

Contrat de sous-traitance relatif à la protection des données à caractère personnel

Table des matières

[1. Objet 4](#_Toc124943746)

[2. Traitements de données faisant l’objet de la sous-traitance 4](#_Toc124943747)

[2.1 Nature(s) et finalité(s) des opérations 5](#_Toc124943748)

[2.2 Nature des données et catégories des personnes concernées 5](#_Toc124943749)

[3. Durée du contrat 5](#_Toc124943750)

[4. Obligations du Sous-traitant 5](#_Toc124943751)

[4.1 Obligations réglementaires 5](#_Toc124943752)

[4.2 Obligations de sécurité et de confidentialité 7](#_Toc124943753)

[4.3 Obligation d’assistance, d’alerte et de conseil 8](#_Toc124943754)

[4.4 Hébergement de données de santé 9](#_Toc124943755)

[4.5 Sous-traitance ultérieure 9](#_Toc124943756)

[5. Obligations du Responsable de traitement 10](#_Toc124943757)

[6. Droit d’information des personnes concernées 11](#_Toc124943758)

[7. Durée de conservation des données 11](#_Toc124943759)

[8. Exercice des droits des personnes concernées 11](#_Toc124943760)

[9. Notification des violations de données à caractère personnel 12](#_Toc124943761)

[10. Sort des données 13](#_Toc124943762)

[11. Délégué à la protection des données 13](#_Toc124943763)

[12. Registre des catégories d’activités de traitement 14](#_Toc124943764)

[13. Flux transfrontaliers de données 14](#_Toc124943765)

[14. Documentation 14](#_Toc124943766)

[15. Responsabilité et Assurance 14](#_Toc124943767)

[15.1 Responsabilité du Sous-traitant 14](#_Toc124943768)

[15.2 Engagement de confidentialité en cas d’opération de maintenance ou de Télémaintenance dans le cadre d’une sous-traitance 15](#_Toc124943769)

[15.3 Assurance 15](#_Toc124943770)

[16. Annexe 17](#_Toc124943771)

[16. Description des traitements 17](#_Toc124943772)

Entre les soussignés :

**[Société prestataire],** Immatriculé sous le n° [numéro SIREN], dont le siège social se situe [adresse postale]

Représenté [Nom – Prénom et fonction du représentant]

(ci-après, « **Sous-traitant** » ou le « **Prestataire** »)

d'une part,

ET

**Le Groupement Régional d’appui au développement de la e-santé** (GRADeS Occitanie),

Immatriculé sous le n° SIREN : 130 023 807, dont le siège social se situe au 10 Rue des Trente-six Ponts, 31400 Toulouse

Représenté par Madame Julie DURAND, en qualité de Directrice

(ci-après, « le **Responsable de traitement** » ou le « **Client** »)

d’autre part,

Ci-après individuellement dénommés une « **Partie** » et ensemble les « **Parties** ».

Etant préalablement exposé que :

Les **Parties** ont signé un marché n°2026-01 avant pour objet la tierce maintenance applicative pour le TUCS du GRADeS E santé Occitanie. Dans le cadre de l’exécution des prestations qui lui sont confiées, le **Prestataire** est amené à traiter des données à caractère personnel pour le compte du **Client**.

Les **Parties** reconnaissent expressément que, dans ce cadre, le **Client** définit les moyens et les finalités du ou des traitements en cause, de sorte qu’il est le responsable du ou desdits traitements, le **Prestataire** agissant en qualité de sous-traitant, conformément à la réglementation relative à la vie privée.

Préambule

Depuis le 25 mai 2018, le règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (ci-après, « le **RGPD** ») consacre une logique de responsabilisation de tous les acteurs impliqués dans le traitement des données à caractère personnel, dès lors qu’elles concernent des résidents européens, que ces acteurs soient ou non établis au sein de l’Union européenne.

