OCI INFORMATIQUE & DIGITAL

CONDITIONS PARTICULIERES

« HEBERGEMENT (IAAS, PAAS ET SAAS) ET SAUVEGARDE (CLOUDEO) DE DONNEES DE SANTE »

Version en vigueur à compter du 18 mai 2026

Le présent document décrit les Conditions particulières applicables aux Prestations spécifiques d'hébergement de données de santé sur une solution d'hébergement.

Elles viennent préciser les conditions générales de service du Prestataire (les « **CGS** ») dans leur dernière version en vigueur disponible sur son site Internet à l'adresse suivante : https://www.oci.fr/conditions-generales/.

Article 1. Champ d'application

Le Prestataire a développé un catalogue de services d'hébergement et notamment de mise à disposition d'une solution informatique d'hébergement de données en mode locatif externalisé, appelée « Cloudéo », permettant de consacrer des ressources pour chaque Client afin de répondre aux besoins de ce dernier lorsqu'il souhaite héberger des données de santé.

Article 2. Définitions spécifiques

En sus des définitions prévues aux CGS, certaines définitions sont spécifiquement applicables aux prestations couvertes par les présentes Conditions particulières :

« **Certification HDS** » désigne la certification « Hébergeur de Données de Santé » (HDS) (basée sur le référentiel v2.0) dont l'Hébergeur est titulaire dont le périmètre est repris à **l'Annexe A** ;

« **Données de connexion** » 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 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 ;

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

« **Hébergement** » désigne selon le cas un Hébergement dédié ou mutualisé ;

« **Hébergement dédié** » désigne la mise à disposition par le Prestataire d'un environnement d'hébergement sur la Solution d'hébergement dans lequel les éléments le constituant sont exclusivement allouées au Client ;

« **Hébergement mutualisé** » désigne la mise à disposition par le Prestataire d'un environnement d'hébergement sur la Solution d'hébergement dans lequel les éléments le constituant sont partagées par le Client avec d'autres clients ;

« **Incident** » désigne une panne liée à la Solution d'hébergement ou à l'Hébergement mutualisé ou dédié ;

« **Ressources** » désigne le Computer Processing Unit (CPU), la mémoire vive (RAM) et la capacité de stockage ainsi que la bande passante allouée au Client dans le cadre de la mise à disposition de la Solution d'hébergement. Dans le cadre d'une prestation de *housing*, les ressources peuvent être physiques (emplacement dans un date center, alimentation électrique, connectivité) et système ;

« **Solution d'hébergement** » désigne la solution d'hébergement fournie par un Affilié du Prestataire (ci-après l'« **Hébergeur** » qui agit en tant qu'hébergeur de Données de santé au sens de l'article L. 1111-8 du Code de la santé publique et bénéficie de la Certification HDS) composée de matériels physiques constituant l'infrastructure matérielle ainsi que la couche logicielle permettant la virtualisation de la Solution d'hébergement et des Ressources destinées au traitement des Données. La Solution d'hébergement est utilisée comme base pour mettre à disposition du Client les Prestations sur lesquelles il bénéficie d'un droit d'accès et d'utilisation.

Article 3. Obligations spécifiques des Parties

Données de connexion – Conformément au droit applicable, chaque Partie conserve pendant une durée d'un (1) an à compter du jour de leur enregistrement, toutes les Données de connexion dont elle a la charge.

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.

3.1. Obligations spécifiques du Client

Interlocuteurs privilégiés – 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.

3.2. Obligations spécifiques du Prestataire

Hébergeur de Données de santé – Pour les Prestations par lesquelles le Client héberge des Données de santé sur la Solution d'hébergement (la mention « HDS » doit être présente dans l'Offre commerciale), le Prestataire atteste que l'Hébergeur est détenteur de la Certification HDS en sa qualité d'« hébergeur-infogéreur ». La Certification HDS de l'Hébergeur est disponible sur le site internet du Prestataire https://www.oci.fr/vos-experiences/nos-certifications et sur le site de l'Agence du numérique en santé. A la demande du Client, le Prestataire pourra également lui communiquer une copie des rapports d'audit de la Certification HDS.

