RGPD article 28
Engagement de conformité du sous-traitant

1. TRAITEMENT DES DONNEES PERSONNELLES

A titre liminaire, il est précisé que chacune des Parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel, et en particulier, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (« RGPD »).

L'adhérent a notamment sélectionné le Service de Prévention et de Santé au Travail au regard de son engagement quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à respecter les exigences du présent article et du droit applicable à la protection des données.

Il est convenu entre les Parties que l'adhérent est le responsable de traitement et que le PSTVL est le sous-traitant au sens du règlement européen précité.

L'adhérent en tant que responsable de traitement s'engage à respecter les principes de la protection des données et à ne transmettre au PSTVL que des données à caractère personnel obtenues licitement, conformément aux textes précités. Le PSTVL s'engage, quant à lui, à traiter les données uniquement pour les seules finalités qui font l'objet de la sous-traitance.

2. LA SOUS-TRAITANCE

Périmètre

L'employeur est tenu par la loi de prendre toutes les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale de ses salariés (article L. 4121-1 du Code du travail). L'employeur ne doit pas seulement diminuer le risque, mais l'empêcher. Cette obligation est une obligation de résultat[1].

Le traitement des données personnelles est donc mis en œuvre sur la base légale de l'obligation légale du Responsable de traitement.

Par convention d'adhésion auprès du PSTVL l'adhérent rempli son obligation légale.

	Objectif	**Moyens**
Adhérent	• Remplir une obligation légale de sécurité, • Etablir la convocation à la visite médicale.	• Désigner un service de santé au travail, Adhérer, • Transmettre des données permettant d'établir la convocation. • Déclarer les risques d'expositions
PSTVL	Par convention d'adhésion :	Par convention d'adhésion :

[1] Cour de cassation, chambre sociale, 22 février 2002, pourvoi n° 99-18389

	• Remplir une obligation légale de sécurité de l'adhérent vis-à-vis de ses salariés, • Etablir la convocation à la visite médicale des salariés du mandant.	• Collecter les données permettant d'établir la convocation et le DMST, • Mettre en œuvre la convocation à partir des données de contact du salarié, • Gérer la convocation selon les risques d'exposition déclarés par **l'adhérent**

Le PSTVL ne collecte des données de santé qu'auprès du salarié suivi.

Le PSTVL ne transmet aucune information relevant du secret médical à l'adhérent.

L'adhérent ne transmet aucune consigne au PSTVL pour la collecte de données nécessaires au DMST et la mise en œuvre du Dossier Médical en Santé au Travail.

Par conséquent, le PSTVL est Responsable de traitement du DMST.

Le traitement réalisé sur le DMST par PSTVL est exclu du périmètre de la sous-traitance.

2.1 Description du traitement de données à caractère personnel

Le PSTVL est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires à l'exécution du présent contrat. Ce traitement de données à caractère personnel a pour finalité la mise en œuvre de prestations de Santé au Travail pour l'adhérent.

Dans le cadre de ses missions, le PSTVL sera amené à traiter des données à caractère personnel concernant les salariés de l'adhérent et notamment leurs noms, prénoms, dates de naissance, postes de travail occupés, nature des contrats de travail et éventuellement leurs dossiers médicaux.

La nature du traitement consiste en : collecte, stockage, hébergement, utilisation des données personnelles en vue de l'exécution du Contrat.

La finalité du traitement est d'assurer :

- La gestion commerciale entre l'adhérent et PSTVL et les services de son offre socle,
- La gestion socio-administrative de ses services entre le PSTVL et le salarié concerné (organisation des visites médicales, entretien de suivi...).
- L'ouverture du Dossier médical en santé au Travail.

Les catégories de personnes concernées par ce traitement sont

- Les salariés suivis de l'adhérent,
- Les collaborateurs du PSTVL
- Les collaborateurs des sous-traitants du PSTVL (hébergeur, infogéreur et tiers archiveur)

RGPD article 28
Engagement de conformité du sous-traitant

2.2 Obligations du PSTVL

2.2.1 Le PSTVL s'engage

- à traiter les données uniquement pour les seules finalités définies au point 1 de la présente clause

- à traiter les données conformément aux instructions documentées du responsable de traitement figurant au présent contrat. Si PSTVL considère qu'une instruction constitue une violation du règlement général sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le responsable de traitement.

