

**Clauses de conformité au Règlement Général sur la Protection des Données**

**Groupement Hospitalier de Territoire des Alpes du Sud**

Etablissement support : Centre Hospitalier Intercommunal des Alpes du Sud (CHICAS)

1, place Auguste Muret

05000 GAP

(ci-après, « le responsable de traitement »)

Etablissement(s) concerné(s) au niveau du Groupement Hospitalier de Territoire (sous direction commune) :

CHICAS

Centre Hospitalier les Escartons de Briançon

Centre Hospitalier d’Embrun

Centre Hospitalier d’Aiguilles-en-Queyras

d'une part,

ET

**Société XXXX fournissant le logiciel/ la prestation XXXX**

(ci-après, « le sous-traitant »)

d’autre part,

# I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s’engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les 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 applicable à compter du 25 mai 2018 (ci-après, « le règlement européen sur la protection des données »).

# II. Description du traitement faisant l’objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) [...].

La ou les **finalité(s)** du traitement sont (à décrire lors de la signature) :

……………………………………………………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………………………………………..

**La nature des opérations** réalisées sur les données est (cochez les cases correspondantes lors de la signature) :

☐ la collecte de DCP

☐ l’enregistrement de DCP

☐ l’organisation, la structuration de DCP

☐ la conservation de DCP

☐ l’adaptation, la modification, l’extraction de DCP

☐ la consultation, l’utilisation de DCP

☐ la communication de DCP par transmission, la diffusion ou toute autre forme de mise à disposition

☐ le rapprochement, l’interconnexion de DCP

☐ la limitation, l’effacement, la destruction de DCP

**Les données à caractère personnel traitées** sont (cochez les cases correspondantes lors de la signature) :

☐ État-civil, identité, données d'identification, images (ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.

☐Vie personnelle (ex. habitudes de vie, situation familiale, etc.)

☐Vie professionnelle (ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)

☐Informations d’ordre économique et financier (ex. revenus, situation financière, données bancaires, etc.)

☐ Données de connexion (ex. adresses IP, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)

☐ Données de localisation (ex. déplacements, données GPS, GSM, ...)

☐ Internet (ex. cookies, traceurs, données de navigation, mesures d’audience, ...)

☐ Autres catégories de données

**Données sensibles :**

☐ origine prétendument raciale ou ethnique,

☐ opinions politiques,

☐ convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes,

☐ données génétiques et biométriques,

☐ des données concernant la santé,

☐ données concernant la vie sexuelle ou l’orientation sexuelle des personnes,

☐ données relatives aux condamnations pénales ou aux infractions,

☐ numéro d'identification national unique (NIR ou numéro de sécurité sociale).

Préciser les données exactes qui sont traitées (à remplir lors de la signature)

……………………………………………………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………………………………………..

Les **catégories de personnes concernées** sont(cochez les cases correspondantes lors de la signature) **:**

Patient de l’établissement

Professionnels de l’établissement

Autre (à préciser) : ………………………………………….

# III. Durée du contrat

Le présent contrat entre en vigueur à compter du ……/………/……… pour une durée de …………….……..

# IV. Obligations du sous-traitant vis-à-vis du responsable de traitement

## Obligations générales :

Le sous-traitant s'engage à :

* traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet de la sous-traitance
* traiter les données conformément aux instructions documentées du responsable de traitement figurant en annexe du présent contrat. Si le sous-traitant considère qu’une instruction constitue une violation du règlement européen 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. En outre, si le sous-traitant 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
* aider le responsable de traitement pour la réalisation d’analyses d’impact relative à la protection des données.
* aider le responsable de traitement pour la réalisation de la consultation préalable de l’autorité de contrôle.

## Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement 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).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d’exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique au Délégué à la Protection des Données du groupement hospitalier de territoire ([dpo@chicas-gap.fr](mailto:dpo@chicas-gap.fr)).

## Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance par courriel avec accusé de réception à l’adresse suivante : [dpo@chicas-gap.fr](mailto:dpo@chicas-gap.fr). 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. Il est rappelé que la notification doit se faire dans les 72h à l’autorité de contrôle. Ainsi le sous-traitant devra transmettre toute information en sa possession permettant de réaliser la déclaration compte tenu du fait que la notification contient au moins :

* la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
* le nom et les coordonnées du délégué à la protection des données ;
* la description des conséquences probables de la violation de données à caractère personnel ;
* la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n’est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

## Information des personnes concernées par une violation

Le sous-traitant s’engage à aider le responsable de traitement à respecter ses obligations en la matière.

