CONDITIONS PARTICULIERES SPECIFIQUES

–

« OCI CLOUD – HDS »

Les présentes conditions particulières spécifiques à l'hébergement de données de santé (ci-après les « **CP HDS** ») constituent le socle unique de la relation commerciale entre les parties, telles que définies dans cet article (ci-après les « **Parties** »). Elles définissent les conditions dans lesquelles le prestataire – dont les coordonnées sont reprises dans l'offre commerciale remise au client, puis dans les factures associées (le « **Prestataire** ») – délivre au client professionnel (le « **Client** ») les Prestations.

Les CP HDS ont pour objet de définir les conditions juridiques, techniques et commerciales des Prestations souscrites et souscriptibles par le Client au titre de projets d'hébergement de données de santé.

1. Champ d'application - opposabilité

Le champ d'application de l'article 1 des CGH est complété comme suit :

Dans le cadre de ses activités, le Client a souhaité bénéficier des services du Prestataire, certifié « Hébergeur de données de santé », afin d'héberger ses données de santé.

La Prestation est souscrite par le biais de l'Offre commerciale et / ou du Bon de commande concerné qui précise notamment les conditions financières.

2. Définitions

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

Les définitions suivantes sont ajoutées à l'article 2 – Définitions des CGH :

« **Certification HDS** » : désigne la certification « Hébergeur de Données de Santé » dite « HDS » (référentiel de certification HDS applicable à la date de signature des présentes conditions particulières : « Référentiel de certification HDS – Mai 2018 ») ;

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

3. Obligations des Parties

L'article 5 des CGH est complété comme suit :

3.1. Obligations communes

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, le Prestataire indique à ce jour conserver ses politiques de sécurité dans leur dernière version pour leur durée d'applicabilité et les versions en cours de modification. 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. Des éléments peuvent être décrits au sein de la politique de confidentialité du Prestataire disponible sur son site internet (https://www.oci.fr/mentions-legales/).

3.2. Obligations du Prestataire

Hébergeur de Données de Santé – Pour proposer puis exécuter les Prestations, le Prestataire doit bénéficier de la Certification HDS. En tout état de cause, le Prestataire ne pourra pas refuser de communiquer ses rapports d'audit de Certification HDS à son Client, dès lors que ce dernier lui en fait la demande et le fournira dans un délai maximum de trente (30) jours après la demande du Client. Il en va de même pour les autres certifications dont le Prestataire bénéficie (ex : ISO 27001).

Sécurité – A la date de signature des CP HDS, les mesures techniques et organisationnelles mises en place sont décrites à l'**Annexe 2** des présentes conditions particulières. 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.

3.3. Obligations du Client

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 des présentes CP HDS 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.

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, 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.

Information – Afin de satisfaire à l'obligation de collaboration, le Client s'engage, pendant toute la durée du Contrat, à informer, préalablement et par écrit, le Prestataire de toute Prestation qu'il envisage de confier à un tiers ou d'exécuter lui-même, pouvant avoir un impact significatif sur l'exécution des Prestations objet du Contrat. Il informe également le Prestataire de toute modification ou toute évolution technique introduites par lui ou imposées dans le cadre légal applicable.

Dans une telle situation, le Prestataire s'engage à analyser les conséquences qui en découlent sur les Prestations réalisées et à aviser le Client de toute incompatibilité. Le Prestataire pourra, sur demande du Client, valider la faisabilité technique et financière si cette situation induit de modifier les Prestations et / ou de souscrire à des Prestations complémentaires.

Coopération – En plus de la désignation d'un interlocuteur privilégié, le Client doit désigner un point de contact qui soit 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.*) et lui fournit les coordonnées à compter de la souscription des Prestations.

Il lui appartient également à ce titre (i) de s'assurer de la formation de son personnel à l'utilisation de la Solution, (ii) de prendre en compte les conseils fournis par écrit par le Prestataire en veillant à se conformer aux mises en garde de celui-ci et (iii) de s'assurer de la bonne application, par ses collaborateurs et tout tiers intervenant pour son compte, des dispositions des présentes conditions particulières.

4. Etendue des Prestations

Périmètre général des Prestations – le périmètre général des Prestations initialement souscrites par le Client par le biais de l'Offre commerciale initiale est décrit dans l'Offre commerciale.

De manière plus générale et sauf cas particuliers dont les modalités seront prévues par les Parties, les prestations proposées par le Prestataire et que le Client peut souscrire se font en adéquation avec le périmètre de la Certification obtenue décrit en **Annexe 1**.

Le Client est susceptible de demander au Prestataire de prendre en charge des Prestations supplémentaires.