Il impose des obligations spécifiques aux sous-traitants qui doivent notamment aider les responsables de traitement dans leur démarche permanente de mise en conformité de leurs traitements. C’est pourquoi le **Client** inclut les présentes clauses de conformité au **RGPD** afin de définir clairement les responsabilités de chacune des **Parties**.

Le **Prestataire** reconnaît le caractère strictement confidentiel de toutes les données à caractère personnel auxquelles il a ainsi accès. Par conséquent, il reconnaît que l’ensemble de ces données est soumis au respect de la règlementation applicable en France et dans l’Union européenne dans le domaine de la protection des données à caractère personnel incluant notamment :

* Les textes adoptés au sein de l’Union Européenne (**RGPD**) et les lois locales susceptibles de s’appliquer aux données à caractère personnel traitées dans le cadre du contrat,
* Les textes et décisions émanant d’autorités de contrôle, notamment de la Commission Nationale de l’Informatique et des libertés (la loi informatique et libertés, etc.),
* Le cas échéant, les textes, recommandations édictées ou reprises par le Comité européen à la protection des données ou de toute organisation ou autorité dans le secteur de la protection des données à caractère personnel,
* Le cas échéant, les référentiels sectoriels applicables, ayant trait aux traitements de Données à caractère personnel concernant la santé, et qui relève de la vie privée et du secret professionnel.

# Objet

Le présent accord relatif à la protection des données à caractère personnel (ci-après, l’«**Accord**») a pour objet de définir les conditions dans lesquelles le **Sous-traitant** s’engage à effectuer, dans le respect de la réglementation en vigueur et pour le compte du **Responsable de traitement**, les opérations de traitement de données à caractère personnel, définies ci-après, nécessaires à l’exécution des prestations confiées.

# Traitements de données faisant l’objet de la sous-traitance

Le **Sous-traitant** est autorisé pendant toute la durée du contrat à traiter pour le compte du **Responsable de traitement** des données à caractère personnel nécessaires pour la fourniture et l’exécution des prestations définies dans le marché.

Pour l’exécution du service objet du présent contrat, le **Responsable de traitement** met à la disposition du **Sous-traitant** les informations nécessaires suivantes :

## 2.1 Nature(s) et finalité(s) des opérations

La nature des opérations réalisées sur les données est : cf. 16. Annexe du présent Accord.

La ou les finalité(s) du traitement sont : cf. 16. Annexe du présent Accord.

## 2.2 Nature des données et catégories des personnes concernées

Les données à caractère personnel traitées sont cf. 16. Annexe du présent Accord.

Les catégories de personnes concernées sont cf. 16. Annexe du présent Accord.

# Durée du contrat

Le présent **Accord** entre en vigueur à compter de la signature de l’Accord pour toute la durée du marché n°2026-01.

# Obligations du Sous-traitant

## 4.1 Obligations réglementaires

Lorsqu’un sous-traitant intervient dans la mise en œuvre d’un traitement de données à caractère personnel, il doit offrir « des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée » (article 28 du règlement européen).

Concrètement, cela implique que le **Sous-traitant** doit :

* Etablir avec le **Responsable de traitement** le présent **Accord** afin de préciser les obligations de chaque **Partie** et reprenant les dispositions de l’article 28 du règlement européen,
* Traiter les données à caractère personnel conformément aux « instructions documentées » du **Responsable de traitement**, et les recenser par écrit,
* Demander l’autorisation écrite du **Responsable de traitement** si, en tant que sous-traitant, il fait lui-même appel à un sous-traitant,
* Mettre à la disposition du **Responsable de traitement** toutes les informations nécessaires pour démontrer le respect de ses obligations et pour permettre la réalisation d’audits (sur la base, par exemple, du référentiel de la CNIL pour la délivrance de labels en matière de procédure d'audit),
* Tenir un registre qui recense tous les traitements qu’il effectue pour le compte du **Responsable de traitement**,
* Traiter les données à caractère personnel uniquement pour les seules finalités qui font l’objet de la sous-traitance,
* Notifier au **Responsable de traitement** toute violation de données à caractère personnel,

Lorsque le **Sous-traitant** est tenu de procéder à un traitement sur les données en vertu du droit de l’Union ou du droit de l’État membre auquel il est soumis, il doit informer le **Responsable de traitement** de cette obligation juridique préalablement au traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public. Les mêmes conditions s’appliqueront au traitement réalisé à la demande d’une autorité agissant dûment dans le cadre de ses pouvoirs ou d’une juridiction compétente agissant en dernier ressort.

