

CONDITIONS PARTICULIERES

« HEBERGEMENT HDS – OCI CLOUD »

Version en vigueur à compter du 22 avril 2025

Le présent document décrit les conditions particulières applicables aux Prestations spécifiques d'hébergement de données de santé sur la solution d'hébergement « OCI Cloud » (ci-après « **CP HDS OCI Cloud** »). Elles viennent préciser les conditions générales de service du Prestataire dans leur dernière version en vigueur disponible sur son site Internet à l'adresse suivante : <https://www.oci.fr/conditions-generales/> (les « **CGS** »).

Champ d'application

Le paragraphe « Champ d'application des CGS et opposabilité » de l'article 1 RELATION CONTRACTUELLE ENTRE LES PARTIES des CGS est complété comme suit :

Les Prestations se rapportent à l'intégration, l'exploitation, l'évolution et l'hébergement de solutions informatiques incluant de la Donnée de santé et/ou à la sauvegarde de Données de santé. Dans ce cadre, le Prestataire a développé une solution informatique d'hébergement de données en mode locatif externalisé, appelée « OCI Cloud », permettant de consacrer des ressources pour chaque Client afin de répondre aux besoins de ce dernier.

Définitions

Les termes portant une majuscule dans les CGS et réutilisés au sein des présentes CP HDS OCI Cloud ont la même signification que celle qui leur est donnée dans les CGS.

Les définitions suivantes sont ajoutées à l'article 2 DEFINITIONS des CGS :

« **Certification HDS** » : désigne la certification de l'Hébergeur « Hébergeur de Données de Santé » (HDS) (référentiel de certification HDS applicable à la date de signature de l'Offre commerciale : « Référentiel de certification HDS – Mai 2018 ») dont le périmètre est repris à l'**Annexe 1** ;

« **Données de santé** » : désigne l'ensemble des Données à caractère personnel relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soin de santé) qui révèlent des informations sur l'état de santé d'une personne physique et qui sont traitées par le Client.

« **Données de trafic** » : désigne l'ensemble des données d'accès collectées par l'une des Parties à partir de la Solution d'hébergement. Elles englobent notamment les adresses IP des équipements se connectant à la Solution d'hébergement, les horodatages des données réceptionnées, les logs d'accès ou encore les logs de statut des équipements connectés ;

« **Données temporaires** » : désigne les Données générées pendant l'exécution d'une tâche, inutiles une fois la tâche concernée terminée et automatiquement supprimées par le processus ;

« **Dossier technique** » : désigne les informations relatives au Client, relevées par le Prestataire et conservées par lui à des fins de réalisation et au suivi des Prestations (par exemple : interlocuteurs privilégiés etc.) ;

« **Fiches techniques** » : désigne les prestations d'hébergement au catalogue du Prestataire contenues dans le *Cloudbook* et décrivant lesdites prestations. Le Prestataire met régulièrement à jour le *Cloudbook* et le tient à disposition du Client sur demande ;

« **Incident** » : désigne une panne liée à la Solution d'hébergement ;

« **Solution d'hébergement** » : désigne la solution d'hébergement mise à disposition par Groupe OCI SAS, Affiliée du Prestataire (ci-après l'« **Hébergeur** ») et mise à la disposition du Client par le Prestataire dans le cadre de l'exécution du Contrat, notamment composée des ressources serveurs, du stockage et de la connectivité destinés au traitement des Données.

Hiérarchie des documents

Le premier paragraphe de l'article 3 HIERARCHIE DES DOCUMENTS est remplacé comme suit :

Le contrat est formé par les documents contractuels suivants, présentés par ordre hiérarchique de valeur juridique croissante :

- Le cahier des charges ou tout autre document précontractuel, décrivant les besoins du Client ;
- L'Offre commerciale et les Prestations additionnelles ;
- Les CGS et leurs éventuelles annexes ;
- Les présentes CP HDS OCI Cloud ;
- Les Fiches techniques dans leur dernière version en vigueur.

(ci-après le « **Contrat** »).

Obligations des Parties

Le paragraphe « Sécurité » de l'article 5.1 OBLIGATIONS DU PRESTATAIRE des CGS est remplacé comme suit :

Sécurité – Le Prestataire s'engage à mettre en œuvre les moyens techniques et organisationnels permettant d'empêcher toute altération, perte, destruction, accès ou utilisation frauduleuse des Données contenues dans la Solution d'hébergement. Il s'engage ainsi à respecter l'état de l'art en la matière, celui-ci se définissant comme l'ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des données publiquement accessibles à un instant donné, et des informations qui en découlent de manière évidente. Le Client reconnaît que les mesures de précaution et de sécurité, par exemple de sauvegarde, qu'il prend contribuent à la fiabilité et à la sécurité des Prestations et s'engage à les envisager dans la mesure où toutes les mesures de sécurité non spécifiquement confiées au Prestataire dans l'Offre commerciale relèvent de sa responsabilité. En cas de survenance d'un incident de sécurité avéré et imputable au Prestataire, le Prestataire s'engage à y remédier dans les meilleurs délais, dans la mesure des Prestations effectivement souscrites par le Client. Le Prestataire ne saurait en aucun cas être tenu pour responsable des incidents de sécurité et de cybersécurité résultant de la négligence ou du manquement du Client et/ou de tout autre tiers impliqué ou choisi par le Client, à ses obligations en matière de sécurité et de cybersécurité. A la date de signature de l'Offre commerciale, les mesures techniques et organisationnelles mises en place sont décrites à l'**Annexe 2**. Elles pourront régulièrement être mises à jour par le Prestataire qui s'engage, à ce titre, à ne pas les remplacer par des mesures ne garantissant pas un

niveau de sécurité au moins équivalent, sauf accord préalable du Client.

En sus des mesures décrites à l'**Annexe 2**, les Prestations peuvent nécessiter que le Client souscrive à des Prestations complémentaires visant à mettre des mesures de sécurité complémentaires en place (exemples : la couche 4 nécessite la souscription à une solution logicielle de bastion, la couche 5 une solution logicielle de gestion des logs), celles-ci feront l'objet d'une Offre commerciale.

L'article 5.1 OBLIGATIONS DU PRESTATAIRE des CGS est complété comme suit :

Hébergeur de Données de Santé – Pour proposer puis exécuter les Prestations, le Prestataire fait appel à l'Hébergeur. En tout état de cause, le Prestataire ne pourra pas refuser de communiquer les rapports d'audit de la Certification HDS de l'Hébergeur à son Client, dès lors que ce dernier fait la demande au Prestataire et le fournira dans un délai maximum de trente (30) jours après sa demande.

Conservation des Données de trafic – Conformément au droit applicable, le Prestataire conservera pendant une durée d'un (1) an à compter du jour de leur enregistrement, toutes les Données de trafic dont celui-ci a la charge.

L'article 5.2 OBLIGATIONS DU CLIENT des CGS est complété comme suit :

Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) – Le Client est tenu de respecter la PGSSI-S, en ce incluant le respect de tous les référentiels opposables. La signature de l'Offre commerciale par le Client matérialise son engagement et le recueil dudit engagement. Il reviendra au Client de contrôler que les mesures de sécurité mises en œuvre par le Prestataire lui permettent de répondre à la PGSSI-S.

Interlocuteur privilégié – Le Client désigne d'une part un interlocuteur privilégié dont le rôle est de gérer et s'assurer de la bonne exécution des Prestations et d'autre part un point de contact qui est en mesure de désigner au Prestataire un professionnel de santé lorsque cela est nécessaire (ex : accès aux données de santé, gestion des relations avec le patient, etc.). Le Client communique leurs coordonnées au Prestataire, au démarrage des Prestations, puis lors de tout changement.