## Sous-traitance ultérieure

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Le sous-traitant doit communiquer lors de la signature des présentes clauses la **liste des sous-traitants amenés à intervenir sur les données** du responsable de traitement. En cas de changement envisagé concernant l’ajout ou le remplacement d’autres sous-traitants, le **sous-traitant informe préalablement et par écrit** le responsable de traitement. 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 responsable de traitement dispose d’un délai minimum de 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 responsable de traitement 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 responsable de traitement. Il appartient au sous-traitant initial de s’assurer que le sous-traitant ultérieur présente les mêmes garanties et que ces garanties sont suffisantes. Les mesures techniques et organisationnelles doivent être appropriées à la sensibilité des données traitées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l’exécution par l’autre sous-traitant de ses obligations.

## Transfert de données vers un pays tiers ou une organisation internationale (hors UE)

Le sous-traitant s’engage à ce que le traitement de données n’ait lieu que dans un Etat membre de l’Union Européenne. A défaut, le sous-traitant s’engage à s’assurer que tout transfert de données à caractère personnel vers un pays tiers soit réalisé vers un pays disposant d’un niveau de protection adéquat au sens de l’article 45 du RGPD. Tout transfert de données en **dehors de l’UE nécessitera le consentement écrit préalable** du responsable de traitement et ne pourra être réalisé que si les exigences légales ou règlementaires sont respectées.

## Mesures de sécurité

Le sous-traitant s’engage à mettre en œuvre *a minima* les mesures de sécurité suivantes :

* la pseudonymisation et le chiffrement des données à caractère personnel
* les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante 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
* en cas de traitement de données de santé, le sous-traitant devra être conforme au cadre juridique de l’hébergement de données de santé fixé à l’article L.1111-8 du Code de Santé Publique et à la circulaire n0 6282-SG du 5 juillet relative à la doctrine d’utilisation de l’informatique en nuage (qualification SecNumCloud)

## Durée de conservation et sort des données

Le sous-traitant s’engage à appliquer les durées de conservation légales au regard des données traitées via les outils et les prestations proposées ou, le cas échéant, les durées correspondant à la finalité du traitement.

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s’engage à restituer toutes les données à caractère personnel au responsable de traitement sous une forme exploitable et de manière chiffrée.

Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

## Délégué à la protection des données

Le sous-traitant communique au responsable de traitement 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 règlement européen sur la protection des données.

Le délégué à la protection des données est (à remplir lors de la signature par le sous-traitant) :

Prénom, nom : ………………………………………………………………………………………………………………………………….

Adresse postale : ……………………………………………………………………………………………………………………………….

Courriel : ……………………………………………………………………………………………………………………………………………

Téléphone : …../……./……./……/…….

## Registre des catégories d’activités de traitement

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d’activités de traitement effectuées pour le compte du responsable de traitement comprenant :

* le nom et les coordonnées du responsable de traitement 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 responsable du traitement;
* 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 règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées;

Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :

* la pseudonymisation et le chiffrement des données à caractère personnel;
* des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
* des 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.

## Documentation

Le sous-traitant s’engage à mettre à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

## Analyse d’impact sur la vie privée

Le sous-traitant s’engage à apporter une assistance raisonnable dans la réalisation des analyses d’impact relatives à la protection des données dans la mesure où le responsable de traitement est tenu de le faire en vertu de la loi applicable.

# VI. Obligations du responsable de traitement

## Obligations générales

Le responsable de traitement s’engage à :

* fournir au sous-traitant les données visées au § II des présentes clauses
* documenter par écrit toute instruction concernant le traitement des données par le sous-traitant
* veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant
* superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant

## Exercice des droits des personnes

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

Le responsable de traitement est responsable de la réponse 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). Il pourra être aidé par le sous-traitant.

## Notification des violations à l’autorité de contrôle

Il appartient au responsable de traitement de réaliser les notifications de violation à l’autorité de contrôle à partir des éléments en sa possession et, le cas échéant, des éléments fournis par le sous-traitant.

## Information des personnes concernées par une violation

Le responsable de traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

* la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
* le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
* la description des conséquences probables de la violation de données à caractère personnel ;
* la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

**Signature**

Date, Cachet de l’entreprise, Prénom et Nom du signataire :