Evolution des Prestations – Dans le cadre de l'exécution du Contrat, il s'agit alors de Prestations complémentaires car elles ne sont pas comprises dans le Contrat à sa date d'acceptation mais s'inscrivent dans le cadre des Prestations proposées par le Prestataire (ci-après les « Prestations complémentaires »). Les Prestations complémentaires ne pourront être proposées que sous réserve de leur faisabilité (technique, juridique et financière) ainsi que, dans certains cas, de l'acceptation d'une Offre commerciale préalable par le Client.

Prestations Tierces – En l'absence de Données de santé, le Client peut également souscrire à une Prestation « classique » d'hébergement, régie par les CGH. En tout état de cause, il revient au Client de vérifier la présence ou non de Données de santé pour lesquelles un hébergement spécifique est nécessaire. Il peut également souscrire à des Prestations Tierces (notamment de services managés) auprès du Prestataire (ex : assistance fonctionnelle au Client, interventions ponctuelles du Prestataire, supervision d'outils pour le compte du Client, *etc.*). Dans ce cas, les Parties conviennent que ces Prestations Tierces seront régies par des conditions générales disponibles sur le site internet du Prestataire. Les Prestations Tierces réalisées par le Prestataire peuvent être limitées à celles que le Prestataire peut réaliser dans le cadre du périmètre de la Certification HDS dont il bénéficie (voir détails en **Annexe 1**).

5. Conditions de mise en œuvre des Prestations

5.1. Conditions générales

Le Prestataire s'engage à fournir au Client l'ensemble des Prestations, pour la durée et selon les conditions prévues au Contrat.

Les Prestations couvertes par les présentes CP HDS s'inscrivent en principe dans le périmètre de la Certification obtenue par le Prestataire et décrit en Annexe 2.

Dans le cadre de la fourniture des Prestations, le Client assure avoir pris connaissance, préalablement à la signature de l'Offre commerciale, de la documentation remise par le Prestataire concernant ces dernières.

A la demande du Client, les Prestations sont fournies dans le cadre d'une infrastructure qui peut être partagée ou dédiée, utilisant les ressources de l'infrastructure hébergée mise à disposition par le Prestataire, sous réserve du respect par le Client des obligations lui incombant, notamment en ce qui concerne l'acquittement du prix dû au titre du Contrat.

Le Client ne pourra utiliser les applicatifs auxquels les Prestations souscrites donnent accès que dans les conditions définies par le Contrat.

Le Prestataire garantit un accès aux Prestations et une exécution de ces derniers conformément aux Niveaux de services communiqués au Client dans les documents contractuels et notamment en Annexe 2.

Le Client est informé que la connexion à la Solution (et par conséquent la réalisation des Prestations) s'effectue via le réseau Internet. Il 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, qui sont par définition indépendantes de sa volonté.

5.2. Sauvegarde

Sauvegarde de la Solution – Par principe, le Prestataire n'effectue aucune sauvegarde des Données hébergées sur la Solution par le Client. Le Prestataire a explicitement informé le Client que celui-ci est responsable de la sauvegarde des Données qu'il héberge dans la Solution et des dangers liés à cette absence de sauvegarde (par exemple en cas de perte ou de dommage affectant les Données), et qu'il lui revient de s'assurer de la cohérence et du contenu desdites sauvegardes.

Le Client peut souscrire, par le biais de l'Offre commerciale initiale, puis, à tout moment et de manière complémentaire, à des Prestations de sauvegarde proposées par le Prestataire. Les Parties décrivent alors les modalités des Prestations Complémentaires de sauvegarde dans une Offre commerciale ou un Bon de Commande et dans les conditions particulières applicables auxdites Prestations Complémentaires.

Sauf dispositions contraires, les Prestations Complémentaires de sauvegarde souscrites ne s'appliquent qu'aux Données nativement présentes dans la Solution.

Sauvegarde vers la Solution – le Client peut souscrire auprès du Prestataire des Prestations Tierces notamment relatives à la sauvegarde de ses Données (ex. sauvegarde externalisée). Pour ce faire, le Prestataire peut accompagner le Client dans le choix de solutions logicielles tierces. Les Données à sauvegarder souhaitées par le Client ne font pas l'objet d'une sauvegarde complémentaire dans la Solution, s'agissant d'une Prestation Tierce. En effet, les Données répliquées depuis une solution tierce dans la Solution ne sont pas considérées comme des Données nativement présentes dans la Solution.

En tout état de cause, le Prestataire garantit la sécurité de la sauvegarde et met en œuvre, à ce titre, les mesures de sécurité appropriées.

5.3. Localisation de l'hébergement

Le Prestataire s'engage à héberger la Solution dans un pays de l'Union européenne. A la date de signature des CP HDS, les lieux d'hébergement possibles sont :

- La France.