Au terme de la prestation et selon les instructions du **Responsable de traitement**, le **Sous-traitant** doit, après réversibilité complète validée par écrit par le **Responsable de traitement** :

* Supprimer toutes les données.
* Détruire les copies existantes sauf obligation légale de les conserver.

Le cas échéant, si cette démarche s’avère nécessaire, le **Sous-traitant** s’engage, sans surcout, à réaliser et à fournir toute analyse d’impact relative à la protection des données traitées dans le cadre des **Prestations.**

Aussi, le **Sous-traitant** s’interdit de :

* Traiter et/ou consulter les données à caractère personnel à d’autres fins que l’exécution des prestations qu’il effectue pour le **Responsable de traitement** au titre des **Prestations** (même si l’accès à ces données est techniquement possible),
* Divulguer, sous quelque forme que ce soit, tout ou partie des données à caractère personnel traitées, et ce y compris à ces sous-traitants (ci-après nommés « **Sous-traitant ultérieur »)**, en dehors des cas prévus dans le présent **Accord** ou de ceux prévus par une disposition légale ou réglementaire,
* Prendre copie ou stocker, quelles qu'en soient la forme et la finalité, tout ou partie des informations ou données à caractère personnel contenues sur les supports ou documents qui lui ont été confiés ou qu’il a recueillis, en dehors des cas couverts par le présent **Accord**.

## 4.2 Obligations de sécurité et de confidentialité

Conformément à la réglementation sur la protection des données, le **Sous-traitant** prend toutes précautions utiles notamment au regard de la nature des données à caractère personnel et des risques présentés par les traitements, pour préserver la sécurité et la confidentialité des données à caractère personnel transmises, traitées ou conservées et empêcher leur déformation, altération, endommagement, destruction de manière fortuite ou illicite, perte, divulgation et/ou tout accès à ces données par des tiers non autorisés préalablement de manière accidentelle ou illicite.

Le **Sous-traitant** met en œuvre toutes les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel, en prenant en compte l'état des connaissances, les coûts de mise en œuvre et la nature, la portée, le contexte et les finalités des traitements.

A ce titre, le **Sous-traitant** s’engage notamment à réaliser les traitements dans le respect de l’état de l’art et, selon les besoins, à mettre en œuvre les mesures suivantes, conformément aux règles issues de la politique générale de sécurité des systèmes d’information de santé (PGSSI-S) :