Accès aux Données – L'Hébergeur a rédigé une procédure portant sur l'accès aux Données par le Client et lui permettant la mise à disposition, la restitution ainsi que la destruction des Données à caractère personnel du Client (incluant les Données de santé) à tout moment (sur demande du Client et à condition que cela n'empêche pas la réalisation des Prestations), que le Prestataire s'engage à remettre au Client, à sa demande, dans les trente (30) jours suivants ladite demande. Cette procédure est utilisée en phase de Réversibilité et précise les opérations envisageables de Réversibilité (incluant tous types de Données) demandées par le Client.

Procédure en cas de défaillance de l'Hébergeur – L'Hébergeur dispose de procédures destinées à couvrir toute défaillance éventuelle de sa part ou de la part de ses sous-traitants, en ce inclus les cas relatifs à une évolution technique ou réglementaire. Le Prestataire tient ces procédures à la disposition du Client si ce dernier lui en fait la demande. Cette procédure prévoit *a minima* une information à destination du Client ainsi que son accord préalable si cette défaillance impacte négativement les Niveaux de service ou les Prestations.

3.3. Faculté d'audit

Le Client peut, au cours de l'exécution du Contrat, vérifier la conformité des Prestations fournies et notamment les mesures de sécurité mises en place par le Prestataire dans le cadre des Prestations en procédant, sous réserve du respect des dispositions prévues au présent article, à des audits. 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 documentaire – Sauf à justifier de limitations raisonnables, le Prestataire met à la disposition du Client à sa demande la documentation nécessaire pour démontrer le respect de toutes ses obligations. En tout état de cause, le Prestataire ne pourra refuser de communiquer au Client les documents suivants : la copie de la Certification HDS et le rapport d'audit associé, la copie de l'éventuelle certification HDS de ses sous-traitants, la procédure encadrant la mise à disposition et la restitution et la destruction des Données à caractère personnel du Client.

Audit physique – Dans le cas où l'audit documentaire n'aurait pas permis de vérifier la conformité du Prestataire à ses engagements contractuels ou qu'il laisserait apparaître un possible manquement à ces derniers, le Client pourra, dans la limite d'une (1) fois par an, diligenter un audit.

Cet audit, dont le lieu devra être convenu entre les Parties, devra tenir compte des conditions prévues entre le Prestataire et ses éventuels Fournisseurs (par exemple : interdiction de réaliser un audit physique).

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 quinze (15) 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. Il est d'ores et déjà entendu que (i) 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 justifie dûment dans sa demande et (ii) 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.
- La durée de l'audit ne pourra pas excéder deux (2) Jours Ouvrés ;
- L'identité de la ou des personnes qui effectueront l'audit, étant entendu que l'auditeur ne pourra être un tiers concurrençant de manière directe ou indirecte le Prestataire et/ou l'un de ses Affiliés.

L'audit sera défini au préalable entre le Prestataire, l'auditeur et le Client. 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.

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 au Contrat, à la Réglementation applicable et/ou 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.

Article 4. Périmètre des Prestations

Périmètre initial – Le Client a souscrit à des Prestations par le biais d'une Offre commerciale qui s'inscrivent dans les présentes Conditions particulières. Les principales prestations que le Prestataire propose sont décrites aux Fiches techniques et en **Annexe B** des présentes Conditions particulières.

Dans le cas où le Prestataire (i) ferait évoluer techniquement les Prestations ou (ii) serait tenu de se conformer à une nouvelle exigence légale ou réglementaire et que cette mise en conformité impacte négativement les Niveaux de service et/ou les Prestations (et notamment la disponibilité, l'intégrité, la confidentialité ainsi que l'auditabilité des Données hébergées), le Prestataire s'engage à en informer le Client dans les meilleurs délais.

