**ANNEXE 7 : EXEMPLE D’AVENANT CONTRACTUEL POUR LES PRESTATAIRES INFORMATIQUES**

*Cet exemple d’avenant concerne un avenant relatif à un contrat pour la fourniture d’une solution informatique. Il peut être adapté aux prestations et services fournis par les autres prestataires.*

\* \* \*

**AVENANT AU CONTRAT N°\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Le présent avenant a pour objet de venir compléter le contrat n° \_\_\_\_\_\_\_\_\_\_\_\_ conclut entre les Parties et concernant la fourniture des prestations qui y sont prévues, afin de mettre en conformité le contrat avec les dispositions du Règlement 2016/679/UE du Parlement européen et du Conseil 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 (dit et ci-après « le RGPD »).

Il fait partie intégrante du contrat ***[Option]*** et remplace l’article \_\_ relatif à la protection des données.

1. **Engagements des Parties**

**1.1** Chaque Partie respectera les engagements prévus dans le présent article et veillera à ce que son personnel permanent ou temporaire et chacun de ses sous-traitants respectent ses termes.

A ce titre, dès lors que le Prestataire, dans le cadre de l’exécution des prestations telles que prévues au présent Contrat, est amené à traiter des données personnelles, au sens de la loi applicable, du Client et/ou des Utilisateurs (ci-après « les Données »), le Prestataire s’engage à :

* respecter les lois et réglementations applicables en matière de protection des données personnelles, c’est-à-dire le Règlement européen n°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 des données (ci-après « RGPD »).
* traiter de telles Données uniquement si cela est requis pour l’exécution des finalités listées ci-après et tel qu’autorisé ou exigé par la loi ;
* garder les Données strictement confidentielles ;
* prendre les mesures de sécurité organisationnelles, physiques et techniques appropriées afin de protéger les Données ;
* n’effectuer de transfert des Données en-dehors de l’Union européenne qu’avec l’autorisation préalable du Client et dans un cadre sécurisé conformément aux exigences de la législation applicable, c’est-à-dire vers un pays présentant un niveau de protection dit adéquat au sens des autorités européennes de protection des données personnelles, et notamment la CNIL.

**1.2** Le Client demeure « responsable du traitement » au sens de la réglementation applicable, des données personnelles de ses clients et/ou employés et/ou partenaires, qu’il peut fournir au Prestataire pour l’exécution du présent Contrat, et s’engage à respecter ladite réglementation applicable.

Le Prestataire est quant à lui « sous-traitant » au sens du RGPD.

1. **Obligations du Client**

**2.1 Finalités des traitements** : le Client détermine sous sa responsabilité les finalités des traitements confiés au Prestataire, lesquelles sont les suivantes : ***+++ ces éléments sont donnés à titre d’exemple pour les SSTI +++***

* hébergement des données, conforme aux exigences liées à l’hébergement de données de santé (agrément)
* accès aux données dans le cadre des prestations de maintenance et d’assistance

**2.2 Catégories des données personnelles à traiter** : les données personnelles que le Prestataire sera amené à manipuler concernent : ***+++ ces éléments sont donnés à titre d’exemple pour les SSTI +++***

* données administratives, de prévention et de suivi de la santé au travail

**2.3 Conservation des données** : les données personnelles confiées au Prestataire seront conservées par ses soins, pour le compte du Client, pendant la durée du Contrat. A son échéance, pour quelle que cause que ce soit, le Prestataire détruira l’ensemble des Données. ***+++ le processus de restitution des données est à prendre en compte si rien n’est prévu au contrat initial +++***

**2.4 Propriété des Données** : le Client conserve la responsabilité de sa base de données. Il est expressément convenu que pendant la durée et l’exécution du Contrat, et en cas de traitement de données personnelles par le Prestataire, celui-ci agira uniquement pour le compte et sur instructions du Client, sur la base des stipulations du présent Contrat, aux seules finalités et pendant les durées stipulées ci-avant. Le Prestataire s’engage à supprimer l’ensemble des données personnelles à première demande du Client, et en toute hypothèse à l’expiration du Contrat.

**2.5** Le Client s’engage par ailleurs à :

* permettre au Prestataire l’accès aux Données ;
* documenter par écrit toute instruction concernant le traitement des Données par le Prestataire ;
* veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD de la part du sous-traitant ;
* superviser le traitement.

1. **Obligations du Prestataire**

Dans le cadre de l’exécution du présent Contrat et de la fourniture du Progiciel, le Prestataire :

* fournit une Solution strictement respectueuse des principes de proportionnalité, de minimisation et de limitation des données personnelles, assurant que seules les données pertinentes, telles que définies par le Client, sont traitées au sein de la Solution, pour les seules finalités convenues et sous le contrôle des seules personnes ayant à en connaitre.
* met à disposition dans le cadre de la Solution les mesures techniques et organisationnelles appropriées afin de protéger les données personnelles confiées au Prestataire par le Client ou directement confiées par les personnes physiques concernées via la Solution, de manière permanente et documentée, contre la destruction accidentelle ou illégale, la perte accidentelle, l’altération, la diffusion ou l’accès non-autorisé.

Par ailleurs, le Prestataire s’engage à :

* traiter les données conformément aux instructions documentées du responsable de traitement figurant en annexe du présent contrat. Si le Prestataire considère qu’une instruction constitue une violation du RGPD, il en informe immédiatement le Client. En outre, si le Prestataire est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l’Union ou du droit de l’Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public
* garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat
* veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :
  + s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
  + reçoivent la formation nécessaire en matière de protection des données à caractère personnel
* prendre en compte, s’agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut

1. **Sous-traitance**

Le Prestataire peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le Client de tout changement envisagé concernant l’ajout ou le remplacement d’autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l’identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le Client dispose d’un délai maximum de 10 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le Client n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent Contrat pour le compte et selon les instructions du Client. Il appartient au Prestataire de s’assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD.

1. **Droit d’information des personnes concernées**

Il appartient au Client de fournir l’information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

Le Prestataire s’engage à apporter tout son soutien au Client afin de remplir cette obligation d’information.

1. **Exercice des droits des personnes concernées**

Dans la mesure du possible, le Prestataire doit aider le Client à s’acquitter de son obligation de donner suite aux demandes d’exercice des droits des personnes concernées : droit d’accès, de rectification, d’effacement et d’opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l’objet d’une décision individuelle automatisée (y compris le profilage).

Le sous-traitant doit répondre, au nom et pour le compte du responsable de traitement et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d’exercice de leurs droits, s’agissant des données faisant l’objet de la sous-traitance prévue par le présent contrat.

1. **Notification des violations de Données**

Le Prestataire indique / notifie au Client toute violation de données à caractère personnel dans les meilleurs délais et en tout état de cause dans un délai maximum de 24 heures après en avoir pris connaissance et par écrit. Cette notification est accompagnée de toute documentation utile afin de permettre au Client, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente.

1. **Limitation de l’utilisation des données**

Le Prestataire s’engage à s’abstenir d’exploiter ou utiliser, faire des copies ou créer des fichiers des données personnelles au sein du système d’information du Client à ses propres fins ou pour le compte de tiers. Le traitement d’une donnée personnelle correspondra strictement à l’exécution des finalités stipulées ci-avant, dans le seul cadre de l’exécution du Contrat.

1. **Modification et suppression des Données**

Durant l’exécution du Contrat, le Prestataire s’engage à modifier ou supprimer, à la demande du Client, et uniquement lorsque le Client n’a pas la possibilité de le faire lui-même, toute Donnée en sa possession, notamment en cas d’exercice par un individu de ses droits d’accès, de rectification et de suppression.