Conditions spécifiques
Hébergement de Données de Santé (HDS)

ENTRE,

OUTSCALE, Société par Actions Simplifiée au capital de 1 849 930 €, immatriculée registre du commerce et des sociétés de Nanterre sous le n° 527 594 493, dont le siège social est sis 1, rue Royale – 319 Bureaux de la Colline – 92210 Saint Cloud, prise en la personne de son représentant légal en exercice domicilié en cette qualité audit siège, ayant tous pouvoirs à l'effet des présentes.

Ci-après dénommé OUTSCALE ;

ET,

Ci-après dénommé le CLIENT ;

Ensemble les Parties.

Préambule

OUTSCALE est un prestataire français de services informatiques en nuage s'appuyant sur des infrastructures situées sur le territoire français. OUTSCALE propose la mise à disposition du CLIENT de ressources (Machines Virtuelles, Service de Stockage Objet, etc.), au sein de l'Infrastructure OUTSCALE, ainsi que, le cas échéant, de services connexes.

Le CLIENT est une société spécialisée dans

Le CLIENT souhaitant commander à OUTSCALE un ou plusieurs service(s) de type IaaS dans leur version conforme au référentiel HDS, OUTSCALE et le CLIENT sont convenus des présentes Conditions Spécifiques pour encadrer la fourniture desdits services conformément au référentiel HDS tel que défini ci-après.

Ceci étant rappelé, les Parties ont convenu des présentes Conditions Spécifiques prises en application des conditions générales préalablement signées entre les Parties, lesquelles constituent le contrat entre OUTSCALE et le CLIENT pour le/les service(s) commandé(s).

ARTICLE 1. Périmètre de certification

Depuis le 3 décembre 2019 OUTSCALE est certifié Hébergeur de Données de Santé sur les activités suivantes :

- Mise à disposition et le maintien en conditions opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
- Mise à disposition et maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;
- Mise à disposition et maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
- Mise à disposition et maintien en conditions opérationnelles de l'infrastructure virtuelle du système d'information utilisé pour le traitement de données de santé.

Les activités listées ci-dessus correspondent aux finalités des traitements de données réalisés par OUTSCALE.

OUTSCALE garantit qu'elle possède la Certification des Hébergeurs de Données de Santé à caractère personnel (ci-après la Certification HDS) nécessaire à la réalisation du présent Contrat et qu'elle s'efforcera de le maintenir tout au long du Contrat. La perte de la Certification HDS entraînera la résiliation du contrat dans les conditions prévues à l'article Fin de la prestation, Restitution et Réversibilité.

Le périmètre HDS est audité annuellement et un certificat est émis chaque année attestant de la certification d'Outscale pour les activités entrant dans le périmètre de certification.

ARTICLE 2. Documents contractuels

Ces Conditions Spécifiques (ci-après les Conditions Spécifiques ou le Contrat) prévalent sur les conditions générales signées entre les parties sur lesquelles elles sont basées.

En cas de contradiction entre ces Conditions Spécifiques et les conditions générales, les Conditions Spécifiques prévaudront. Les éléments qui ne sont pas abordés dans ces Conditions Spécifiques seront pour leur part régies par les conditions générales.

ARTICLE 3. Description des Prestations

En plus des Prestations décrites aux conditions générales, OUTSCALE assure la Réversibilité de la production du CLIENT à la fin des Prestations conformément à l'article Fin de la prestation, Restitution et Réversibilité.

Outscale s'engage à garantir la disponibilité, l'intégrité, la confidentialité et l'auditabilité des données hébergées.

ARTICLE 4. Localisation des données

L'Infrastructure d'OUTSCALE supportant la Plateforme de Stockage des Données de Santé sera toujours installée dans des datacenters certifiés ISO/CEI 27001 : 2013 et situés en France Métropolitaine.

OUTSCALE ne transférera pas les Données du CLIENT en dehors des lieux d'hébergement susmentionnés sans accord préalable du CLIENT.

ARTICLE 5. Recours à des tiers

Dans le cadre des Prestations, le CLIENT est informé que OUTSCALE fait appel aux prestataires externes suivants :

Tiers	**Prestations**
EQUINIX	Datacenter (site de production)
INTERXION	Datacenter (site de sauvegarde)
TELEHOUSE	Datacenter (site d'interconnexion)
DASSAULT SYSTEMES	Datacenter (site de production)
SIPARTECH	Fibre noire
RATP Connect	Fibre noire
BSO	Fibre noire
INTERDATA	Fibre noire
ZAYO	Fibre noire
LUMEN	Fibre noire

Le CLIENT autorise OUTSCALE à faire intervenir ces prestataires dans le cadre de la fourniture du Service.