Validation des Prestations – le Client s'engage à prendre connaissance de toute la documentation fournie par le Prestataire dans le cadre de la réalisation des Prestations (avant et pendant leur réalisation). Il s'engage également, s'agissant des Fiches techniques à en prendre connaissance à la date de signature de l'Offre commerciale et à en valider et en respecter le contenu.

Prérequis pour la mise en production d'applications – S'agissant des applications mises en production par le Client, il lui appartient de s'assurer de la conformité de celles-ci avec ses obligations légales. Pour des applications contenant de la Donnée de santé, il appartient spécifiquement au Client :

- De mettre en place et d'appliquer une méthodologie de vérification des applications qu'il héberge ;
- De s'assurer du respect des prérequis définis et communiqués par le Prestataire à sa demande pour la partie hébergement ;
- De garantir que l'application ne perturbera pas les performances globales du système hébergé et n'amoindrira pas le niveau de sécurité de la Solution d'hébergement, charge à lui d'informer le Prestataire afin que celui-ci puisse procéder aux vérifications et à la communication des informations nécessaires éventuelles aux fins d'éviter lesdites perturbations et / ou la diminution éventuelle du niveau de sécurité.

Conservation des Données de trafic – Conformément au droit applicable, le Client conservera pendant une durée d'un (1) an à compter du jour de leur enregistrement, toutes les Données de trafic dont celui-ci a la charge.

Par ailleurs, les Parties ajoutent un article 5.3 RETENTION DU CORPUS DOCUMENTAIRE PAR LES PARTIES :

Rétention du corpus documentaire entre les Parties – Les Parties conviennent qu'elles conserveront tous les éléments relatifs au corpus documentaire existant entre elles pour la durée nécessaire. A cet égard et à titre d'exemple, l'Hébergeur indique à ce jour conserver ses politiques de sécurité dans leur dernière version pour leur durée d'applicabilité augmentée d'une durée de trois (3) ans. Les documents contractuels quant à eux sont conservés pour la totalité de la relation commerciale entre le Client et le Prestataire augmentée d'une durée de dix (10) ans.

Description du périmètre des Prestations

Le paragraphe « Périmètre des Prestations » de l'article 6 ETENDUE DES PRESTATIONS des CGS est complété comme suit :

Les Prestations sont fournies dans le cadre d'une infrastructure qui peut être partagée ou dédiée, utilisant les ressources de la Solution d'hébergement.

Les Niveaux de service (auxquels il est fait référence dans les CGS) applicables aux Prestations sont définis en **Annexe 1** des présentes CP HDS OCI Cloud.

Modalités de réalisation des Prestations

Le paragraphe « Réception des Prestations » de l'article 7 MODALITES DE REALISATION DES PRESTATIONS des CGS est précisé comme suit :

Réception des Prestations – Les Prestations d'installation de l'hébergement et de sauvegarde couvertes par les présentes CP OCI Cloud font l'objet d'une recette (dont les modalités peuvent être précisées lors d'une réunion de cadrage si le Client a souscrit à une Prestation de gestion de projet). Le Prestataire met à disposition du Client un cahier de recette pour lequel le Client dispose d'un délai de quinze (15) jours pour formuler ses éventuelles réserves. En l'absence de telles réserves, la date de fourniture du cahier de recette correspond à la date de Mise en service. En cas de réserves confirmées par le Prestataire, le Prestataire procède à leur correction dans un délai maximal de trente (30) jours et en informe le Client. La date de mise à disposition de la correction constitue la Mise en service.

Les sections et paragraphes suivants sont ajoutées à l'article 7 MODALITES DE REALISATION DES PRESTATIONS des CGS :

Connexion à la Solution d'hébergement – La connexion à la Solution d'hébergement (et par conséquent la réalisation des Prestations) s'effectue via le réseau internet. Le Client est ainsi averti des aléas techniques qui peuvent affecter ce réseau et entraîner des ralentissements ou des indisponibilités rendant la connexion impossible. Le Prestataire ne peut être tenu responsable des difficultés d'accès aux Prestations dus à des perturbations du réseau internet indépendantes de sa volonté.

Sauvegarde

Le Client est responsable de la sauvegarde des Données qu'il héberge dans la Solution d'hébergement et des dangers liés à une éventuelle absence de sauvegarde (par

exemple en cas de perte ou de dommage affectant les Données).

Le Client peut souscrire à des prestations de sauvegarde proposées par le Prestataire (décrites notamment : au sein de l'Offre commerciale, dans la Fiche technique, dans les présentes CP OCI Cloud). Les modalités de la Prestation sont décrites dans le Contrat (et notamment : au sein de l'Offre commerciale). Le Prestataire s'engage à utiliser des méthodes de sauvegarde fiables.

Dans tous les cas, le Client doit s'assurer de la vérification de l'intégrité des Données et des Contenus sauvegardés ainsi que de la cohérence du contenu desdites sauvegardes, notamment en réalisant ou en faisant réaliser des tests de restauration à échéances régulières.

Sauvegarde de la Solution d'hébergement – Les Prestations de sauvegarde de la Solution d'hébergement porte sur la sauvegarde des Données nativement présentes dans la Solution d'hébergement.

Sauvegarde vers la Solution d'hébergement – Lorsque le Client souscrit à Prestations de sauvegarde de Données non-nativement présentes dans la Solution d'hébergement (par exemple : sauvegarde externalisée), le Prestataire peut accompagner le Client dans le choix d'un Produit de tiers voire dans la mise en place de cette sauvegarde. Le Client est informé que les Données répliquées depuis une solution-tierce vers la Solution d'hébergement ne sont pas considérées comme des Données nativement présentes dans la Solution d'hébergement.

Supervision de la sauvegarde – Dans le cas où le Client souscrit à de la supervision de sa sauvegarde, le Prestataire met en place une supervision qui permet de vérifier la bonne exécution du processus de sauvegarde (c'est-à-dire la réalisation des jobs de sauvegarde). Le Client reçoit les alertes ainsi paramétrées.

Perte des éléments sauvegardés – Lorsque le Client a souscrit à une Prestation de sauvegarde, le Prestataire s'engage alors à entreprendre des efforts raisonnables pour restaurer les Données et Contenus éventuellement perdus à partir des sauvegardes les plus récentes. La perte de Données et/ou de Contenus n'est pas considérée comme un dommage indirect au sens de l'article 12 RESPONSABILITE des CGS si celle-ci s'inscrit dans une défaillance du système de sauvegarde attribuable au Prestataire et que cette défaillance a causé un préjudice au Client. A ce titre, ne sont pas attribuables au Prestataire les pertes résultant d'un cas de force majeure affectant le Prestataire, des actes de piratage informatique, des indisponibilités du Fournisseur éditant le Produit logiciel de sauvegarde, des erreurs du Client et/ou de tout autre tiers intervenu sur l'Infrastructure de ce dernier.

Evolution de la Prestation de sauvegarde – Lorsque la sauvegarde est associée à une capacité de stockage, l'ajout de stockage par le Prestataire est une Prestation additionnelle.

Localisation de la Solution d'hébergement

Le Prestataire s'engage à héberger la Solution d'hébergement dans l'espace géographique suivant : France.

