ANNEXE : SOUS-TRAITANCE DES DONNEES PERSONNELLES PAR CERTILIENCE

ARTICLE 1 OBJET

Les présentes clauses ont pour objet de déterminer les obligations spécifiques s'appliquant entre le Client tel qu'identifié au Contrat (ci-après « **le responsable de traitement** ») et CERTILIENCE (ci-après « **le sous-traitant** ») en matière de protection des données à caractère personnel.
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 RGPD** »).

ARTICLE 2 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 les prestations de services décrites au contrat auquel le présent document est annexé.
La nature des opérations réalisées sur les données consistera principalement à recevoir, stocker et conserver ces données pour le compte du responsable de traitement. Eventuellement, en fonction des prestations de services commandées par le responsable de traitement et en lien direct avec celles-ci, les opérations réalisées sur les données pourront consister pour le sous-traitant à consulter, extraire, dupliquer, sauvegarder, archiver les données. A l'issue de leur relation contractuelle, les opérations réalisées sur les données pour consister pour le sous-traitant à restituer, effacer ou détruire les données.
Le responsable de traitement communiquera spontanément au sous-traitant, au plus tard au début de la fourniture des services faisant l'objet du contrat, la ou les finalité(s) du traitement, les données à caractère personnel traitées ainsi que les catégories de personnes concernées. Le responsable de traitement pourra également mettre à la disposition du sous-traitant toutes informations supplémentaires qu'il jugerait nécessaires.
Le responsable de traitement communiquera par écrit au sous-traitant l'ensemble des informations listées au présent article par voie électronique à l'adresse email suivante : rgpd@certilience.fr.
Le responsable de traitement attirera l'attention du sous-traitant lorsque les données qu'ils traitent concerneront des catégories particulières de données au sens de l'article 9 du RGPD ou des données relatives aux condamnations pénales et aux infractions au sens de l'article 10 du RGPD.

Le responsable de traitement reconnaît être parfaitement informé que le sous-traitant n'est pas homologué comme étant un hébergeur de données de santé au sens de la réglementation du Code de la santé publique. Par conséquent, le responsable de traitement garantit que les données personnelles que le sous-traitant sera amené à traiter ne concernent pas des données de santé entendues comme toute données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne.

ARTICLE 3 DUREE DU CONTRAT

Les présentes clauses de sous-traitance des données personnelles entrent en vigueur au même moment que le contrat auquel elles sont annexées et pour la même durée stipulée entre les parties. Elles pourront d'un commun accord entre les parties être amendées par voie d'avenant.

ARTICLE 4 OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DE TRAITEMENT

Obligations générales
Le sous-traitant s'engage à :

1. **traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance ;**
2. **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 RGPD 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.

3. **garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat ;**
4. **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.
5. **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**

Sous-traitance
Le sous-traitant 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 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 d'un mois 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 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. 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.

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.

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 à l'adresse de courrier électronique indiquée par le responsable de traitement dans le contrat et/ou à l'adresse de courrier électronique indiquée dans son espace client.

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 à l'adresse de courrier électronique indiquée par le responsable de traitement dans le contrat et/ou à l'adresse de courrier électronique indiquée dans son espace client. 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.

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 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.
Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, 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.

Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations
Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données. Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle. Ces prestations d'assistance seront indemnisées par le responsable de traitement au coût horaire applicable en vigueur (taux horaire actuel de 125 € HT), compte-tenu de la nécessité de mobiliser des ressources techniques et humaines pour l'exécution de ces prestations.