OUTSCALE s'assure que ces prestataires présentent un niveau de protection équivalent de garantie au regard des obligations pesant sur OUTSCALE.

OUTSCALE peut remplacer un ou plusieurs des prestataires ci-dessus ou recourir à un nouveau prestataire sous réserve de notifier préalablement le CLIENT en respectant un délai raisonnable.

OUTSCALE s'assure que les changements de prestataires ne conduisent pas à une réduction du niveau de sécurité sauf accord préalable du CLIENT.

Le CLIENT, une fois notifié, a la possibilité de résilier le présent contrat en cas de désaccord avec le changement de prestataire.

ARTICLE 6. Prestations à la fin de l'hébergement, Restitution et Réversibilité des données de santé

A la fin de l'hébergement, pour quelque raison que ce soit, et notamment dans le cas de perte ou de retrait de la Certification HDS, OUTSCALE s'engage à permettre la restitution de la totalité des données de santé du CLIENT et la réversibilité des prestations conformément au présent article.

La Réversibilité consiste à permettre au CLIENT de récupérer toutes les Données qui composent ses Systèmes en vue de les transférer chez un autre prestataire que OUTSCALE.

Pour ce faire, OUTSCALE met à la disposition du CLIENT ou des tiers compétents désignés par lui des API ouvertes, ainsi que la documentation associée, qui lui permettent d'assurer la récupération et le transfert de ses Données vers sa propre infrastructure ou celle d'un autre prestataire.

En cas de terminaison du Contrat, pour quelque raison que ce soit, y compris à la l'initiative d'OUTSCALE, OUTSCALE maintiendra uniquement les prestations de stockage de données et l'accès à la Plateforme pendant un (1) mois à compter de la date de la fin du Contrat lui permettant uniquement de récupérer l'ensemble de ses Données.

À l'issue de ce délai d'un (1) mois, le CLIENT transmettra à OUTSCALE un procès-verbal signé de « récupération des données terminée ». À compter de la réception de ce procès-verbal, OUTSCALE mettra fin à l'accès nécessaire à la récupération des Données et effacera toutes les Données du CLIENT et n'en conservera aucune trace.

Si à l'issue de ce délai d'un (1) mois, le CLIENT n'a pas adressé de procès-verbal signé de « récupération des données terminée » ou de demande de suppression du compte auprès du support OUTSCALE et après mise en demeure par lettre recommandée avec avis de réception au CLIENT, OUTSCALE, d'émettre le procès-verbal signé de « Récupération des données terminée », restée infructueuse pendant les quinze (15) jours ouvrés suivants sa réception, OUTSCALE pourra facturer l'immobilisation des espaces de stockages sur lesquels les Données sont encore présentes pendant 13 (treize) mois maximum. Au-delà de ce délai, OUTSCALE se réserve le droit de supprimer les Données dont il est question, ce que le CLIENT reconnaît et accepte.

Toutes les données du CLIENT sont effacées définitivement au plus tard dix (10) jours et deux (2) heures après la fin de la Réversibilité. Il s'agit du délai de conservation de la sauvegarde.

Par ailleurs, OUTSCALE peut proposer une Prestation d'assistance du CLIENT à la Réversibilité soumise à la passation d'un Bon de Commande.

ARTICLE 7. Suppression des données

Le CLIENT peut contacter le support CLIENT pour demander la suppression du compte CLIENT du CLIENT à tout moment.

A la fin des prestations, OUTSCALE s'engage à supprimer les données à caractère personnel et notamment de santé et sans en garder de copie.

Le CLIENT autorise OUTSCALE à procéder à la destruction des données du CLIENT conformément à la phase de Réversibilité.

OUTSCALE délivre une attestation de bon effacement des données à la demande du CLIENT.

ARTICLE 8. Conformité à la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)

Le CLIENT est informé par le présent contrat qu'il est tenu de respecter la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) élaborée par la Délégation à la stratégie des systèmes d'information de santé (DSSIS) du Ministère des affaires sociales et de la santé et l'agence du numérique en santé (ANS) et ses référentiels opposables tels que définis dans les textes légaux et réglementaires.

Le CLIENT s'engage par la signature du présent document à respecter la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) et ses référentiels opposables tels que définis dans les textes légaux et réglementaires, sans que OUTSCALE n'ait d'obligation de contrôle sur ce point.

ARTICLE 9. Contacts

Le CLIENT communique à OUTSCALE lors de la conclusion du Contrat les coordonnées du référent contractuel à contacter pour le traitement des incidents ayant un impact sur les données de santé. Ce référent doit être en mesure de désigner à OUTSCALE un professionnel de santé lorsque cela est nécessaire.