- à garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat.

- à 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. À ce titre, PSTVL s'engage à fournir la liste des personnes ayant accès aux données à caractère personnel et à la mettre à jour en cas de changement dans un délai maximum de sept (7) jours.

- à 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

2.2.2 Droit d'information des personnes concernées

Le PSTVL garantit que les personnes concernées par les opérations de traitement ont été informées des droits dont ils disposent dans les conditions des articles 13 ou 14 du RGPD (selon ce qui est applicable).

2.2.3 Exercice des droits des personnes

Le PSTVL garantit que les personnes concernées par le traitement de données à caractère personnel pourront exercer leurs droits d'accès, de rectification et d'effacement des données les concernant auprès du PSTVL et qu'ils pourront également en demander la portabilité et s'opposer aux traitements de leurs données ou en demander la limitation. Enfin, les titulaires de ces données pourront émettre des directives sur la conservation, la suppression ou la communication de leurs données personnelles après leur décès.

Le PSTVL s’engage à remplir ses obligations relatives à l’exercice du droit d’accès aux données de santé de la personne concernée dans un délai de 7 jours suivants l’accusé réception de la demande.

Le PSTVL a rédigé un protocole pour la mise à disposition du DMST aux salariés suivis, aux tiers de confiance.

Le PSTVL a rédigé une procédure de mise à disposition de données de santé aux tiers autorisés.

2.2.4 Notification des violations de données à caractère personnel

Le PSTVL notifie au responsable de traitement toute violation de données à caractère personnel dans les plus brefs délais après en avoir pris connaissance.

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

2.2.5 Appui du PSTVL auprès du responsable de traitement dans le cadre de ses obligations réglementaires

Le PSTVL appuie le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données à caractère personnel traitées dans le cadre de l'exécution du présent contrat et, pour la réalisation de la consultation préalable de l'autorité de contrôle.

Le PSTVL s'engage également à coopérer avec l'autorité de protection des Données Personnelles en coordination avec l'adhérent le cas échéant.

2.2.6 Mesures de sécurité

Le PSTVL est tenu de prendre toutes les mesures techniques et organisationnelles, afin de garantir la confidentialité et l'intégrité des données à caractère personnel et, d'éviter, que ces informations ne soient détruites, altérées ou divulguées à un tiers qui n'a pas à en connaître.

Le PSTVL s'engage à documenter de manière précise l'évaluation des mesures techniques et organisationnelles prises et à mettre à disposition du responsable de traitement cette documentation.

Notamment, le PSTVL s'engage à :

- Prendre toutes mesures de sécurité, notamment matérielles, pour assurer la confidentialité, la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat.

  Concrètement le PSTVL a mis en place -entre autres mesures- la pseudonymisation de données, le verrouillage automatique de postes, renforcé sa politique des mots de passe, le chiffrement de ses équipements, un pare-feu, une revue annuelle des habilitations, des mesures de journalisation, réseau interne non visible aux visiteurs, etc.

- Mettre en œuvre les moyens permettant de rétablir la disponibilité des Données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique (sauvegardes de données réalisées par des prestataires certifiés ISO 27001 et HDS).

- Traiter et héberger les Données exclusivement sur le territoire de l'Union Européenne et informer l'adhérent de la localisation exacte des lieux de Traitements de Données à caractère personnel de quelque nature qu'ils soient (hébergement, backup, maintenance, administration, helpdesk...).

- Ne prendre aucune copie des documents et supports d'informations qui lui sont confiés à l'exception de ceux nécessaires à l'exécution de la présente prestation prévue au Contrat,

- Effectuer des contrôles internes réguliers de la protection des Données Personnelles et en tenir les résultats à disposition de l'adhérent. A ce titre, le PSTVL déclare avoir mis une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du Traitement, et en fournir la preuve à première demande de l'adhérent ou de l'autorité de protection des Données.

Le PSTVL reconnaît que les données à caractère personnel utilisées et traitées dans le cadre du présent contrat sont la propriété de l'adhérent. Par conséquent, PSTVL s'interdit d'utiliser à quelque fin que ce soit, autre que pour la stricte exécution des prestations lui incombant au titre du présent contrat, ces données.

2.2.7 Conservation des données à caractère personnel

Les données à caractère personnel collectées sont conservées pour la durée nécessaire à l'accomplissement de ces finalités objets du contrat ou conformément à ce que la réglementation applicable exige.