Article 5. Limites générales des Prestations

La responsabilité du Prestataire ne pourra pas être engagée par le Client en cas de préjudice subi par le Client ou des tiers du fait des Produits logiciels, Données ou des Contenus hébergés sur la Solution d'hébergement dont le Client a seul la maîtrise et que ce dernier héberge et/ou stocke sur la Solution d'hébergement.

Article 6. Droits de propriété intellectuelle sur la Solution d'hébergement

Le Prestataire garantit qu'il dispose des droits nécessaires aux fins de mettre à disposition du Client, dans le cadre des Prestations, la Solution d'hébergement, l'Hébergeur ou les ayants-droits restant seuls titulaires de l'ensemble des droits, notamment de propriété intellectuelle, portant sur la Solution d'hébergement.

Article 7. Modalités spécifiques de Réversibilité

Les opérations incluses dans le cadre de la Réversibilité simple sont les suivantes :

Offre IaaS (opérations envisageables)		
	Option 1	**Option 2**
Opération possible de Réversibilité	Fourniture des fichiers de sauvegarde (format Veeam pour les VM, XML ou équivalent pour les fichiers de configuration	Fourniture d'un pont de migration via Veeam Replication ou via VMWAre Cloud Director Availability (selon possibilités techniques et offres souscrites)
Prérequis	Le Client devra fournir un NAS qui sera réinitialisé par l'Hébergeur et dont la capacité de stockage doit être suffisante au regard de la quantité de fichiers.	N/A
Tarif forfaitaire de la Réversibilité : 3 000 € HT (tarif 2026)		

Offre PaaS (Kubernetes managé) (opérations incluses)

- Fourniture de l'export total des fichiers « manifest » du cluster Kubernetes via un lien de téléchargement sécurisé au format YAML compressé dans une archive ZIP,
- Fourniture des données stockées au format NFS soit *via* :
  ○ La mise à disposition d'un NAS avec capacité suffisante par le Client, qui sera réinitialisé par l'Hébergeur.
  ○ Des transferts réseaux via le protocole SFTP, destination fournie par le Client.

Tarif forfaitaire de la Réversibilité : 3 000 € HT (tarif 2026)

Offres SaaS (services mutualisées et infogérées tels que bureaumobile et mailmobile) (opérations envisageables)		
	Option 1	**Option 2**
Opération possible de Réversibilité	Fourniture des fichiers dans leur format d'origine via un lien de téléchargement	Fourniture des fichiers dans leur format d'origine sur une unité de stockage NAS
Prérequis	N/A	Le Client fournira un NAS qui sera réinitialisé par l'Hébergeur et dont la capacité de stockage est suffisante.

Tarif forfaitaire de la Réversibilité : 2 000 € HT (tarif 2026)

Précisions sur le *housing* – Dans le cas du *housing*, le Prestataire s'engage à restituer au Client le matériel appartenant au Client. Le Client reconnaît alors que les conditions d'accès au datacenter sont définies par le Fournisseur et doivent être strictement appliquées par le Prestataire et/ou le Client si le Client est autorisé à s'y rendre. Le Client reconnaît par ailleurs que la procédure de réversibilité dans le cadre d'un hébergement en mode *housing* peut générer une interruption de service.

Précisions quant à l'obligation de collaboration du Client – De son côté, le Client s'engage à fournir toute l'assistance requise pour mener à bien la Réversibilité, et notamment, le cas échéant, à impliquer tout tiers en temps utiles et à garantir sa collaboration. Dans le cas du *housing* spécifiquement, il doit par exemple être tenu compte des modalités financières et opérationnelles imposées par le Fournisseur du datacenter. Par ailleurs, le Client s'engage à vérifier les Données restituées dans les cinq (5) jours suivant leur remise par le Prestataire. Sans retour de la part du Client, il est réputé avoir reçu et accusé réception de la bonne restitution des Données.