Les coordonnées du référent contractuel du CLIENT sont les suivantes :

NOM :

PRÉNOM :

FONCTION :

ADRESSE EMAIL :

NUMERO DE TELEPHONE :

Le CLIENT notifie sans délai OUTSCALE de la modification des coordonnées du référent contractuel.

Cette liste de contact pourra être transmise à l'autorité compétente qui en fait la demande, notamment dans le cas d'une suppression ou d'un retrait de la Certification HDS.

ARTICLE 10. Notification du CLIENT

Outscale s'engage à informer ou à consulter ses clients en cas de transmission de données personnelles le concernant dans le cadre d'une réquisition, saisie ou décision judiciaire, juridiquement contraignante, sauf à ce que la notification soit interdite par ladite saisie.

Les modalités d'information ou de notification du CLIENT quand la communication des données doit nécessairement être autorisée par la réquisition, saisie ou décision judiciaire concernée. Un résumé des opérations réalisées pourra être réalisé par échange de courriels ou par courrier par lettre recommandée avec accusé de réception.

La procédure de notification du CLIENT en cas de transmission de données personnelles dans ce contexte pourra être communiquée au CLIENT sur demande.

ARTICLE 11. Audits sur les systèmes du CLIENT

1. Communications de documents de conformité au CLIENT

OUTSCALE met en place des mesures techniques et organisationnelles afin de répondre aux objectifs de sécurité et de protection des données personnelles, telles que définies dans ses politiques de sécurité. Ces politiques pourront être transmises au CLIENT sur demande après la signature d'un accord de confidentialité.

OUTSCALE pourra communiquer les rapports d'audit, de certification, de qualification ou d'agrément au CLIENT qui en fait la demande.

Outscale met à la disposition du CLIENT la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits.

2. Audit des applications mises en production par le CLIENT

OUTSCALE pourra permettre au CLIENT d'auditer ses systèmes ou applications mis en production, sous réserve que le CLIENT informe OUTSCALE préalablement au lancement de ladite opération, et ce dans un délai raisonnable d'au moins trente (30) jours, afin notamment d'éviter que cet accroissement d'activité ne soit analysé comme une anomalie de sécurité et n'entraîne une éventuelle suspension temporaire des prestations. L'audit réalisé par le CLIENT ne doit pas impacter l'activité d'OUTSCALE. Les Parties fixeront conjointement la date de déroulement de l'audit. Les audits sont réalisés aux frais du CLIENT. Les ressources engagées par Outscale pour la réalisation de cet audit par le CLIENT seront facturées au CLIENT. L'audit

sera effectué à des conditions d'horaires et de lieu raisonnables et dans la limite d'un audit par an au maximum.

OUTSCALE a la capacité d'exclure certains éléments du périmètre de l'audit réalisé par le CLIENT, qu'il s'agisse d'éléments du périmètre organisationnel ou du périmètre technique, comme notamment les éléments mutualisés et les pentests. OUTSCALE pourra décider de limiter cet audit du CLIENT à un audit documentaire.

Outscale s'engage également à fournir des rapports d'audit externes indépendants pour les parties qu'il aurait exclues du périmètre (comme les zones mutualisées ou les pentests) à la demande du CLIENT.

Les résultats de l'audit seront exploités par les deux parties dans le but d'apporter des solutions aux éventuelles problématiques rencontrées.

ARTICLE 12. Utilisation des données de santé

OUTSCALE s'engage à ne pas traiter les données de santé hébergées à d'autres fins que l'exécution de l'activité d'hébergement de données de santé.

OUTSCALE ne pourra notamment pas utiliser les données à des fins marketing, publicitaires, commerciales ou statistiques.

ARTICLE 13. Modalités d'accès aux données de santé

Seul le CLIENT a accès aux données de santé hébergées sur son ou ses comptes CLIENT. OUTSCALE s'interdit d'accéder aux données de santé du CLIENT.

Mises à part les mesures de sécurité mises en œuvre par OUTSCALE pour sécuriser l'accès aux comptes prévues dans les conditions générales, le CLIENT est seul responsable de l'accès à ses données de santé.

L'accès aux Prestations est assuré par les clés d'accès au service, soit l'ensemble des identifiants (login, mot de passe, clé d'API, etc.) permettant au CLIENT de s'authentifier avant de pouvoir consommer et piloter des prestations. Les clés d'accès sont dédiées à un compte précis. Le CLIENT s'engage à ne pas les partager.

Le CLIENT met en œuvre les moyens de contrôle d'accès et de gestion des identités pour les utilisateurs sous sa responsabilité qui utilisent des interfaces de gestion des comptes et des droits d'accès hors de celles fournies par OUTSCALE.