6. Propriété intellectuelle

L'article 17.3 est modifié comme suit :

Dans le cadre des CP HDS et conformément à la description des Prestations pouvant être confiées par le Client au Prestataire (voir articles 4 et 5 des CP HDS), le Client est susceptible d'héberger et d'utiliser des logiciels qui lui sont propres ou qui sont édités par des tiers, peu important que les licences soient directement acquises auprès de l'éditeur par le Client ou par le biais du Prestataire. Le Client fera son affaire de prendre connaissance et de respecter les conditions d'utilisation et notamment les droits de propriété intellectuelle afférents à ces logiciels. Le Client veillera à souscrire le nombre de licences nécessaires, celui-ci pouvant évoluer au cours du Contrat. Il reconnaît en outre être seul responsable de la mise en œuvre de ces logiciels et applications (en ce incluant par exemple la gestion des habilitations) conformément aux obligations qui lui sont faites au titre du présent Contrat.

7. Audit

Les Parties conviennent d'ajouter un article sur la réalisation d'un audit :

Le Client peut, au cours de l'exécution des CP HDS, 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 les présentes conditions particulières par le biais d'un audit documentaire et /

ou 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 collaboré 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 aux présentes CP HDS.

7.1. 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).

7.2. Audit physique

Dans le cas où l'audit documentaire révèlerait l'éventualité d'un manquement du Prestataire au regard des engagements qu'il prend au titre des CP HDS ou n'aurait pas permis de vérifier la conformité du Prestataire à ses engagements, le Client pourra procéder à un audit sur le site convenu avec le Client – dans les conditions prévues dans les relations entre le Prestataire et ses éventuels sous-traitants (ex : interdiction de réaliser un audit physique).

Sous réserve de la réalisation préalable de l'audit de sécurité documentaire et que les conditions prévues au paragraphe précédent soit remplie, le Prestataire permet au Client de réaliser un audit sur site dont le lieu 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 les présentes CP HDS. Toutefois, dans le cadre où le Client souhaiterait auditer une application mise en production ou faisant l'objet d'une sauvegarde par le Client sur la Solution (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 et fournira tout complément d'informations sur demande du Prestataire.
- La durée de l'audit ne pourra pas excéder deux (2) jours ;
- 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 de travail 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.

7.3. 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 présent 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.

8. Résiliation

L'article 10 des CGH est complété comme suit :

Absence de Certification HDS – Si au cours du Contrat, le Prestataire venait à perdre la Certification HDS pour quelle que raison que ce soit, il en informera le Client dans les meilleurs délais et ce dernier aura la faculté de résilier par l'envoi d'une notification. Le Client pourra demander la réversibilité des Prestations conformément à l'article 11 des CGH et l'article 9 des CP HDS.

9. Réversibilité

L'article 11 des CGH est complété comme suit :

Restitution des éléments du Client – En plus des dispositions sur la restitution dans les CGH, les Parties conviennent que le Client s'engage à accuser réception de la bonne restitution de ces informations dans les quarante-huit (48) heures suivant la remise. Durant ce délai, le Prestataire

conserve les Données et les supprime conformément au délai indiqué au paragraphe ci-dessous (exemple de Données temporaires).

Procédures – Le Prestataire a rédigé une procédure portant sur :

- La mise à disposition, la restitution ainsi que la destruction des Données à caractère personnel du Client à tout moment (sur demande du Client et à condition que cela n'empêche pas la réalisation par le Prestataire des Prestations souscrites), que le Prestataire s'engage à remettre au Client, à sa demande, dans les trente (30) jours suivants ladite demande.
- Les opérations de réversibilité incluant tous types de Données demandées par le Client à la fin du Contrat.

10. Niveaux de services

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 être 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 du Prestataire, le Client a la faculté de résilier le présent Contrat-cadre et / ou les Bons de commande concernés conformément à l'article 11 des CGH modifié.

Au jour de la signature du présent Contrat, le Prestataire 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 :

Certificat hébergeur-infogéreur	
Descriptif des prestations certifiées	Certification HDS
Couche 1 – MISE A DISPOSITION ET MAINTIEN EN CONDITION OPERATIONNELLE DE L'INFRASTRUCTURE MATERIELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMEENT DE DONNEEES 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 » à l'article 11 des CP HDS.
Couche 2 – 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 3 – MISE A DISPOSITION ET MAINTIEN EN CONDITION OPERATIONNELLE DE LA PLATEFORME D'HEBERGEMENT D'APPLICATIONS DU SYSTEME D'INFORMATION	Oui
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	Non – par le biais des Prestations que le Prestataire propose dans le cadre des présentes CP HDS, le Prestataire n'administre ni n'exploite le système d'information du Client contenant des Données de santé. Il est rappelé à ce titre qu'il revient au Client de s'assurer que le(s) tiers (ex : un éditeur, un prestataire-tiers *etc.*) intervenant sur son système d'information contenant de la Donnée de santé répondent aux exigences HDS, ce périmètre étant formellement exclu des présentes CP HDS 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 – Le Prestataire garantit un taux de disponibilité de 99,9 % de la Solution, ce taux n'incluant pas les incidents techniques impromptus intervenant en-dehors des heures ouvrées (9 heures – 12 heures et 14 heures – 17 heures 30) et/ou les opérations techniques préplanifiées principalement opérées la nuit à partir de 22 heures et étant calculé à partir de la Solution et non à partir des équipements du Client.