Audit

Le Client peut, au cours de l'exécution du Contrat, vérifier la conformité des Prestations fournies et notamment des mesures de sécurité mises en place par le Prestataire en procédant, sous réserve du respect des dispositions prévues au présent article, à des audits. Il peut faire ou faire faire, par tout auditeur mandaté par lui ne concurrençant

pas les activités commerciales du Prestataire ou de l'un de ses Affiliés et soumis à une obligation de confidentialité adéquate, procéder à toute vérification qui lui paraîtrait utile pour s'assurer du respect des obligations fixées par le Contrat par le biais d'un audit documentaire puis d'un audit physique. Le Prestataire s'engage à contribuer à ces audits.

En tout état de cause, le Client prend à sa charge tous les frais occasionnés par l'audit et rembourse au Prestataire toutes les dépenses et frais justifiés occasionnés par cet audit, y compris le temps consacré à l'audit en fonction du taux horaire moyen du personnel du Prestataire ou de ses Sous-traitants ayant collaborés à l'audit et dans la limite du taux horaires pratiqué entre les Parties.

Toutes les informations entrant dans le cadre de l'audit (en ce incluant les informations intégrées aux conclusions de l'audit, quelles que soient leur forme) seront soumises à une stricte obligation de confidentialité conformément aux dispositions prévues au Contrat.

Audit de sécurité documentaire – Sauf à justifier de limitations raisonnables, le Prestataire met à la disposition du Client la documentation nécessaire pour démontrer le respect de toutes ses obligations (ex : rapport de Certification HDS).

Audit physique – Dans le cas où l'audit documentaire révélerait l'éventualité d'un manquement du Prestataire au regard des engagements qu'il prend au titre du Contrat ou n'aurait pas permis de vérifier la conformité du Prestataire à ses engagements, le Client pourra procéder à un audit physique, sous réserve de tenir compte des conditions prévues dans les relations entre le Prestataire et ses éventuels sous-traitants (par exemple : interdiction de réaliser un audit physique). Le lieu de réalisation de l'audit devra être convenu entre les Parties.

Pour mettre en œuvre un tel audit, le Client s'engage à informer, par écrit, le Prestataire du démarrage de la vérification avec un délai de préavis minimum de trente (30) jours avant la date prévue d'audit, en lui indiquant :

- L'objet et le périmètre de l'audit (entre autres : les méthodes utilisées pour l'audit et les Données auditées) qui ne sauraient être plus larges que ce qui est couvert par le Contrat. Toutefois, si le Client souhaite auditer une application mise en production ou faisant l'objet d'une sauvegarde par le Client sur la Solution d'hébergement (et ce, quand bien même l'application n'est ni éditée, ni mise à disposition par le Prestataire), les Parties reconnaissent que l'administration et l'exploitation de ladite application n'entrent pas dans le Périmètre des Prestations réalisées par le Prestataire et ne peut donc faire l'objet d'un audit qu'à condition que les Prestations ou les mesures de sécurité associées soient en lien avec ladite application et que le Client en justifie dûment dans sa demande. Il fournira tout complément d'informations sur demande du Prestataire.
- La durée de l'audit ne pourra pas excéder deux (2) Jours Ouvrés ;
- L'identité de la ou des personnes qui effectueront l'audit.

Le Prestataire sera en droit d'exclure du périmètre de l'audit la vérification par le Client de certains éléments mutualisés sous sa responsabilité, à la condition que le Prestataire soit en mesure de fournir les résultats d'un audit externe indépendant sur ces éléments.

L'audit se déroulera pendant les Jours ouvrés et aux Heures Ouvrées du Prestataire et/ou de ses sous-traitants concernés et ne devra, en aucune façon porter atteinte au secret des affaires du Prestataire, ni lui causer une quelconque désorganisation au-delà de la mise à disposition par le Prestataire ou ses Sous-traitants des

ressources humaines, logiques ou matérielles permettant la réalisation de l'audit.

En tout état de cause, l'audit ne devra pas perturber l'activité des autres clients du Prestataire.

Conclusions de l'audit – Le Client mettra gratuitement à disposition du Prestataire le rapport d'audit produit, également soumis aux obligations de confidentialité prévues au Contrat. Ce document pourra être fourni par le Prestataire à tout Affilié du Prestataire et ou aux Sous-traitants concernés.

Dans l'hypothèse où des écarts à la réglementation applicable et à la Certification HDS seraient constatés durant l'audit, les Parties s'engagent à échanger et collaborer de bonne foi pour la mise en œuvre des mesures nécessaires.

Fin du Contrat

L'article 10 FIN DU CONTRAT des CGS est complété comme suit :

Absence de Certification HDS – Si au cours du Contrat, l'Hébergeur venait à perdre la Certification HDS pour quelle que raison que ce soit, le Prestataire en informera le Client dans les meilleurs délais et ce dernier aura la faculté de résilier les Prestations par l'envoi d'une notification. Le Client pourra alors demander la réversibilité des Prestations.

Responsabilité

L'article 12 RESPONSABILITE des CGS est complété comme suit :

Exclusions de responsabilité – La responsabilité du Prestataire ne pourra par ailleurs pas être engagée par le Client en cas :

- D'inaccessibilité de la Solution d'hébergement, si l'origine de cette inaccessibilité résulte des équipements relevant de la maîtrise du Client, la charge de la preuve de cette origine incombant au Prestataire ;
- D'intrusions ou utilisations non-autorisées ou illicites des identifiants et mots de passe du Client, sauf s'il est

Annexe 1 – Niveaux de service

Hébergement de Données de santé – Pour les Prestations pour lesquelles le Client a défini la nécessité de prévoir un hébergement spécifique du fait de la présence de Données de santé, le Prestataire atteste que l'Hébergeur est détenteur de la Certification HDS en sa qualité d'« hébergeur-infogéreur ». Le Client pourra demander au Prestataire de lui fournir l'attestation y relative, étant entendu qu'en cas de perte / de retrait / de non-renouvellement / de modification (à la baisse) du périmètre de la Certification HDS, le Client a la faculté de résilier les Prestations conformément à l'article 10 FIN DU CONTRAT des CGS.

Au jour de la signature de l'Offre commerciale, l'Hébergeur bénéficie d'une Certification HDS qu'il a obtenue en date du 20 décembre 2023 et qui a une durée de validité allant jusqu'au 19 décembre 2026.

La Certification HDS porte sur le périmètre suivant :

Descriptif des prestations certifiées	Certification HDS
Couche 1 – MISE A DISPOSITION ET MAINTIEN EN CONDITION OPERATIONNELLE DES SITES PHYSIQUES PERMETTANT D'HEBERGER L'INFRASTRUCTURE MATERIELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMENT DES DONNEES DE SANTE	Oui, si le Client a souscrit à des prestations de housing.
Couche 2 – MISE A DISPOSITION ET MAINTIEN EN CONDITION OPERATIONNELLE DE L'INFRASTRUCTURE MATERIELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMENT DE DONNEES DE SANTE	Oui, dans la mesure où le Prestataire fait appel à un Sous-traitant qui répond aux exigences du Référentiel HDS. Voir également la mesure « Sécurité physique et contrôle d'accès des datacenters » en Annexe 2.
Couche 3 – MISE A DISPOSITION ET MAINTIEN EN CONDITION OPERATIONNELLE DE LA PLATEFORME D'HEBERGEMENT D'APPLICATIONS DU SYSTEME D'INFORMATION	Oui

démontré par le Client qu'elles résultent d'une défaillance du Prestataire dans la sécurisation de la Solution d'hébergement ;

- De préjudice subi par le Client ou des tiers du fait du contenu hébergé sur la Solution d'hébergement, dont le Client a seul la maîtrise ;
- De préjudice subi par le Client ou des tiers et lié à des produits tiers à la Solution d'hébergement, si l'origine du préjudice ne peut être imputée au Prestataire.