ARTICLE 14. Collaboration pour l'exercice des droits des personnes concernées

Dans le cadre de son obligation de collaboration pour l'exercice des droits des personnes concernées par des traitements de données personnelles, OUTSCALE aidera le CLIENT à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, droit de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données personnelles, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage). Si les personnes

concernées exercent auprès d'OUTSCALE des demandes d'exercice de leurs droits, OUTSCALE adressera ces demandes dans les meilleurs délais par courrier électronique au CLIENT afin de lui permettre de répondre aux demandes dans le délai légal d'un mois.

OUTSCALE s'engage à mettre à disposition du CLIENT les procédures pour lui permettre de répondre aux demandes d'exercice des droits des personnes concernées, à la demande de ce dernier.

De plus, il est précisé que le CLIENT qu'en tant que responsable du traitement des données personnelles de santé éventuellement concernées par le présent Contrat, aura dans certains cas l'obligation de réaliser une analyse d'impact préalable sur la protection des données personnelles de santé qu'il traite, démarche dans laquelle OUTSCALE pourra éventuellement l'assister sur demande.

ARTICLE 15. Modifications et évolutions techniques

Le CLIENT reconnaît et accepte par les présentes que OUTSCALE pourra être amené à modifier les services ou à mettre en place de nouveaux services afin d'apporter les évolutions techniques nécessaires à la réalisation de ces services ou lorsque ces évolutions ou modifications sont imposées par le cadre légal applicable à OUTSCALE.

Il est précisé que les modifications et évolutions techniques mises en place n'auront pas d'impact sur le niveau de sécurité des Services conformément à l'article Mesures techniques et organisationnelles de sécurité et de protection des données.

L'introduction de nouveaux Services ou la modification ou la maintenance de services existants font l'objet d'une communication au CLIENT *a minima* une (1) semaine avant leur mise en service.

La planification de ces nouveaux services ou la modification des services existants est réalisée en adéquation avec les exigences de services

Dans le cas où des évolutions imposées par le cadre légal applicable à OUTSCALE entraîneraient un changement de circonstances imprévisibles lors de la conclusion du Contrat, la Partie qui n'a pas accepté d'assumer un risque d'exécution excessivement onéreux pourra demander une renégociation du Contrat à son cocontractant.

ARTICLE 16. Garanties et procédures en cas de défaillance

OUTSCALE met en place des garanties et des procédures permettant de couvrir toute défaillance éventuelle de sa part notamment par les SLA auxquels il s'engage, les assurances auxquelles il a souscrit et ses certifications notamment la certification ISO 27001 avec des procédures qui couvrent non limitativement les exigences de sécurité des systèmes d'information, la continuité d'activité, la gestion des vulnérabilités.

ARTICLE 17. Intégrité des échanges

Les données personnelles transitant par un réseau de communication feront l'objet d'un chiffrement avec des protocoles (notamment le protocole TLS sur les calls API) permettant notamment de s'assurer que ces données sont bien reçues par le système cible.

ARTICLE 18. Modalités du transfert des données

OUTSCALE garantit que les données CLIENT, hébergées sur la plateforme, ne seront pas transmises à des tiers par OUTSCALE.

ARTICLE 19. Mesures techniques et organisationnelles de sécurité et de protection des données

Les principales mesures de sécurité techniques et organisationnelles ainsi que les mesures complémentaires liées à la protection des données sont décrites dans les conditions générales.

L'évolution de ces mesures techniques et organisationnelles ne peut conduire à la diminution du niveau de sécurité sauf accord préalable du CLIENT.

La matrice des responsabilités d'OUTSCALE, synthétisant les responsabilités respectives des Parties et les mesures techniques et organisationnelles de sécurité mises en œuvre par OUTSCALE au travers des référentiels auxquels elle se conforme, est annexée au présent document.

ARTICLE 20. Traçabilité

Les actions réalisées par le CLIENT sur la plateforme font l'objet d'une journalisation. Le CLIENT a la possibilité de demander ces journaux à OUTSCALE par une demande au support par le biais de l'ouverture d'un ticket support. OUTSCALE fournira au CLIENT sur demande les logs d'accès à l'API. Il est de la responsabilité du CLIENT de satisfaire à l'obligation de tracer les actions des utilisateurs des applications de santé auxquelles OUTSCALE n'a pas accès.

Les administrateurs OUTSCALE n'ont pas d'accès aux systèmes d'information de santé hébergés sur l'infrastructure OUTSCALE.

Société OUTSCALE Nom Titre Signature	Le CLIENT Nom Titre Signature

ANNEXE 1 – CERTIFICAT HDS

ANNEXE 2 – CERTIFICAT ISO

ANNEXE 3 – MATRICE DES RESPONSABILITES