Disponibilité des solutions logicielles tierces – en cas d'interaction entre la Solution et une solution logicielle tierce, par exemple dans le cadre de l'hébergement d'une solution tierce dans la Solution, 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.

Maintenance et disponibilité – à la Solution et plus largement aux Prestations peut être momentanément interrompu 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.

11. Mesures organisationnelles et techniques de sécurité HDS

Ces mesures techniques et organisationnelles de sécurité ont été définies par le Prestataire et sont considérées comme acceptées par le Client à la signature du présent Contrat. Ces mesures concernent uniquement le périmètre décrit à l'article 10 des présentes CP HDS (complété le cas échéant de Prestations complémentaires selon le mécanisme prévu à l'article 4 des présentes CP HDS), à condition que ce périmètre s'inscrive dans le périmètre de la Certification HDS décrit à l'article 10 des CP HDS.

ORGANISATIONNELLES		
Gouvernance de la protection des données à caractère personnel / désignation d'un DPO	Le Sous-traitant 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.	Voir article XIII des conditions particulières transverses relatives à la sous-traitance de Données à caractère personnel.
Gouvernance de la sécurité des systèmes d'information	Le Sous-traitant Ultérieur OCI Cloud 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 HDS 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	Le Sous-traitant Ultérieur OCI Cloud 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 Sous-traitant garantit la confidentialité des Données et plus particulièrement des Données à caractère personnel.	Voir article 13 des CGH ; Concernant les Données à caractère personnel, voir plus spécifiquement article V. 3. des conditions

	Certains traitements peuvent justifier que les collaborateurs du Sous-traitant 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).	particulières transverses relatives à la sous-traitance de Données à caractère personnel.
Protection des Données dès la conception	Le Sous-traitant intègre la protection des Données à caractère personnel dans la réalisation de ses Prestations, y compris les exigences de sécurité. La méthode « *privacy by design* » 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 Sous-traitant réalise, sur souscription du Client et en cas possibilité de réaliser des Prestations dans le cadre de la couche 5 de la Certification HDS, les développements et tests sont réalisés dans des environnements informatiques séparés de ceux en production, et en utilisant des Données fictives ou anonymisées fournies à cet effet.	Voir article V. 5. des conditions particulières transverses relatives à la sous-traitance de Données à caractère personnel.
Politique du zéro papier	Le Sous-traitant met en place une politique zéro papier.	
Supports amovibles	Les employés du Sous-traitant et de ses Affiliés 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 surveillances des activités de l'hébergement	Les activités des administrateurs sont régulièrement contrôlées par le Sous-traitant Ultérieur OCI Cloud à travers l'analyse des traces techniques et organisationnelles.	
Gestion des incidents	Le Sous-traitant et ses Affiliés ont établi 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. Le Sous-traitant et / ou ses Affiliés analysent 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 Sous-traitant 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 Sous-traitant pour détecter les menaces de sécurité et les vulnérabilités potentielles, et de réagir rapidement pour minimiser les risques.	
Sensibilisation et formation	Le Sous-traitant 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 Sous-traitant 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 Sous-traitant 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.	Voir article 22 des CGH ; Voir article VI des conditions particulières transverses et spécifiques relatives à la sous-traitance de Données à caractère personnel.
Certifications	ISO 27001 Certification HDS	Voir article 10 des CP 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 Sous-traitant 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 Sous-traitant et ses Affiliés suivent 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	Pour le Sous-traitant et ses Affiliés, l'accès aux systèmes 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	Le Sous-traitant 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 à privilèges	L'usage des programmes utilitaires à privilèges est restreinte.	
Activité de surveillance	Le Sous-traitant 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	Le Sous-traitant 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 ultérieurs.	Voir article 11 des CGH ; Voir article XII des conditions particulières transverses et spécifiques relatives à la sous-traitance de Données à caractère personnel.
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 Sous-traitant 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 Sous-traitant 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 Sous-traitant 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 Responsable de traitement est responsable de mettre en place ou non des sauvegardes de ses Données. Lorsque l'option est souscrite auprès du Sous-traitant, le Sous-traitant réalise 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.	Voir article 5.2 des CP HDS.
Révision et gestion des changements	Le Sous-traitant 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.	Voir article 3 des CP HDS ; Voir article XI des conditions particulières relatives à la sous-traitance de Données à caractère personnel.