Propriété intellectuelle

L'article 15 PROPRIETE INTELLECTUELLE des CGS est complété par la section suivante :

Droits de propriété intellectuelle sur la Solution d'hébergement

Dans le cadre de l'exécution du Contrat, le Prestataire accorde au Client, en contrepartie du paiement du prix, une licence non-exclusive, non-cessible et non-transférable d'utilisation de la Solution d'hébergement, pendant toute la durée du Contrat et pour le monde entier, sous réserve de conditions particulières ou limitées en fonction de la zone géographique.

Les Parties conviennent que nonobstant le droit accordé par le Prestataire au Client, le Prestataire ou les ayants-droits restent seuls titulaires de l'ensemble des droits, notamment de propriété intellectuelle, portant sur la Solution d'hébergement.

Le Prestataire garantit le Client contre toute action qui résulterait de l'utilisation par ce dernier de la Solution d'hébergement qu'il met explicitement à sa disposition dans le cadre du Contrat, sous réserve du respect par le Client des limites des droits concédés par le Prestataire et/ou ses Fournisseurs.

Protection des données à caractère personnel

Par dérogation à l'article 16 PROTECTION DES DONNEES A CARACTERE PERSONNEL des CGS, l'accord de sous-traitance RGPD applicable entre les Parties est repris en **Annexe 3** des présentes Conditions particulières.

Couche 4 – MISE A DISPOSITION ET MAINTIEN EN CONDITION OPERATIONNELLE DE L'INFRASTRUCTURE VIRTUELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMENT DES DONNEES DE SANTE	Oui
Couche 5 – ADMINISTRATION ET EXPLOITATION DU SYSTEME D'INFORMATION CONTENANT LES DONNEES DE SANTE	Oui Toutefois, il est rappelé à ce titre qu'il revient au Client de s'assurer qu'il bénéficie d'un contrat de prestation d'administration et d'exploitation avec le(s) tiers (ex : un éditeur, un prestataire-tiers etc.) intervenant sur son système d'information contenant de la Donnée de santé et que ledit tiers réponde aux exigences HDS, ce périmètre étant formellement exclu des présentes CGS et de la responsabilité du Prestataire. De ce fait, il incombe au Client la responsabilité de gérer toutes les autorisations et habilitations d'accès à son système d'information par les Utilisateurs dont il a la responsabilité.
Couche 6 – SAUVEGARDES EXTERNALISEES DES DONNEES DE SANTE	Oui

Disponibilité générale de la Solution d'hébergement – Le Prestataire garantit un taux de disponibilité de 99,9 % de la Solution d'hébergement, ce taux correspondant au temps où la Solution d'hébergement ne fait pas l'objet d'une interruption de service sur une année calendaire. Ne sont pas considérés comme des interruptions de services les incidents techniques majeurs dont la cause est extérieure à l'action du Prestataire et/ou les opérations techniques préplanifiées (à titre indicatif, celles-ci sont principalement opérées la nuit à partir de 22 heures) ainsi que les événements de force majeure. Le taux est calculé à partir de la Solution d'hébergement et non pas à partir des équipements du Client.

Maintenance et disponibilité – L'accès à la Solution d'hébergement et plus largement aux Prestations ou leur utilisation peuvent être momentanément interrompus pour des raisons de nécessité liées aux services proposés par le Prestataire et notamment afin d'assurer la maintenance des serveurs du Prestataire. Dans cette hypothèse, le Client sera informé par e-mail à l'adresse indiquée dans son Dossier technique au minimum dans un délai de soixante-douze (72) heures en cas de maintenance planifiée et en cas de maintenance critique par le biais d'une information sur le Portail client, disponible au plus tard dans les 48 heures suivant l'opération de maintenance critique.

Disponibilité des Produits logiciels et/ou des solutions logicielles tierces – En cas d'interaction entre la Solution d'hébergement et un Produit logiciel ou une solution logicielle tierce, par exemple dans le cadre de l'hébergement d'un tel Produit logiciel ou d'une solution logicielle tierce dans la Solution d'hébergement, les niveaux de service et le taux de disponibilités sont librement fixés par l'éditeur de ladite solution tierce. Dans ce cas, le Client se réfère aux conditions d'utilisation et niveaux de service des éditeurs concernés. Sauf précision contraire, le Prestataire intervient uniquement pour la mise à disposition des licences de la solution tierce retenue par le Client.

Il est rappelé à ce titre que du fait du périmètre de la Certification HDS obtenue par le Prestataire, le Prestataire n'intervient pas sur le système d'information contenant de la Donnée de santé du Client.

Annexe 2 – Mesures techniques et organisationnelles de la Certification HDS

En sus des mesures techniques et organisationnelles de sécurité définies par le Client, des mesures techniques et organisationnelles de sécurité ont été définies par le Prestataire, par le biais de l'Hébergeur et sont considérées comme acceptées par le Client à la signature de l'Offre commerciale. Ces mesures concernent uniquement le Périmètre des Prestations, à condition que les Prestations s'inscrivent dans le périmètre de la Certification HDS décrit à l'**Annexe 1**.

ORGANISATIONNELLES	
Gouvernance de la protection des Données à caractère personnel / désignation d'un DPO	Le Prestataire applique une gouvernance de protection des Données à caractère personnel à l'ensemble de ses activités. Cette gouvernance inclut la désignation d'un délégué à la protection des données.
Gouvernance de la sécurité des systèmes d'information	L'Hébergeur applique une gouvernance de la sécurité des systèmes d'information, qui repose sur un Système de Management de la Sécurité de l'Information (SMSI) certifié ISO27001 pour ses activités d'hébergement. L'activité d'hébergement est interfacée avec la BU cybersécurité, dont l'expertise est certifiée en cybersécurité par le biais du label ExpertCyber.
Gestion des risques	L'Hébergeur a instauré une approche visant à maîtriser les risques de sécurité en vue de détecter les risques qui pèsent sur les Données à caractère personnel, d'évaluer leur probabilité d'occurrence et de concevoir et approuver des plans d'action pour les maîtriser.
Confidentialité	Le Prestataire garantit la confidentialité des Données et plus particulièrement des Données à caractère personnel. Certains traitements peuvent justifier que les collaborateurs du Prestataire signent des accords de confidentialité spécifiques (par exemple : les personnes en charge de l'administration, de l'exploitation ou de la maintenance des systèmes d'information).
Protection des Données dès la conception	Le Prestataire intègre la protection des Données à caractère personnel dans la réalisation de ses Prestations, y compris les exigences de sécurité. La méthode « <i>privacy by design</i> » est appliquée dès la phase de conception, pour permettre la conformité avec le droit des personnes concernées, ainsi que pour prévenir les erreurs, pertes, modifications non autorisées ou mauvais usage de ces Données. Lorsque le Prestataire réalise, sur souscription du Client et en cas possibilité de réaliser des Prestations dans le cadre de la couche 5 de la Certification HDS, des développements et tests, ceux-ci le sont dans des