Article 8. Dispositions spécifiques applicables à la protection des Données à caractère personnel

Les Parties appliquent les dispositions prévues dans l'accord de sous-traitance RGPD repris en **Annexe C.**

Le Prestataire indique si l'Hébergeur et/ou ses sous-traitants sont soumis à une réglementation extra-communautaire permettant un accès aux Données de santé, conformément au tableau des garanties disponible sur le site internet du Prestataire au lien suivant : Nos certifications techniques | OCI, dans la rubrique « Hébergement de données de santé ». Ce document contient également les éventuels certificats des sous-traitants participant à l'activité d'hébergement.

Article 9. Hypothèse spécifique de fin du Contrat

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.

ANNEXE A
CERTIFICATION HDS ET MESURES DE SECURITE

Article 1. Certification HDS

Le Prestataire indique que la Certification HDS est valide depuis le 20 décembre 2023 et a une durée de validité allant jusqu'au 19 décembre 2026.

Descriptif des prestations certifiées	Certification HDS	Contrat de service associé
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, 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 » au sein des mesures de sécurité.	Contrat d'hébergement HDS
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, si le Client a souscrit à des prestations de housing.	Contrat d'hébergement HDS
Couche 3 – MISE A DISPOSITION ET MAINTIEN EN CONDITION OPERATIONNELLE DE LA PLATEFORME D'HEBERGEMENT D'APPLICATIONS DU SYSTEME D'INFORMATION	Oui	Contrat d'hébergement HDS
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	Contrat d'hébergement HDS, avec services managés possibles : maintenance curative, maintenance préventive, gestion des demandes de changement, supervision d'éléments…
Couche 5 – ADMINISTRATION ET EXPLOITATION DU SYSTEME D'INFORMATION CONTENANT LES DONNEES DE SANTE	Oui – 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 du système d'information des Données de santé, avec son ou ses éditeurs de logiciels contenant des données de santé. Par ailleurs, le Client doit s'assurer que le(s) tiers (par exemple : l'éditeur, le prestataire-tiers *etc.*) intervenant sur son système d'information contenant de la Donnée de santé réponde(nt) aux exigences HDS, ce périmètre étant formellement exclu du présent Contrat et de la responsabilité du Prestataire. 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.	Contrat d'hébergement HDS, avec services managés possibles : maintenance curative, maintenance préventive, gestion des demandes de changement, supervision d'éléments voire prestations portant sur l'administration et/ou l'exploitation de Produits logiciels métiers contenant des Données de santé souscrites par le Client
Couche 6 – SAUVEGARDES EXTERNALISEES DES DONNEES DE SANTE	Oui	Contrat d'hébergement HDS, avec prestation de sauvegarde, services managés possibles : maintenance curative, maintenance préventive, gestion des demandes de changement, supervision d'éléments…

Article 2. Mesures de sécurité

La Solution d'hébergement fait l'objet de mesures d'ordre technique et organisationnel définies par l'Hébergeur équivalentes à celles prescrites par le référentiel de la norme ISO 27001. Ces mesures ont pour objectif de limiter et/ou de restreindre les menaces, vulnérabilités et risques ou conséquences associées portant sur l'intégrité, la disponibilité et la confidentialité de la Solution d'hébergement dans son ensemble. 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 qu'il prend, par exemple de sauvegarde, 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.

Par ailleurs, 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).

Ainsi, en sus des mesures de sécurité définies par le Client, le Prestataire et l'Hébergeur ont défini des mesures techniques et organisationnelles de sécurité (ayant notamment vocation à encadrer l'accès aux Données hébergées). Celles-ci peuvent être modifiées, à tout moment et sans préavis, à condition que ces modifications n'engendrent pas une diminution du niveau de protection garanti initialement.