* La pseudonymisation et le chiffrement des données à caractère personnel,
* Informer et sensibiliser son personnel,
* Accès aux données à l’aide d’un moyen d’authentification conforme aux recommandations de la CNIL et, selon les besoins, au référentiel d’identification des acteurs sanitaires et médico-sociaux et au référentiel d’authentification des acteurs de santé issus de la PGSSI-S,
* Définition des profils d’habilitation, suppression des permissions d’accès obsolètes et limitation de l’accès aux outils et interfaces d’administration aux seules personnes habilitées,
* Mise en œuvre des systèmes automatiques de traçabilité (journaux),
* Définition d’une politique de sécurité adaptée aux risques du traitement et incluant les objectifs de sécurité ainsi que les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre,
* Mise en œuvre des moyens permettant de garantir la confidentialité, l’intégrité, la disponibilité et la résilience constantes de la solution et des services de traitement,
* Mise en œuvre des moyens permettant de rétablir la disponibilité des données à caractère personnel et l’accès à celles-ci dans les délais appropriés en cas d’incident physique ou technique,
* Mise en œuvre d’une procédure visant à tester, à analyser et à évaluer régulièrement l’efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement,
* Lorsque le **Sous-traitant** intervient à distance sur les données, le cas échéant, pour les besoins des prestations d’installation, de paramétrage, de télésurveillance, de télémaintenance et de téléassistance, il s’engage à se conformer aux règles ci-après précisées, issues de la PGSSI-S et, en particulier, celles issues du référentiel sur les règles pour les interventions à distance sur les systèmes d’information de santé.
* Isoler les données du **Responsable de traitement** de toute autre donnée à caractère personnel qu’il pourrait traiter par ailleurs pour le compte de tiers ou pour son propre compte,
* Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent Accord. Ainsi, le **Sous-traitant** prendra toute mesure permettant d’empêcher toute utilisation détournée, malveillante ou frauduleuse des données à caractère personnel. De même, les personnes autorisées à traiter les données doivent s’engager à respecter la confidentialité ou être soumis à une obligation légale appropriée de confidentialité et le Sous-traitant doit veiller à ce qu’elles reçoivent la formation nécessaire en matière de protection des données.

## 4.3 Obligation d’assistance, d’alerte et de conseil

Le **Sous-traitant** doit également assister et conseiller le **Responsable de traitement** dans leur conformité à certaines obligations prévues par le règlement européen (analyses d’impact, notification de violation, sécurité, confidentialité, destruction des données, contribution aux audits...) :

* Si une « instruction documentée » du **Responsable de traitement** constitue une violation des règles en matière de protection des données, le **Sous-traitant** doit l’en informer immédiatement,
* Lorsqu’une personne exerce ses droits (accès, rectification, effacement, portabilité, ...) le **Sous-traitant** doit, dans toute la mesure du possible, aider le **Responsable de traitement** à donner suite à cette demande,
* Compte tenu des informations à sa disposition, le **Sous-traitant** doit aider le **Responsable de traitement** à garantir le respect des obligations en matière de sécurité du traitement, de notification de violation de données et d’analyse d’impact relative à la protection des données,
* Le **Sous-traitant** aide le **Responsable de traitement** à respecter les obligations pesant sur lui au regard de la réglementation sur la protection des données ou, lorsqu’il agit en tant que **Sous-traitant**, à aider ses bénéficiaires ou ses utilisateurs, responsables de traitement, à respecter les obligations qui pèsent sur eux, telles que notamment :
  + Ses obligations de notification à la CNIL ou de communication à la personne concernée d’une violation de données à caractère personnel,
  + Son obligation de consultation préalable de la CNIL visée à l’article 36 du **RGPD**.
* Lorsque le **Responsable de traitement** décide ou est contraint de réaliser une analyse d’impact relative à la protection des données pour un traitement qu’il opère, le **Sous-traitant** s’engage, sans surcoût, à l’aider pour la réalisation de cette analyse,
* En cas de contrôle de la CNIL, les **Parties** s’engagent à coopérer entre elles et avec la CNIL :
  + Si le contrôle est effectué chez **Sous-traitant** et concerne les traitements mis en œuvre au nom et pour le compte du **Responsable de traitement**, le **Sous-traitant** en informe immédiatement le **Responsable de traitement** et s’engage à ne prendre aucun engagement pour lui.
  + Si le contrôle est effectué chez le **Responsable de traitement** et porte notamment sur les services délivrés par le **Sous-traitant**, ce dernier fournit toute aide dont le **Responsable de traitement** pourrait avoir besoin ou qui s’avèrerait nécessaire.

## 4.4 Hébergement de données de santé

Dans le cadre de l’infogérance, le **Sous-traitant** s’engage à être certifié hébergeur de données de santé conformément à l’article L.1111-8 al. 5 du Code de la santé publique, et au décret relatif à l’hébergement de données de santé à caractère personnel et au référentiel de certification approuvé par l’arrêté du 11 juin 2018.