	environnements informatiques séparés de ceux en production, et en utilisant des Données fictives ou anonymisées fournies à cet effet.
Politique du zéro papier	L'Hébergeur met en place une politique zéro papier.
Supports amovibles	Les employés du Prestataire et de l'Hébergeur ne sont pas autorisés à utiliser des supports amovibles pour stocker des Données à caractère personnel sensibles à l'exception de supports bien identifiés et avec une méthode de chiffrement.
Vérification et des surveillances des activités de l'hébergement	Les activités des administrateurs sont régulièrement contrôlées par l'Hébergeur à travers l'analyse des traces techniques et organisationnelles.
Gestion des Incidents	L'Hébergeur établit des procédures claires pour le signalement rapide des événements liés à la sécurité des systèmes d'information et des Données à caractère personnel. Des outils spécifiques sont mis en place pour identifier les Incidents et les évaluer en termes de gravité et d'impact. Si nécessaire, des mesures correctives sont prises pour limiter les conséquences des Incidents. L'Hébergeur analyse également les Incidents afin d'identifier les causes profondes et apporter des solutions préventives pour éviter une nouvelle survenance.
Veille relative aux vulnérabilités techniques et de cybercriminalité	Le Prestataire effectue une surveillance constante des vulnérabilités techniques des systèmes d'exploitation et des logiciels utilisés par ses équipes. De plus, une veille relative à la cybercriminalité est également mise en place. Cette surveillance est suivie d'une évaluation des risques afin d'identifier les mesures complémentaires nécessaires pour remédier aux vulnérabilités détectées.
BU Cybersécurité	La BU cybersécurité est en charge de superviser les mesures de sécurité nécessaires pour protéger les systèmes informatiques et les données sensibles de l'entreprise contre les attaques, les intrusions et les violations de la confidentialité. La BU cybersécurité est constituée d'une équipe de professionnels expérimentés en sécurité informatique, tels que des analystes en sécurité, des ingénieurs en sécurité, des architectes de sécurité, des administrateurs de systèmes de sécurité, des auditeurs de sécurité et des experts en gestion de la sécurité. Ces professionnels sont chargés de concevoir, de mettre en œuvre et de gérer les différents programmes de sécurité de l'entreprise. La BU surveille en permanence les systèmes d'information du Prestataire pour détecter les menaces de sécurité et les vulnérabilités potentielles, et de réagir rapidement pour minimiser les risques.
Sensibilisation et formation	Le Prestataire sensibilise et forme ses collaborateurs sur les différents aspects de la protection des Données à caractère personnel en fonction de leurs missions et tâches. Certaines de ces sessions sont obligatoires pour s'assurer que tous les collaborateurs – même ceux qui ne traitent pas de Données à caractère personnel, sont informés des exigences réglementaires en vigueur et des bonnes pratiques à respecter.
Contrôles de conformité	Le Prestataire vérifie périodiquement l'efficacité de ses dispositifs de protection des Données à caractère personnel pour assurer la sécurité de ses traitements. En outre, elle mandate des organismes certifiés ou d'autres tiers reconnus pour leur compétence pour effectuer des contrôles et vérifications.
Gestion des Fournisseurs	Le Prestataire gère la sous-traitance ultérieure en s'assurant que ses sous-traitants ultérieurs respectent les exigences de sécurité et de protection des Données à caractère personnel. Un processus de sélection rigoureux est mis en place pour choisir des Sous-traitants conformes à la réglementation en vigueur et disposant des certifications et compétences nécessaires. Des contrats de sous-traitance sont établis pour préciser les obligations du Sous-traitant en matière de sécurité et de confidentialité. Des contrôles réguliers sont effectués pour s'assurer que les Sous-traitants respectent les exigences contractuelles et réglementaires.
Certifications	ISO 27001 Certification HDS
TECHNIQUES	
Sécurité physique et contrôle d'accès des datacenters	Les datacenters sont certifiés ISO 27001 et tier 3. La sécurité physique des sites sur lesquels les Données à caractère personnel sont traitées est garantie. Pour accéder aux sites, un système de contrôle d'accès par badge et/ou digicode est mis en place. Pour empêcher toute intrusion physique, des systèmes de détection d'intrusion avec alarme, de vidéosurveillance et des restrictions d'accès à certains locaux sont également en place. De plus, des mesures de prévention des incendies sont également mises en place avec une centrale de détection associée à des détecteurs de fumée et des extincteurs manuels. Les datacenters disposent de mesures de sécurité complémentaires telles que des solutions de détection et d'extinction automatique en cas d'incendie, des dispositifs de secours électrique et une protection contre les risques d'inondation ou de construction dans une zone inondable.
Surveillance des accès informatiques et gestion des privilèges	Le Prestataire met en place un système de contrôle d'accès logique fondé sur le principe de séparation des tâches et de privilège minimum. Tous les Utilisateurs qui accèdent à un système d'information sont authentifiés au moyen d'un compte nominatif. Le Prestataire suit une politique de mots de passe exigeant des critères de complexité et un renouvellement régulier, ainsi qu'une politique d'habilitation basée sur le principe du privilège minimum et de la séparation des rôles.
Compte nominatif	L'accès aux systèmes par le Prestataire se fait à l'aide d'identifiants uniques et nominatifs. Pour les Sous-traitants autres et, de manière générale pour les Utilisateurs du Client, l'accès aux systèmes se fait selon les principes définis par le Client. A titre indicatif, sur demande du Client, le Prestataire peut proposer une politique d'accès basée, en principe, sur une solution de bastion.
Surveillance et traçabilité de l'activité des administrateurs	Les accès et les actions effectués par les administrateurs système et les opérateurs techniques sur les systèmes administrés sont enregistrés de manière nominative. Les traces de ces accès peuvent être fournies sur demande.
Surveillance et traçabilité technique et de sécurité	L'Hébergeur garantit la traçabilité des actions de ses intervenants, des défaillances et des événements liés à la sécurité de l'information pour les composants et les systèmes qui soutiennent les activités d'infrastructure virtuelle, de plateforme logicielle, d'administration/exploitation et de sauvegarde externalisée.
Fuite de Données	Des mesures de prévention de la fuite de Données sont appliquées aux systèmes, aux réseaux et à tous les autres terminaux qui traitent, stockent ou transmettent des informations sensibles.
Filtrage web	Si le Client utilise le firewall mutualisé, il bénéficie d'un filtrage UTM.
Restriction de programmes utilitaires	L'usage des programmes utilitaires à privilèges est restreint.