MESURES ORGANISATIONNELLES	
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 ISO 27001.
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'actions pour les maîtriser.
Confidentialité	Le Prestataire garantit la confidentialité des Données et plus particulièrement des Données à caractère personnel. Certains traitements peuvent justifier que le Prestataire mette en œuvre des obligations de confidentialité renforcée spécifiques avec certains collaborateurs du Prestataire ou de l'Hébergeur (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 « *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. **Option HDS :** Lorsque le Prestataire réalise, sur souscription du Client à des Prestations s'inscrivant 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 surveillance 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	L'Hébergeur effectue une surveillance régulière 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 (i) 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 incidents de sécurité et (ii) concevoir, mettre en œuvre et suivre les programmes de sécurité chez le Prestataire. 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. L'Hébergeur a mis en place un dispositif de détection et de remédiation des incidents de sécurité. Dans ce cadre, la BU Cybersécurité surveille les systèmes d'information concernés pour détecter les menaces de sécurité et les vulnérabilités potentielles, et de réagir rapidement pour minimiser les risques. **Option :** Le Client peut souhaiter disposer d'un tel dispositif sur la Solution d'hébergement et souscrire, à cette fin, à une Prestation complémentaire dite « EDR/SOC ».
Sensibilisation et formation	L'Hébergeur 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.

MESURES 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 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.
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. **Option HDS :** La mise en place du bastion est rendue obligatoire pour les Prestations associées à la couche 5.
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 au Client à sa 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 à privilèges	L'usage des programmes utilitaires à privilèges est restreint.
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 intervenants 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.
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 protocoles sécurisés pour les sites web	L'Hébergeur 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.
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.
Chiffrement	Sur les réseaux publics, les flux sont chiffrés. Les Données fournies par le Client doivent être chiffrées avant réception par l'Hébergeur. 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. **Option HDS :** Le Client peut souscrire à une Prestation de sauvegarde (sauvegarde externalisée – couche 6 ou sauvegarde associée aux Prestations s'inscrivant dans les autres couches). Dans ce cas, 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.

ANNEXE B
CATALOGUE ET DESCRIPTION DES PRESTATIONS

Article 1. Catalogue de prestations

De manière générale, les Prestations d'hébergement portent sur la réservation par le Prestataire de Ressources qu'il met à disposition du Client en fonction de ce qui est précisé dans l'Offre commerciale. Ces Ressources permettent ensuite au Client de bénéficier d'un Hébergement mutualisé ou dédié pour répondre aux besoins exprimés par le Client. Les Ressources constituant l'Hébergement font l'objet d'un maintien en conditions opérationnelles par le Prestataire.

Lorsque l'Hébergement est mis en place par le Prestataire, celui-ci facture les frais de mise en service (FMS) ou d'accès au service (FAS) prévus à l'Offre commerciale.

1.1. Hébergement

1.1.1 Abonnement à l'Hébergement

En parallèle de la souscription aux licences nécessaires, l'abonnement à l'Hébergement inclut :
- La réservation de Ressources,
- Le droit d'accès et d'utilisation des Prestations à compter de leur Mise en service ;
- Le maintien en conditions opérationnelles de ces Ressources,
- Les éventuels services managés.

1.1.2 Mise en service des Prestations

Type d'hébergement	Installation de l'Hébergement réalisée par	Mise en service de l'Hébergement à compter de la transmission par le Prestataire au Client de…
Hébergement mutualisé	Installation obligatoire par le Prestataire	Ses identifiants de connexion à l'Hébergement mutualisé
Hébergement dédié	Installation possible par le Prestataire	Ses identifiants de connexion à l'Hébergement dédié
Hébergement dédié	Installation possible par le Client	Ses identifiants de connexion à la plateforme de virtualisation

Les Prestations d'installation de l'Hébergement font l'objet d'une Recette (dont les modalités peuvent être spécifiquement précisées lors d'une réunion de cadrage si le Client a souscrit à une Prestation de gestion de projet). Par défaut, la procédure de Recette est la suivante : le Prestataire met à disposition du Client un cahier de recettage 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 recettage 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.