## 4.5 Sous-traitance ultérieure

Le **Sous-traitant** peut faire appel à un autre sous-traitant (le Sous-traitant ultérieur) pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le **Responsable de traitement** 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 Responsable de traitement dispose d’un délai minium de 48h 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** ne peut sous-traiter, au sens de la réglementation sur la protection des données, tout ou partie des prestations, notamment vers un pays qui n’est pas situé dans l’Union Européenne, qu’après avoir obtenu l’accord préalable, écrit et exprès du **Responsable de traitement**.

Dans tous les cas, le **Sous-traitant** s’engage à :

* Informer et signer avec son ou ses **sous-traitants ultérieurs** un contrat écrit faisant référence à cet **Accord**, et imposant au **Sous-traitant ultérieur** les mêmes obligations en matière de protection des données que celles fixées dans le présent **Accord**,
* Mettre à la charge du **Sous-traitant ultérieur** toutes les obligations nécessaires pour que soient respectées la confidentialité, la sécurité et l’intégrité des données, et pour que lesdites données ne puissent être ni cédées ou louées à un tiers à titre gratuit ou non, ni utilisées à d’autres fins que celles définies dans le présent **Accord**,
* Communiquer au **Responsable de traitement** une copie du contrat conclu avec son ou ses **Sous-traitants ultérieurs** et à défaut une description des éléments essentiels du contrat, incluant la mise en œuvre des obligations relatives à la protection des données.

Le **Sous-traitant ultérieur** est tenu de respecter les obligations du présent **Accord** pour le compte et selon les instructions du **Responsable de traitement**. Il appartient au **Sous-traitant** 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 du règlement européen sur la protection des données.

Lorsque les **Sous-traitants ultérieurs** ne remplissent pas leurs obligations en matière de protection des données et en regard des dispositions du présent **Accord**, le **Sous-traitant** en demeure pleinement responsable devant le **Responsable de traitement**.

Le **Sous-traitant** s’engage à procéder à des vérifications régulières et appropriées, pendant la toute la durée du présent **Accord**, du respect par les **Sous-traitants Ultérieurs** de leurs obligations contractuelles et/ou règlementaires en matière de protection des données à caractère personnel. Le **Sous-traitant** s’engage à documenter les résultats desdites vérifications et à les communiquer au **Responsable de traitement** sur demande écrite de ce dernier.

# Obligations du Responsable de traitement

Le **Responsable de traitement** s’engage à :

* Déterminer les finalités des traitements de données sous-traités,
* Fournir par écrit toute « instruction documentée » concernant le traitement des données effectué 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**,
* Respecter ses obligations issues du **RGPD** en ce qui concerne les traitements des données sous-traités et notamment son obligation d’informer les personnes concernées sur le traitement de leurs données à caractère personnel dans le cadre des **Prestations**. A cet égard, le **Sous-traitant** s’engage à fournir au **Responsable de traitement** toutes les informations nécessaires, y compris toute information technique concernant les **Prestations**, pour lui permettre de réaliser une information complète et utile des personnes concernées relative aux traitements de leurs données à caractères personnel.

# Droit d’information des personnes concernées

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.

# Durée de conservation des données

Il appartient au **Responsable de traitement** de fixer la durée de conservation des données.

# Exercice des droits des personnes concernées

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 à dpo@esante-occitanie.fr

Cette notification est accompagnée de toute information utile afin de permettre au **Responsable de traitement** de donner suite à la demande.

Le **Sous-traitant** s’engage à aider, sans surcoût et dans toute la mesure du possible, le **Responsable de traitement** à s’acquitter de son obligation de donner suite aux demandes d’exercice des droits des personnes concernées qu’il s’agisse (sans que cela soit limitatif) du droit : d’accès, de rectification, d’effacement, d’opposition, de limitation du traitement, de portabilité des données, de ne pas faire l’objet d’une décision individuelle automatisée (y compris le profilage).