à privilèges	
Activité de surveillance	L'Hébergeur surveille ses réseaux, systèmes et applications pour détecter les comportements anormaux et prend les mesures appropriées pour évaluer les éventuels Incidents de sécurité de l'information.
Segmentation des Données	L'Hébergeur met en œuvre diverses solutions pour garantir la segmentation des Données, afin d'empêcher l'accès à ces dernières par d'autres clients ou par les collaborateurs qui n'ont pas besoin d'y accéder dans le cadre de leurs fonctions. Ces solutions de cloisonnement comprennent des cloisonnements physiques tels que l'utilisation de serveurs physiques dédiés, des cloisonnements de réseau tels que le firewalling et les VLAN, ainsi que des solutions de cloisonnement logiciel pour les bases de Données et les fichiers.
Journalisation des activités	Les activités des utilisateurs et administrateurs des systèmes d'information, ainsi que les événements de sécurité associés, sont enregistrés. Ces enregistrements contiennent au minimum des informations telles que l'identifiant, la date et l'heure de la connexion et de la déconnexion. En fonction de la sensibilité des Données à caractère personnel, les actions effectuées sur ces Données à caractère personnel peuvent également être enregistrées.
Suppression des Données	Avant toute réutilisation du Matériel, les Données sont détruites de manière permanente et irréversible, conformément aux stipulations contractuelles. Ces exigences sont également reportées sur les Sous-traitants du Prestataire.
Sécurisation des échanges et flux de données	Pour assurer la sécurité des transferts de fichiers, tels que ceux utilisant les protocoles SFTP et HTTPS, des protocoles sont mis en place pour garantir la confidentialité et l'authentification des serveurs. Les supports utilisés pour les échanges de données sont également équipés de moyens de chiffrement des fichiers et des données, tels que des clés de chiffrement ou des mots de passe, pour protéger leur confidentialité Le cloisonnement réseau et le filtrage des flux sont également mis en place, avec une politique d'interdiction par défaut, pour renforcer la sécurité.
Sécurité des postes administrateurs	Les postes de travail des intervenants sont équipés de divers mécanismes de sécurité, tels que des mécanismes de verrouillage de session, des pare-feux, et un antivirus. L'accès aux postes de travail des collaborateurs est protégé par un chiffrement de partition (Bitlocker). Une restriction des USB est également en place.
Sécurité des serveurs	Seules les personnes autorisées ont accès aux outils et interfaces d'administration des serveurs. Les administrateurs disposent d'un compte personnel nominatif et de mots de passe spécifiques pour accéder à ces outils. Par ailleurs, les systèmes d'exploitation des serveurs sont régulièrement mis à jour afin de garantir leur sécurité.
Utilisation de protocole sécurisés pour les sites web	Le Prestataire utilise les protocoles TLS pour protéger les Données à caractère personnel affichées ou transmises sur les pages web, telles que les pages d'authentification et de formulaire. L'accès aux comptes administrateurs est limité aux équipes chargées des actions d'administration sur les sites web et les logiciels sécurisés pour les sites et logiciel.
Protection contre les programmes malveillants (malware)	Le Prestataire utilise une protection antivirale contre les programmes malveillants et elle est renforcée par une sensibilisation appropriée des Utilisateurs. L'EDR surveille en permanence le comportement des applications.
Chiffrement	Le Prestataire utilise la cryptographie, en sélectionnant des algorithmes de chiffrement appropriés, la gestion des clés de chiffrement et l'utilisation de certificats numériques pour assurer la confidentialité, l'intégrité et l'authenticité des informations, ainsi que pour garantir la disponibilité des informations en cas d'incident de sécurité. Sur les réseaux publics, les flux sont chiffrés. Les Données à caractère personnel sont transférées sur des réseaux publics en utilisant des protocoles et des algorithmes de chiffrement. Les Données fournies par le Client doivent être chiffrées avant réception par le Prestataire. Ce dernier ne peut s'engager sur ce chiffrement.
Sauvegarde	Le Client est responsable de mettre en place ou non des sauvegardes de ses Données. Lorsque l'option est souscrite auprès du Prestataire, des sauvegardes complètes et incrémentielles des Données sont effectuées régulièrement et stockées dans un emplacement distinct de celui où les Données à caractère personnel sont conservées. Une réplication des Données d'un datacenter à l'autre est possible.
Révision et gestion des changements	Le Prestataire ou l'Hébergeur peut modifier, à tout moment et sans préavis, tout ou partie des mesures de sécurité techniques et organisationnelles. Cependant, ces modifications ne visent pas à diminuer le niveau de protection des Données à caractère personnel.

Annexe 3 – Accord de sous-traitance RGPD

Article 1 : Définitions

Les termes portant une majuscule et réutilisés au sein du présent Accord qui n'auront pas été définis au Contrat auront la même signification que celle qui leur est donnée dans la Réglementation applicable. En sus, le Client s'engage en sus à respecter le Code de la santé publique et tout document de la Certification (par exemple : la PGSSI-S) et le Prestataire, tant que la Certification HDS est maintenue, le référentiel y relatif.

Le Sous-traitant est autorisé à agir selon les instructions du Responsable de traitement et à traiter les Données à caractère personnel du Responsable de traitement dans la mesure nécessaire à la fourniture des Prestations qui sont définies à l'Offre commerciale conclue entre les Parties.

Les modalités de traitement sont décrites en **Annexe A** du présent Accord.

Article 3 : Durée de l'Accord

Article 2 : Description du traitement faisant l'objet de la sous-traitance

Le présent Accord entre en vigueur pour la durée de l'Offre commerciale et expire à l'arrivée au terme pour laquelle raison que ce soit de ladite Offre commerciale.

Article 4 : Obligations du Responsable de traitement vis-à-vis du Sous-traitant

Le Responsable de traitement s'engage à :

- Respecter la Réglementation applicable ;
- Fournir au Sous-traitant les Données à caractère personnel concernées ;
- Documenter par écrit toute instruction concernant le traitement des Données à caractère personnel par le Sous-traitant ;
- Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par la Réglementation applicable de la part du Sous-traitant ;
- Superviser le traitement, en compris le fait de réaliser des audits et/ou des inspections du Sous-traitant.

Article 5 : Obligations du Sous-traitant vis-à-vis du Responsable de traitement

Le Sous-traitant s'engage à :

- Ne traiter les Données à caractère personnel que **pour les seules finalités** qui font l'objet de la sous-traitance ;
- Traiter les Données à caractère personnel **conformément aux instructions documentées** du Responsable de traitement. Si le Sous-traitant considère qu'une instruction constitue une violation de la Réglementation applicable, il en informe immédiatement le Responsable de traitement. En outre, si le Sous-traitant est tenu de procéder à un transfert de Données à caractère personnel 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 ledit transfert, sauf si le droit concerné interdit une telle information ;
- **Garantir la confidentialité** des Données à caractère personnel traitées dans le cadre du présent Accord ;
- Veiller à ce que les personnes autorisées à traiter les Données à caractère personnel en vertu du présent Accord s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité et (ii) 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** ;
- Respecter la Réglementation applicable.

Article 6 : Sous-traitance

Le Sous-traitant peut faire appel à un autre sous-traitant ultérieur (ci-après, le « **Sous-traitant Ultérieur** ») pour mener des activités de traitement spécifiques. Le Sous-traitant informera préalablement et par écrit le Responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'un Sous-traitant Ultérieur. Cette information devra indiquer clairement les activités de traitement sous-traitées ainsi que l'identité et les coordonnées du Sous-traitant Ultérieur. Le Responsable de traitement disposera d'un délai de quinze (15) jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne pourra être effectuée que si le Responsable de traitement n'a pas émis d'objection pendant le délai convenu. En cas d'objection raisonnable et justifiée, le Prestataire peut proposer au Responsable de traitement un Sous-traitant Ultérieur alternatif.

A la date d'entrée en vigueur du présent Accord, le Sous-traitant peut faire appel :

- Aux Sous-traitants Ultérieurs acceptés par le Responsable de traitement ;
- A ses Affiliés (et notamment l'Hébergeur) pour tout ou partie des Prestations ;
- A tous Sous-traitants Ultérieurs mentionnés sur une offre commerciale du Sous-traitant (ex : éditeur).

Le Sous-traitant Ultérieur est tenu de respecter les obligations du présent Accord. Il appartient au Sous-traitant de s'assurer que le Sous-traitant Ultérieur 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 applicable. Si le Sous-traitant Ultérieur ne remplit pas ses obligations en matière de protection des Données à caractère personnel, le Sous-traitant demeure pleinement responsable devant le Responsable de traitement de l'exécution par le Sous-traitant Ultérieur de ses obligations.