1.1.3 Description du maintien en conditions opérationnelles

Le Prestataire réalise le maintien en conditions opérationnelles de la Solution d'hébergement qui comprend la réalisation des opérations suivantes en Heures Ouvrées :
- Supervision de l'utilisation des Ressources,
- Supervision de l'état de santé (on/off) des programmes permettant le bon fonctionnement de l'Hébergement et utilisés par le Prestataire,
- Maintenance évolutive mensuelle de la Solution d'hébergement (*patch management* et *vulnerability management*).

1.1.4 Description de la sauvegarde de l'Hébergement

Principe – Le Client est responsable de la sauvegarde des Données et des Contenus qu'il héberge dans son Hébergement et est informé des dangers liés à une éventuelle absence de sauvegarde (par exemple en cas de perte ou de dommage affectant les Données). En cas de sauvegarde de ces éléments (même quand celle-ci est réalisée par le Prestataire), il revient au Client de s'assurer 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.

Option de sauvegarde – Le Client peut souscrire à des prestations de sauvegarde proposées par le Prestataire à tout moment. On dit alors que le Client procède à une sauvegarde des Données nativement présentes dans la Solution d'hébergement. Le Prestataire s'engage à utiliser des méthodes de sauvegarde fiables et est responsable de la disponibilité de l'espace de sauvegarde. Les Parties définissent le nombre de points de rétention ainsi que la période de rétention associée.

Recette – Les Prestations de mise en place d'une sauvegarde font l'objet d'une Recette (dont les modalités peuvent être spécifiquement 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 recettage 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 recettage 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.

Perte des éléments sauvegardés – 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. En fonction des points de rétention mis en place, la restauration d'un élément précis peut ne pas être possible ou être incomplète, sans que le Prestataire ne puisse en être responsable. La perte de Données et/ou de Contenus n'est pas considérée comme un dommage indirect 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.

1.1.5 Exploitation de l'Hébergement

Le Client est seul responsable de l'installation, de l'exploitation, du paramétrage, de la maintenance et de la sécurité des solutions tierces et environnements (applications, logiciels, systèmes d'exploitation, etc.) déployés sur l'Hébergement. Toutefois, sur souscription du Client, cet Hébergement pourra faire l'objet de services dits « managés », c'est-à-dire que les Parties conviennent que certains services seront réalisés par le Prestataire.

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 et à ses besoins. Le Prestataire ne réalise aucune prestation concernant ces applications dans la mesure où l'administration, l'exploitation et les services connexes de telles applications sont assurés par le Client ou par les tiers qu'il mandate à ces fins. A ce titre, le Client s'engage à :

- Mettre en place et appliquer une méthodologie de vérification des applications qu'il héberge ;
- S'assurer que le Client 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 ;
- S'assurer du respect des prérequis définis et communiqués par le Prestataire à sa demande pour la partie hébergement ;
- 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.
- Gérer les autorisations et habilitations d'accès à son système d'information hébergé par les Utilisateurs.

1.2. Stockage S3

1.2.1 Abonnement à un stockage S3

Le stockage S3 est un espace de stockage mis à disposition du Client (Hébergement dédié) et opéré par ce dernier (sauf service managé souscrit).

Dans ce cadre, en parallèle de la souscription aux licences nécessaires, l'abonnement à un stockage S3 inclut :

- La réservation de Ressources de stockage,
- Le droit d'accès et d'utilisation des Prestations à compter de leur Mise en service ;
- Le maintien en conditions opérationnelles des Ressources de stockage,
- Les éventuels services managés.