Voici les durées de conservations du dossier médical en santé au travail applicables selon la législation en vigueur :

Article R461-3 du Code de Sécurité Sociale	**Tableau des maladies professionnelles**
Article R1112-7 Code de Santé publique	Durée de conservation d'un dossier médical des établissements de santé (20 ans).
Article R4429-6 du Code du travail	Exposition à des agents biologiques pathogènes (durée de conservation 10 à 40 ans à partir de la fin de l'exposition)
Article R4412-55 du Code du Travail	Exposition à des agents chimiques dangereux et agents cancérogènes, mutagènes ou toxiques pour la reproduction (durée de conservation 50 ans à partir de la fin de l'exposition)
Article 35 Décret 90-277 du 28 mars 1990	Décret relatif à la protection des travailleurs en milieu hyperbare (durée de conservation 20 ans à partir de la fin de l'exposition)
Article R4454-9 du Code du Travail	Exposition aux rayonnements ionisants (50 ans à partir de la fin de l'exposition)

Le PSTVL s'abstient en toute hypothèse de reproduire, exploiter ou utiliser les données à caractère personnel du responsable de traitement traitées à l'occasion du contrat, à ses propres fins ou pour le compte de tiers, et s'engage à modifier ou supprimer, soit à la demande du responsable de traitement, soit à la demande d'une personne concernée, toute données à caractère personnel traitée à l'occasion ou en fin d'exécution dudit Contrat.

Le responsable de traitement pourra requérir du PSTVL qu'il lui remette une attestation de suppression des données à caractère personnel de ses salariés.

2.2.8 Délégué à la protection des données (DPO)

Le PSTVL communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données conformément à l'article 37 du règlement général sur la protection des données.

Julianna Révi, DPO externalisée

dpo@pstvl.fr

2.2.9 Registre des catégories d'activités de traitement

Dans certaines hypothèses mentionnées à l'article 30§2 du règlement général sur la protection des données, le PSTVL devra tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement.

2.2.10 Documentation / audit

Le PSTVL met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations.

L'adhérent se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par le PSTVL. Toute non-conformité fera l'objet d'un plan d'action corrective qui devra être mis en place dans les meilleurs délais, aux frais du PSTVL.

2.2.11 Sous-traitance ultérieure

Le PSTVL ne pourra pas sous-traiter l'exécution des prestations à une autre société, sans l'accord préalable de l'adhérent. Tout sous-traitant ultérieur proposé par PSTVL devra faire l'objet d'une approbation préalable écrite de l'adhérent et sera soumis à l'ensemble des stipulations du présent article, sous la responsabilité du PSTVL.

Dans l'hypothèse d'une telle approbation, le sous-traitant ultérieur sera tenu de respecter les obligations du présent Contrat pour le compte et selon les instructions de l'adhérent. Il appartiendra au PSTVL 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 que le Traitement réponde aux exigences de la Réglementation.

Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des Données, le PSTVL demeure pleinement responsable devant l'adhérent de l'exécution par le sous-traitant de ses obligations.

Par exception au premier paragraphe, l'adhérent accepte d'ores et déjà le recours au sous- traitant ultérieur

- Proginov, hébergeur et infogéreur certifié
- Trustteam, éditeur de logiciel de gestion médicale en santé au travail
- Iron Montain, tiers archiveur certifié

2.2.12 Hébergement de Données de santé / certification

Les données traitées par PSTVL sont hébergées chez Proginov en France certifié hébergeur de santé (HDS) et certifié norme 27001. Vous pouvez consulter le lien du site de l'agence du numérique en santé concernant la certification HDS (hébergeur de données de santé) de notre hébergeur Proginov : https://esante.gouv.fr/labels-certifications/hds/liste-des-herbergeurs-certifies

2.2.13 Application de la réglementation européenne en matière de transferts de données en dehors de l'Espace Économique Européen

Le PSTVL s'assure qu'aucune Donnée à caractère personnel de l'adhérent n'est transférée hors de l'Espace Économique Européen par lui, ses propres sous-traitants, ou les personnes agissant sous son autorité ou pour son compte. L'adhérent se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect de cette obligation.

Il est ici précisé que les données sont traitées et hébergées en France.