Article 7 : Droit d'information des personnes concernées

Le Responsable de traitement, au moment de la collecte des Données à caractère personnel, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de Données à caractère personnel qu'il réalise. Les Parties peuvent convenir dans certains cas que le Sous-traitant fournira cette information. Dans ce cas, les Parties conviendront de la formulation et du format de l'information avant la collecte de Données à caractère personnel. En sus de cette obligation générale, le Responsable de traitement doit avoir préalablement informé les personnes concernées que leurs Données de santé à caractère personnel seront hébergées sur support numérique.

Article 8 : 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.

Le Responsable de traitement doit répondre, en son nom et pour son compte, et dans les délais prévus par la Réglementation applicable aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des Données à caractère personnel faisant l'objet de la sous-traitance prévue par le présent Accord.

Lors de l'exercice des droits des personnes auprès de lui, le Sous-traitant informe dans les meilleurs délais le Responsable de traitement de la demande exercée.

Dans le cas spécifique où une personne concernée exerce d'un droit d'accès pour obtenir la communication de ses informations médicales (c'est-à-dire des Données de santé dont la durée de vie n'excède pas cinq (5) ans, le Sous-traitant devant avoir l'information), le Sous-traitant informe le Responsable de traitement dans les meilleurs délais et au plus tard dans les quarante-huit (48) heures sur les jours ouvrés. Lorsque seul le Sous-traitant a la possibilité technique de fournir les Données à caractère personnel, le Responsable de traitement formule la demande au Sous-traitant dans les délais et l'informe des délais (délais initiaux, éventuelle prolongation etc.) qui lui sont imposés au titre du cadre légal applicable.

Article 9 : Notification des violations de Données à caractère personnel

Le Sous-traitant notifie au Responsable de traitement toute violation de Données à caractère personnel dans les meilleurs délais et au plus tard quarante-huit (48) heures sur

les jours ouvrés après avoir pris connaissance de la violation et par l'un des moyens suivants :

- Par téléphone, auprès des points de contacts indiqués par le Responsable de traitement au titre des Prestations ; ou
- Par e-mail au référent RGPD / délégué à la protection des données du Responsable de traitement si les coordonnées de celui-ci ont été communiquées au Sous-traitant ou aux points de contacts indiqués par le Responsable de traitement au titre des Prestations.

Ce délai permet au Sous-traitant de mettre en place les actions correctives, même de manière provisoire, analyser la source des anomalies rencontrées et produire un pré-rapport transmis au Responsable de traitement.

Conformément à la Réglementation applicable, 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 référent RGPD / 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 Sous-traitant 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.

Cette notification est accompagnée de toute la documentation utile afin de permettre au Responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

En application de la Réglementation applicable, le Responsable de traitement peut devoir (i) notifier à l'autorité de contrôle compétente la violation de Données à caractère personnel, et ce dans les meilleurs délais (et, si possible, soixante-douze (72) heures au plus tard après en avoir pris connaissance) et (ii) communiquer aux personnes concernées sur l'existence de ladite violation.

Article 10 : Analyse d'impact et consultation préalable

Sur le périmètre des Prestations qui lui a été confié et si le Responsable de traitement lui en fait la demande, le Sous-traitant contribue aux analyses d'impact relative à la protection des données décidées par le Responsable de traitement. Le Sous-traitant assistera également le Responsable de traitement si ce dernier doit consulter l'autorité de contrôle préalablement à la mise en œuvre du traitement considéré.

Le Sous-traitant garantit l'information et son assistance au Responsable de traitement concernant des opérations de contrôle de l'autorité de contrôle, dès lors qu'elles concernent les Prestations. Il en est de même lorsqu'une autorité compétente sollicite des informations de la part du Sous-traitant, par exemple dans le cadre d'une procédure d'infraction ou d'une procédure pénale relative au traitement de Données à caractère personnel lors de la sous-traitance.

Article 11 : Mesures de sécurité

Le Sous-traitant s'engage à mettre en œuvre toutes les mesures de sécurité qui sont à sa disposition et qui permettent d'assurer le niveau de sécurité proportionné au regard de la Réglementation applicable.

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

- 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.

Le Sous-traitant décrit spécifiquement les mesures qui sont mises en œuvre dans le cadre des Prestations au Contrat et en particulier à l'**Annexe 2** des CP HDS OCI Cloud. Le Sous-traitant s'engage à fournir au Responsable de traitement, à sa demande, les informations nécessaires et notamment à démontrer que les mesures techniques et organisationnelles ont été mises en œuvre.

Ces éléments de preuve doivent permettre au Responsable de traitement de vérifier la conformité du Sous-traitant vis-à-vis des exigences de la Réglementation applicable et que la protection des droits de la personne concernée est garantie.

Article 12 : Sort des Données à caractère personnel

Au terme des Prestations ou des opérations impliquant le traitement de Données à caractère personnel, le Sous-traitant s'engage, conformément au délai indiqué au Contrat ou éventuellement, selon les modalités convenues entre les Parties à :

- Renvoyer toutes les Données à caractère personnel au Responsable de traitement ;
- Détruire toutes les Données à caractère personnel.

Article 13 : Délégué à la protection des données

Les Parties se communiquent l'une à l'autre **les coordonnées de leur délégué à la protection des données**, si elles en ont désigné un conformément à la Réglementation applicable. Les Parties s'informeront mutuellement de tout changement des coordonnées du délégué à la protection des données.

Article 14 : 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 et des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données si les coordonnées de celui-ci lui ont été communiquées ;
- 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 et l'instrument de garantie associé ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles applicables au traitement considéré.

Article 15 : Transfert de Données à caractère personnel hors de l'Union Européenne

Le Responsable de traitement autorise le Sous-traitant à procéder à des transferts de Données à caractère personnel hors de l'Union européenne ou à destination de sociétés ne relevant pas exclusivement du droit européen. Dans ce cas, le Sous-traitant y procède conformément à la Réglementation applicable. A ce titre, le Sous-traitant agit en tant que mandataire du Responsable et revêt la qualité d'« Exportateur de Données à caractère personnel » tandis que le Sous-traitant Ulérieur est « Importateur de Données à caractère personnel ». C'est le cas notamment lors du recours à certains Sous-traitants Ulérieurs (par exemple : Fournisseur opérant de tels transferts). Lorsque ce transfert a lieu vers un pays reconnu comme n'offrant pas un niveau suffisant de protection des Données à caractère personnel par la Commission européenne, le Sous-traitant mettra en place des garanties appropriées préalablement à ce transfert. Dans le cas où le Sous-traitant met en place permettant de garantir un niveau de protection équivalant à la Réglementation applicable.

Droit d'audit

Article 16 : Audit

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 de traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Le Responsable de traitement ou tout auditeur mandaté par lui ne concurrençant pas les activités commerciales du Sous-traitant, pourra procéder à toute vérification qui lui paraîtrait utile pour s'assurer du respect des obligations fixées par le présent Accord.

Le Responsable de traitement pourra procéder à cet audit sur le site convenu avec le Sous-traitant, sous réserve des conditions éventuellement prévues dans la relation entre le Sous-traitant et les Sous-traitants Ulérieurs (par exemple : interdiction de réaliser un audit physique) et dans la limite d'un (1) audit par an. Pour ce faire, le Responsable de traitement devra au préalable demander au Sous-traitant que ce dernier lui communique la documentation sur les traitements mis en œuvre pour le compte du Responsable de traitement. Si ceux-ci laissent apparaître l'éventualité d'un manquement aux obligations du Sous-traitant, le Responsable de traitement pourra mettre en œuvre sa faculté d'audit et en informera le Sous-traitant par écrit du démarrage de la vérification avec un délai de préavis minimum de dix (10) jours ouvrés avant la date effective d'audit. L'information devra indiquer (i) l'objet et le périmètre de l'audit, qui ne sauraient être plus larges que le périmètre des Prestations, et (ii) la durée de l'audit qui ne pourra pas excéder deux (2) jours, et (iii) l'identité de la ou des personnes qui effectueront l'audit.