1.2.2 Mise en service des Prestations

Type d'hébergement	Installation de l'Hébergement réalisée par	Mise en service de l'Hébergement à compter de la transmission par le Prestataire au Client de…
Hébergement dédié	Installation possible par le Prestataire	Ses identifiants de connexion à l'interface de stockage S3

1.2.3 Maintien en conditions opérationnelles

Le Prestataire réalise le maintien en conditions opérationnelles de la Solution d'hébergement qui comprend la réalisation des opérations suivantes en Heures Ouvrées :

- Supervision de l'utilisation des Ressources de stockage de l'environnement de stockage S3,
- Supervision de l'état de santé (on/off) des programmes permettant le bon fonctionnement de l'environnement de stockage S3 et utilisés par le Prestataire,
- Maintenance évolutive mensuelle de la Solution d'hébergement (*patch management* et *vulnerability management*).

1.2.4 Utilisation par le Client du stockage S3 pour sauvegarder des Données

A titre indicatif, le stockage S3 est un Hébergement de stockage mis à disposition du Client pour stocker les Données qu'il souhaite. Dans le cas où le Client l'utilise spécifiquement pour stocker des Données de sauvegarde, le Client opère l'espace à sa convenance et définit lui-même les jobs de sauvegarde, les points et périodes de rétention.

Evolution de la Ressource de stockage – L'ajout de stockage par le Prestataire sur du stockage S3 est une Prestation additionnelle. En effet, le Prestataire réalise un service managé de supervision de la capacité de stockage disponible pour le Client dans le stockage S3. Lorsque les seuils paramétrés par l'Hébergeur sont atteints, le Prestataire augmente le stockage (en moyenne : dix pourcents (10 %)).

1.3. Sauvegarde externalisée

Principe – Le Client est responsable de la sauvegarde des Données et des Contenus qu'il héberge sur ses infrastructures ou chez un tiers et est informé des dangers liés à une éventuelle absence de sauvegarde (par exemple en cas de perte ou de dommage affectant les Données). En cas de sauvegarde de ces éléments (même quand celle-ci est réalisée par le Prestataire),

il revient au Client de s'assurer 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.

Options de sauvegarde externalisée – On parle de sauvegarde externalisée lorsque le Client souhaite sauvegarder des Données non-nativement présentes dans la Solution d'hébergement, c'est-à-dire que les Données à sauvegarder proviennent d'une solution-tierce ou d'une infrastructure non-hébergée chez le Prestataire. Dans ce cas, le Prestataire peut accompagner le Client dans le choix d'un Produit logiciel de sauvegarde adaptée voire dans la mise en place du système de sauvegarde souhaité par le Client. Dans ce cadre, le Prestataire propose deux types de sauvegarde externalisée :
- L'Hébergement de sauvegarde externalisée ;
- La sauvegarde O365.

Maintien en conditions opérationnelles – Le Prestataire réalise le maintien en conditions opérationnelles de l'environnement de sauvegarde choisi par le Client.

Service managé possible – Le Prestataire peut superviser la sauvegarde, c'est-à-dire vérifier la bonne exécution du processus de sauvegarde (bonne réalisation ou non des jobs de sauvegarde).

Perte des éléments sauvegardés – 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. En fonction des points de rétention mis en place, la restauration d'un élément précis peut ne pas être possible ou être incomplète, sans que le Prestataire ne puisse en être responsable. Il appartient donc au Client de s'assurer de sa compréhension du fonctionnement des points de rétention, notamment de leur récurrence et des conséquences de cette dernière sur la possibilité de restauration associée. La perte de Données et/ou de Contenus n'est pas considérée comme un dommage indirect si celle-ci s'inscrit dans une défaillance du système de sauvegarde attribuable au Prestataire et que cette défaillance est directement à l'origine du préjudice éventuellement allégué par le Client.

1.3.1 Hébergement de sauvegarde

Description – Le Client peut souhaiter mettre en place un Hébergement de sauvegarde, c'est-à-dire qu'il fait sauvegarder tout ou partie de son infrastructure sur un Hébergement pour lequel il réserve des Ressources de stockage.