# 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 et par les moyens suivants :

* Courriel adressé à dpo@esante-occitanie.fr

Ceci comprend tout incident entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel traitées ou conservées de façon non conforme aux instructions du **Responsable de traitement** et à la réglementation sur la protection des données à caractère personnel, ou l'accès non autorisé à de telles données et par tous moyens.

Cette notification est accompagnée dans le même temps ou par la suite (mais en tout état de cause promptement) de toute documentation utile afin de permettre au **Responsable de traitement** de :

* Notifier cette violation à l’autorité de contrôle compétente (la CNIL) dans les 72h après en avoir pris connaissance et, le cas échéant de communiquer ladite violation aux personnes concernées,
* Lorsqu’il agit en qualité de sous-traitant, de notifier cette violation aux responsables de traitement.

La documentation attendue doit permettre de communiquer, en des termes clairs et simples, 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.

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.

# 10. Sort des données

Au terme des prestations impliquant un traitement des données à caractère personnel ou au plus tard au terme du contrat, le **Sous-traitant** restitue les fichiers et données à caractère personnel au **Responsable de traitement** ou à toute personne tierce désignée dans les conditions définies conjointement, puis détruit les fichiers manuels ou informatisés stockant les données à caractère personnel, sauf disposition impérative contraire résultant du droit communautaire ou du droit d’un Etat membre de l’Union Européenne applicables aux traitements objets du présent **Accord**.

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 la destruction par écrit au **Responsable de traitement** dans un délai de 10 jours ouvrés.

# 11. 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 **RGPD**, ou à défaut un interlocuteur privilégié apte à agir et à répondre à toutes les questions relatives au traitement des données et au respect des obligations prévues dans le présent **Accord** :

Coordonnées du DPO de [nom du prestataire] : [coordonnées]

Toute modification de l’identité de la personne ainsi désignée devra faire l’objet d’une information auprès du **Responsable de traitement** dans les meilleurs délais par tout moyen écrit permettant d’assurer la preuve de sa réception.

# 12. 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** conformément aux stipulations de **l’article 30 du RGPD** comprenant, entre autres :

* Le nom et les coordonnées du **Responsable de traitement** pour le compte duquel il agit, des éventuels **Sous-traitants ultérieurs** et, le cas échéant, des délégués à la protection des données,
* Les catégories de traitements effectués pour le compte du **Responsable de traitement,**
* Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale,
* Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :

# 13. Flux transfrontaliers de données

En cas de transfert de données à caractère personnel vers un pays tiers, n’appartenant pas à l’Union Européenne, ou vers une organisation internationale, le **Sous-traitant** devra obtenir l’accord préalable écrit du **Responsable du traitement**. Si cet accord est donné, le **Sous-traitant** s’engage à coopérer avec le **Responsable du traitement** afin d’assurer le respect des procédures permettant de se conformer à la réglementation sur la protection des données,

# 14. Documentation

Le **Sous-traitant** met à la disposition du **Responsable du traitement**, sur simple demande et par voie électronique et sur support sécurisé, toute la documentation nécessaire pour démontrer le respect de toutes ses obligations et plus largement son niveau de conformité, ainsi que toutes informations permettant 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.

# 15. Responsabilité et Assurance

## 15.1 Responsabilité du Sous-traitant

Outre toute autre action à la disposition du **Responsable du traitement**, chaque des parties assumera, à qui de droit, l’intégralité des frais de justice et débours (y compris les honoraires d’avocats et autres frais professionnels raisonnables), sanctions, amendes, indemnisations, compensation, dommages-intérêts, pénalités et toute autre perte ou préjudice indirect, de toute nature, résultant ou lié, de quelque manière que ce soit, à :

* Tout manquement du **Sous-traitant ou du Responsable de traitement** à ses obligations en vertu de la réglementation relative à la vie privée ;
* Toute violation par le **Sous-traitant ou le Responsable de traitement** du présent **Accord**.

