1. **Préambule**

Le Prestataire est informé qu'il est susceptible d’avoir accès, dans le cadre des présentes, à des données à caractère personnel (ci-après « les Données ») appartenant au Client.

A ce titre, le Prestataire s’engage à utiliser les données qui lui sont confiées par le Client dans le strict respect des présentes dispositions contractuelles et de la législation et réglementation en vigueur et notamment au Règlement (UE)°2016/679 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 (ci-après « RGPD »).

*Décrire :*

* *Le type de prestation (maintenance, infogérance, hébergement, etc.)*
* *La nature des opérations réalisées sur les données,*
* *La ou les finalité(s) du traitement (pourquoi le prestataire a accès aux données pour les services fournis),*
* *Les données traitées et les catégories de personnes concernées*.
* *La durée du traitement*

Le Prestataire s’engage à ne pas traiter de données à caractère personnel pour ses besoins propres ou pour le compte de tiers.

1. **GLOSSAIRE**

Client : Établissement adhérent de la CAIH, utilisateur du marché SALOHME.

Prestataire : la société fournissant un ou plusieurs logiciels, services, matériels dans le cadre du marché SALOHME (Système d’achat de logiciels hors médical) de la CAIH, attribué à la société SCC SA le 03/02/2024 pour une durée de 4 ans.

Titulaire : la société SCC SA.

1. **Obligations du Prestataire vis-à-vis du Client**

Dans le cadre de ses prestations, le Prestataire mettra en œuvre toutes les mesures techniques et organisationnelles adaptées à l’état des connaissances, au contexte, aux finalités du traitement et aux risques afin de protéger les Données et prendra toutes les précautions nécessaires pour préserver la sécurité, la disponibilité, la confidentialité et l’intégrité de ces Données, notamment contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés.

Le Prestataire communiquera au Client l’ensemble des mesures prises pour garantir la sécurité des Données.

Par ailleurs, le Prestataire s’engage notamment à :

* Traiter les données uniquement pour la ou les seule(s) finalité(s) énoncée(s) ci-dessus et conformément aux instructions du Client. Si le Prestataire considère qu’une instruction constitue une violation du RGPD ou de toute autre disposition du droit de l’Union ou du droit des États membres relative à la protection des données, il en informe immédiatement le Client,
* Informer le Client s’il 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,
* 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 elles-mêmes la confidentialité et 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,
* Aider le Client pour la réalisation d’analyses d’impact relatives à la protection des données et pour la réalisation de la consultation préalable de l’autorité de contrôle,
* Communiquer au Client le nom et les coordonnées de son délégué à la protection des données, s’il en a désigné un conformément à l’article 37 du RGPD,
* Indiquer au client si le traitement fait l’objet d’un transfert de données hors de l’Union Européenne, le cas échéant apporter les éléments de preuve exigés par le RGPD, notamment la signature des clauses contractuelles types de la commission européenne concernant un transfert de données dans un pays ne remplissant pas les garanties adéquates.

1. **Sous-traitance**

Le Prestataire peut faire appel à un sous-traitant 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 de 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 de trente (30) 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 susvisé.

Il appartient au Prestataire de s’assurer que le sous-traitant respecte les obligations du présent contrat et présente les mêmes garanties quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la réglementation sur la protection des données. Si le sous-traitant ne remplit pas ses obligations en matière de protection des données, le Prestataire demeure pleinement responsable devant le Client.

1. **Exercice des droits des personnes**

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).

Si les personnes concernées venaient à exercer auprès du Prestataire des demandes d’exercice de leurs droits, ce dernier doit adresser ces demandes dès réception par courrier électronique à l’adresse du responsable de la protection des données du Client.

1. **Notification des violations de données à caractère personnel**

Le Prestataire notifie au Client toute violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance par mail à l’adresse du responsable de la protection des données du Client. Cette notification est accompagnée de la description de la violation, les données concernées, la cause et toute documentation utile afin de permettre au Client, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente.

1. **Mesures de sécurité**

Le Prestataire s’engage à mettre en œuvre les mesures de sécurité suivantes :

*[Décrire les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres :*

* *La pseudonymisation et le chiffrement des données à caractère personnel*
* *Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;*
* *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 ;*
* *Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement]*

1. **Sort des données**

A l’expiration du présent contrat, pour quelque cause que ce soit, le Prestataire devra sans délai et en fonction de la demande du Client, soit détruire les données et toute copie quel qu’en soit le support, soit restituer les données et détruire les copies existantes quel qu’en soit le support, sauf à ce qu’il soit tenu de conserver les données en application de la Règlementation relative à la protection des données, ce dont il s’engage à informer le Client.

Il appartiendra au Prestataire de s’assurer que toutes données ou copies de données qui auraient pu être transmises à un tiers soient également détruites.

En tout état de cause le Prestataire devra apporter la preuve de ces destructions.

1. **Registre des catégories d’activités de traitement**

Conformément au RGPD, le Prestataire déclare tenir par écrit un registre de toutes les catégories d’activités de traitement effectuées pour le compte du Client comprenant :

* Le nom et les coordonnées du Client pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
* Les catégories de traitements effectués pour le compte du Client ;
* Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du RGPD, les documents attestant de l'existence de garanties appropriées ;
* Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

1. **Audit**

Le Client pourra faire procéder, une fois par an, par un cabinet d’audit tenu au secret professionnel et agréé par les deux parties, à l’examen de tout élément permettant de s’assurer de la bonne exécution des dispositions définies au présent contrat. Cet audit aura lieu aux heures d’ouverture des bureaux du Prestataire et sous réserve d’en avoir informé le Prestataire au moins trente (30) jours avant sa mise en œuvre, par lettre recommandée avec accusé de réception. Les frais d’audit seront à la charge du Client sauf dans le cas où l’audit révèlerait un manquement dans le cadre des obligations du Prestataire.

Cet audit pourra être effectué par un cabinet extérieur, pour autant que celui-ci n’exerce pas lui-même une activité concurrente de celle du Prestataire.

Un exemplaire du rapport d’audit sera remis au Prestataire.

Si le rapport d’audit fait apparaître un non-respect des obligations du Prestataire, ce dernier s’engage, dans le cadre d’un plan d’action, à mettre en œuvre, à ses frais, les mesures correctives nécessaires dans un délai de trente (30) jours calendaires à compter de la remise du rapport d’audit.

Les Parties conviennent qu’en tout état de cause, la procédure d’audit ou son absence de mise en œuvre n’exonèrent d’aucune manière le Prestataire du respect de ses obligations contractuelles et ne peuvent être interprétées comme valant acceptation de la qualité des Prestations effectuées.

1. **Obligations du Client vis-à-vis du Prestataire**

Le Client s’engage à :

* Fournir au Prestataire les données nécessaires à la fourniture des services prévus au Contrat,
* Documenter par écrit toute instruction concernant le traitement des données par le Prestataire,
* Veiller, au préalable et pendant toute la durée du Contrat, au respect des obligations prévues par la réglementation sur la protection des données et notamment à l’information des personnes concernées,
* Superviser le traitement, y compris réaliser les audits et les inspections auprès du Prestataire.

1. **Transfert de données**

Le Prestataire s’engage à respecter les principes décrits au chapitre V du RGPD.

Date et signature :

Pour le Prestataire Pour la CAIH