Le Sous-traitant devra mettre à disposition du Responsable de traitement toutes les informations nécessaires pour permettre la réalisation de l'audit. Ces informations seront couvertes par l'obligation de confidentialité.

Le Responsable de traitement prend à sa charge tous les frais occasionnés par l'audit et rembourse au Sous-traitant ou au Sous-traitant Ulérieur toutes les dépenses et frais justifiés occasionnés par cet audit, y compris le temps consacré à l'audit en fonction du taux horaire moyen du personnel du Sous-traitant ou du Sous-traitant Ulérieur ayant collaboré à l'audit, dans la limite du taux horaires pratiqué entre les Parties. Les Parties peuvent au préalable convenir des conditions financières dans une Offre commerciale.

L'audit se déroulera pendant les Jours ouvrés et aux Heures Ouvrées et ne devra en aucune façon porter atteinte au

secret des affaires du Sous-traitant ou du Sous-traitant Ulérieur, ni leur causer une quelconque désorganisation au-delà de la mise à disposition par le Sous-traitant ou du Sous-traitant Ulérieur des ressources humaines, logiques ou matérielles permettant la réalisation de l'audit.

Le Responsable de traitement mettra gratuitement à disposition du Sous-traitant le rapport d'audit produit. Dans l'hypothèse où des écarts seraient constatés durant l'audit, les Parties s'engagent à échanger et collaborer de bonne foi pour la mise en œuvre des mesures nécessaires.

Annexe A – Détails du traitement

Conformément à l'article 2 DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DE LA SOUS-TRAITANCE, les modalités de traitement se présentent de la manière suivante :

Nature des opérations réalisées sur les Données à caractère personnel	Les opérations réalisées sur les Données à caractère personnel dépendent des Prestations portant sur tout ou partie des solutions proposées par le Sous-traitant dans le domaine de l'informatique et des télécom décrites à l'Offre commerciale. Les opérations réalisées sont les suivantes : Collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement. Le Responsable de traitement reconnaît que les Prestations peuvent inclure des produits et des services de tiers traitant les Données à caractère personnel qui sont mis à disposition du Responsable de traitement par l'intermédiaire du Sous-traitant (distribution, achat-revente) définis comme les « Produits ». Il s'agit, sans que cette liste ne soit limitative, des Produits logiciels et prestations associées et/ou du Matériel. Le Responsable reconnaît et accepte que ces tiers sont ses sous-traitants directs (par exemple : éditeur ou hébergeur-tiers d'une solution, constructeur d'un Matériel).
Finalité(s) du traitement	Le traitement est fait par le Sous-traitant pour fournir les Prestations. La finalité du traitement est définie par le Responsable de traitement. Si le traitement effectué par le Responsable de traitement est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques, le Responsable de traitement doit choisir les Prestations qu'il confie avec précaution. Lors de l'évaluation du risque, il est notamment tenu compte des critères suivants, sans toutefois s'y limiter : évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, prise de décision automatisée ayant des effets juridiques ou pouvant affecter de manière significative la personne concernée, suivi systématique des personnes concernées, traitement de catégories particulières de données ou de données sensibles, traitement à grande échelle, croisement de données, combinaison de données, traitement de données concernant des personnes vulnérables, utilisation de nouvelles technologies innovantes méconnues du public pour le traitement. En sus de la fourniture des Prestations, le Sous-traitant est autorisé à conserver les Données à caractère personnel, notamment à des fins statistiques (dans la mesure où celles-ci contiennent des Données à caractère personnel), commerciales, marketing, publicitaires et de développement interne (dans la mesure où ce dernier contiendrait de la Donnée à caractère personnel qui ferait alors

	l'objet de mesures d'anonymisation), et dans le cadre du respect des obligations légales auxquelles le Sous-traitant est soumis. La phrase précédente ne vaut pas pour les Données de santé pour lesquelles il est précisé que leur utilisation à des fins marketing, publicitaires, commerciales ou statistiques est strictement interdite. Toutefois, le Sous-traitant peut être autorisé à conserver les Données à caractère personnel (incluant de la Donnée de santé) dans le cadre du respect des obligations légales auxquelles le Sous-traitant est soumis.
Catégories de Données à caractère personnel traitées	Les catégories de Données à caractère personnel sont déterminées et contrôlées par le Responsable de traitement, à sa seule discrétion. Le Responsable de traitement fournit les Données à caractère personnel nécessaires au Sous-traitant dans le cadre des Prestations. Les Données à caractère personnel peuvent être les suivantes : ☒ Identité ☒ Vie personnelle ☒ Vie professionnelle ☒ Information d'ordre économique et financier ☒ Données techniques (ex : adresse IP, logs, identifiants, nature d'une problématique dès que lors que celle-ci se rapporte à de la Donnée à caractère personnel) ☒ Données de localisation
Catégories de Données à caractère personnel particulières	Conformément à l'article 9 RGPD, il est rappelé au Responsable de traitement par le Sous-traitant que certaines Données à caractère personnel ne doivent, en principe, ni être collectées ni traitées. Le Responsable de traitement devra informer le Sous-traitant si des Données à caractère personnel suivantes sont traitées dans le cadre des Prestations :

	☒ Données sensibles (dont : données de santé, religion, orientation sexuelle etc.) : Données de santé ; ☐ Données d'infraction et/ou de condamnation ; ☐ Données biométriques.
Catégories de personnes concernées	Les catégories de personnes concernées sont déterminées et contrôlées par le Responsable de traitement.
Durée du traitement	La durée du traitement réalisé par le Sous-traitant correspond à la durée de réalisation des Prestations, augmentée de la durée précisée à l'article 12 SORT DES DONNEES A CARACTERE PERSONNEL. Les durées de conservation pour les autres finalités n'excèdent pas la durée nécessaire au traitement concerné (exemple : conservation dans le cadre du respect d'une obligation légale pendant la durée durant laquelle le Sous-traitant est soumis à ladite obligation légale). Concernant les Données temporaires, elles ont leur propre durée de conservation qui dépend de l'opération concernée. Elles sont conservées le temps nécessaire à la réalisation de l'opération (ex : fichier de rollback, mise à jour d'une base de données, transfert de Données).

Conformément à l'article 13 DELEGUE A LA PROTECTION DES DONNEES, le Responsable de traitement doit indiquer au Prestataire les coordonnées de son délégué à la protection des données s'il en a désigné un conformément à la Réglementation applicable.

Le Sous-traitant déclare avoir désigné des référents RGPD par entité, dont les coordonnées sont les suivantes :

Entités OCI ¹ (hors OCI Ouest)	Entité OCI Ouest SAS	Entité SCRIBA SAS ²
dpoci@oci.fr	dpocinantes@oci.fr	rdcp@oci.fr

¹ Il s'agit des entités : OCI 21 SAS, OCI 25 SAS, OCI 51 SAS, OCI 57 SAS, OCI 67 SAS, OCI 68 SAS, OCI 69 SAS, OCI 77 SAS, OCI Formation SAS, RCI SAS, TCI SAS

² SOCIETE DE CONSEILS EN REPROGRAPHIE INFORMATIQUE ET BUREAUTIQUE D'AQUITAINE SAS