## 15.2 Engagement de confidentialité en cas d’opération de maintenance ou de Télémaintenance dans le cadre d’une sous-traitance

Le **Sous-traitant** s’engage à :

* Garantir la confidentialité et la sécurité des données à caractère personnel traitées pour le compte du **Responsable de traitement**, et notamment empêcher qu'elles ne soient déformées, endommagées, consultées par ou communiquées à des personnes non autorisées.
* Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du 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.

## 15.3 Assurance

Le **Sous-traitant** déclare être assuré auprès d’une compagnie d’assurance de premier rang notoirement solvable pour toutes les conséquences dommageables des actes dont il pourrait être tenu responsable au titre du présent **Accord**. Il s’engage expressément à fournir au **Responsable du traitement**, sur simple demande de celle-ci, à tout moment, une attestation d’assurance de responsabilité civile professionnelle en cours de validité et couvrant les risques liés à l’exécution du présent **Accord**.

Fait en deux exemplaires originaux, le \_\_\_\_\_\_\_\_\_\_\_\_\_\_, à \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Cachet et signatures des **Parties** :

|  |  |
| --- | --- |
| Madame Julie DURAND, Directrice du GRADeS e-santé Occitanie | [Nom – Prénom et fonction du signataire] |
|  |  |

# 16. Annexe

Cette liste établie en Annexe est susceptible d’évoluer.Les types de données seront exhaustivement détaillées et mis à jour dans le Registre des traitements du **Responsable de traitement**. De la même manière, le **Sous-traitant** tient un registre des traitements contenant les catégories de traitements effectués pour le compte du **Responsable de traitement.**

## 16. Description des traitements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Données Traitées** | | Les types de données à caractère personnel traitées sont notamment :   1. Données patients (Cf. registre du RT) 2. Données à caractère personnel des acteurs des secteurs sanitaire, social et médico-social de région Occitanie ou régions limitrophes : nom, prénom, coordonnées d’activités (courriel, téléphone, adresse postale professionnel), profession, FINESS, RPPS, ADELI, (Cf. registre du RT) 3. Données administrateurs : horodatage de connexion (date, heure) | | |
| **Nature du traitement** | | La nature des traitements réalisés sur les données comprend notamment :  Gestion de la tierce maintenance applicative :   * Consultation, * Modification/adaptation, * Suppression (effacement ou destruction), * Enregistrement/conservation temporaire, * Transmission/diffusion au GRADeS e-santé Occitanie, * Rapprochement de données avec le PASS Occitanie et Pro Santé connect, * Limitation aux données de l’outil, * Extraction, * Organisation. | | |
| **Finalités** | | La ou les finalité(s) des traitements sont :   1. La maintenance corrective et évolutive des applications, 2. Le maintien en condition opérationnelle des applications 3. Demande de service ou ex 4. Nouveaux projets 5. Suivi des usages | | |
| **Personnes concernées** | | Les catégories de personnes concernées sont :   1. Les patients 2. Les utilisateurs des outils 3. Des professionnels de santé non-utilisateurs de l’outil 4. Les administrateurs | | |
| **Localisation** | | Le Traitement est réalisé dans les endroits suivants :   1. CEGEDIM - Hébergeur de données de santé certifié - 137 rue d’Aguesseau - RCS 790 173 066 - Téléphone : 01 40 09 22 00 | | |
| **Sous-traitants ultérieurs** | | **Nom (Indiquer la raison/dénomination sociale complète)** | **Nature du traitement effectué par le Sous-traitant ultérieur** | **Localisation géographique du traitement effectué par le Sous-traitant ultérieur** |
|  |  | NA |  |  |
|  |  |  |
| **Encadrement transferts** | **des** | **Territoire** | **Nature du traitement dans le pays tiers** | **Encadrement juridique** |
| NA |  |  |