Mesures de sécurité
Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

- Moyens permettant de garantir la confidentialité de l'infrastructure CERTILIENCE :
    - Restriction des accès ;
    - Contrôle d'accès sur les équipements ;
    - Chiffrement des partitions sensibles.
- Moyens permettant de garantir l'intégrité de l'infrastructure CERTILIENCE :
    - Audit régulier de l'infrastructure ;
    - Supervision de l'intégré de certaines données (configuration, Logs) ;
    - Export des traces sur un serveur tiers.
- Moyens permettant de garantir la disponibilité de l'infrastructure CERTILIENCE :
    - Redondance systématique des équipements vitaux ;
    - Supervision de la disponibilité ;
    - Test de redondance régulier.
- Moyens permettant de garantir la résilience de l'infrastructure CERTILIENCE :
    - Redondance des système critiques ;
    - Les systèmes sont dimensionnés pour absorber des perturbations.
- Moyens permettant de rétablir la disponibilité des données et l'accès à celles-ci en cas d'incident physique ou technique :
    - Sauvegarde localement des données ;
    - Sauvegarde des données sur un autre site physique à plus de 200Km.
- Procédures visant à tester, analyser et évaluer l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité :
    - Test de sécurité régulier et automatisé
    - Audit de sécurité régulier déroulé par un auditeur

Le responsable de traitement reconnait que les mesures techniques et organisationnelles listées ci-dessus répondent à ses attentes afin de garantir de façon adéquate la sécurité et la confidentialité des traitements qu'il souhaite mettre en œuvre.
Toutes mesures techniques et organisationnelles supplémentaires à celles listées ci-dessus que le responsable de traitement souhaiterait mettre en œuvre, notamment pour augmenter le niveau de sécurité de ses traitements ou adapter le niveau de sécurité à une évolution de ses traitements, devra être demandée par écrit et fera l'objet d'un devis et d'une facturation supplémentaire spécifiques.

Le responsable de traitement demeure néanmoins tenu de mettre en place au sein de son organisation une politique de sécurité qui lui soit propre afin notamment de :

- sensibiliser ses propres utilisateurs à la confidentialité et la protection des données personnelles;
- gérer les utilisateurs habilités à accéder à l'infrastructure CERTILIENCE ;
- maintenir la confidentialité des identifiants personnels permettant l'accès à l'infrastructure de CERTILIENCE et les renouveler de façon régulière ;
- sécuriser ses postes de travail et son informatique mobile ;
- choisir des applicatifs présentant un niveau de sécurité conforme / adapté à ses traitements ;
- sécuriser et mettre à jour ses applicatifs utilisés ou installés sur l'infrastructure CERTILIENCE afin d'éviter toute vulnérabilité ou malware notamment susceptible d'affecter l'infrastructure CERTILIENCE ;
- sauvegarder de façon régulière ses données en local ;
- privilégier les protocoles sécurisés (HTTPS, TLS, SSH, etc.) lors d'échange entre l'infrastructure CERTILIENCE et lui et/ou des tiers ;
- choisir de chiffrer et/ou pseudonymiser les données hébergées sur l'infrastructure CERTILIENCE ;
- décider en temps utile le remplacement / l'évolution de tout matériel / logiciel (pouvant notamment se traduire par un changement d'offre commerciale), notamment en cas d'obsolescence, de montée en charge et/ou d'évolution de la nature de ses traitements de données personnelles.

Sort des données
Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à :

- détruire toutes les données à caractère personnel ou
- à renvoyer toutes les données à caractère personnel au responsable de traitement ou
- à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement

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 RGPD.

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 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, y compris entre autres, selon les besoins :

paraphe Client :_____

- 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 met 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. Toute demande d'audit et/ou d'inspection devra être demandée par le responsable de traitement par lettre recommandée avec accusé de réception au moins 15 jours avant la date envisagée pour sa réalisation ainsi que sur l'identité des auditeurs envisagés. Le sous-traitant confirmera sous 7 jours au responsable de traitement la possibilité de cette date et faire d'éventuelles réserves objectives (non-concurrence) sur les auditeurs envisagés. Tout audit et/ou inspection ne pourra être réalisée qu'après qu'un accord de confidentialité ait été signé entre CERTILIENCE et l'ensemble des auditeurs.

ARTICLE 5 OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS-A-VIS DU SOUS-TRAITANT

Le responsable de traitement s'engage à :

- fournir au sous-traitant les données visées à l'article 2 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 RGPD de la part du sous-traitant ;
- superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.

Mise à jour du 20 juin 2018

paraphe Client :_____