfaites, en particulier :

Parce que le mandataire assure une protection adéquate des données en concluant avec le sous-sous-traitant des clauses standard de protection des données que le PFPDT a préalablement approuvées, établies ou reconnues

et

En cas de besoin, des mesures supplémentaires ont été convenues et mises en œuvre en complément des clauses standard de protection des données.

1. **Relations de sous-sous-traitance avec des entreprises de sous-traitance**
   1. Le sous-traitant fournit lui-même ses prestations. Le recours à des entreprises de sous-traitance n’est autorisé qu’avec l’accord écrit préalable du mandant.
   2. Il y a une relation de sous-sous-traitance soumise à autorisation dès lors que le sous-traitant fait appel à d’autres sous-traitants pour la fourniture de tout ou partie des prestations convenues dans le contrat.
   3. Le sous-traitant est tenu d’informer le mandant par écrit de tout changement concernant l’entreprise de sous-traitance, notamment du recours à une entreprise de sous-traitance ou de son remplacement, par exemple.
   4. L’entreprise de sous-traitance doit être soigneusement sélectionnée en fonction de son aptitude et de sa fiabilité. Le recours à d’autres sous-traitants dans des pays tiers ne peut avoir lieu que si les conditions légales en matière de protection des données sont remplies.
   5. Le sous-traitant est tenu de transférer contractuellement à l’entreprise de sous-traitance toutes les obligations en matière de protection des données prévues par le contrat et de veiller à ce que l’entreprise de sous-traitance respecte pleinement les dispositions relatives à la protection des données et les exigences contractuelles.
2. **Responsabilité**
   1. Le mandant répond envers la personne concernée de la réparation de dommages ou d’autres prétentions qui surviennent en lien avec le traitement de données personnelles. Un recours direct contre le sous-traitant n’est autorisé que si ce dernier a fait preuve d’une négligence grave ou a intentionnellement enfreint les dispositions du présent contrat.
3. **Dispositions finales**
   1. Toute modification ou tout complément au présent contrat ou à une partie de celui-ci doit revêtir la forme écrite.
   2. Si une clause du présent contrat est déclarée nulle ou inapplicable ou si le présent contrat présente une lacune, la validité et l’applicabilité des autres clauses du contrat n’en sont pas affectées. La clause nulle ou inapplicable est remplacée ou la lacune est comblée par une clause valable et applicable qui, du point de vue des parties, se rapproche autant que possible, sur le plan économique, de l’objectif poursuivi par la clause nulle ou inapplicable.
   3. Le présent accord est exclusivement régi par le droit suisse, à l’exclusion des règles de conflit de lois. Le for est … .

|  |  |
| --- | --- |
| Pour le mandant :  Date, lieu  Signature :  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Nom :  Poste :  Signature :  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Nom :  Poste : | Pour le mandataire :  Date, lieu  Signature :  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Nom :  Poste :  Signature :  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Nom :  Poste : |