Rétention des Données – Les Parties définissent le nombre de points de rétention ainsi que la période de rétention et les jobs de sauvegarde associés.

Maintien en conditions opérationnelles – Le Prestataire réalise le maintien en conditions opérationnelles de la Solution d'hébergement qui comprend la réalisation des opérations suivantes en Heures Ouvrées :
- Supervision de l'utilisation des Ressources,
- Supervision de l'état de santé (on/off) des programmes permettant le bon fonctionnement de l'Hébergement et utilisés par le Prestataire,
- Maintenance évolutive mensuelle de la Solution d'hébergement (*patch management* et *vulnerability management*).

Evolution de la Ressource de stockage – L'ajout de stockage par le Prestataire sur du l'Hébergement de sauvegarde est une Prestation additionnelle. En effet, le Prestataire réalise un service managé de supervision de la capacité de stockage disponible pour le Client dans l'Hébergement de sauvegarde. Lorsque les seuils paramétrés par l'Hébergeur sont atteints, le Prestataire augmente le stockage (en moyenne : dix pourcents (10 %)).

1.3.2 Sauvegarde O365

Le Prestataire propose une prestation de sauvegarde de l'environnement O365 (Microsoft) du Client sur un Hébergement mutualisé. Les points de rétention ainsi que la période de rétention associée dépendent des possibilités offertes par le Produit logiciel choisi.

Point(s) de rétention et période de rétention – Par défaut, cette prestation permet une période de rétention des Données sur une période de douze (12) mois (sauvegarde une (1) fois par jour pendant douze (12) mois), la période de rétention étant atteinte au bout de douze (12) mois de Prestation.

Maintien en conditions opérationnelles – Le Prestataire réalise le maintien en conditions opérationnelles de la Solution d'hébergement qui comprend la réalisation des opérations suivantes en Heures Ouvrées :
- Supervision de l'utilisation des Ressources,
- Supervision de l'état de santé (on/off) des programmes permettant le bon fonctionnement de l'environnement de stockage des Données O365 et utilisés par le Prestataire,
- Maintenance évolutive mensuelle de la Solution d'hébergement (*patch management* et *vulnerability management*).

Article 2. Services managés

Les services managés peuvent être les suivants et peuvent selon les cas, nécessiter une phase de mise en place par le Prestataire :

Service managé	Description du service managé
Pilotage de l'infrastructure	Le Prestataire assure la surveillance, l'administration et l'optimisation technique des Ressources d'infrastructure (serveurs, réseaux, virtualisation). Cette gestion opérationnelle vise à garantir la stabilité et le Niveau de service relatif à la disponibilité.

Comité(s) de pilotage	Lorsque le Client a souscrit à cette prestation, le Prestataire met en place et anime en présence du Client un comité opérationnel selon la récurrence prévue entre les Parties. Le comité opérationnel a pour objectifs (i) de réaliser un bilan des Prestations et d'en étudier la qualité, (ii) de revoir, à la demande du Client, l'atteinte des Niveaux de service, (iii) d'ajuster si nécessaire le périmètre des Prestations, (iv) d'exposer les évolutions liées au service et aux solutions et les impacts éventuels et ajustements nécessaires des Prestations et (v) d'échanger au sujet d'éventuelles difficultés dans l'exécution du Contrat. Le Prestataire rédige un compte-rendu à la suite de chaque comité et le transmet au Client pour validation dans les dix (10) Jours Ouvrés suivant la tenue du comité. Ce compte-rendu contient au minimum la liste des participants, les décisions prises en comité et le plan d'actions associé si un tel plan d'actions a été défini entre les Parties.
Maintien en conditions de sécurité (sécurité des systèmes)	Le Prestataire procède de manière autonome aux mises à jour de sécurité critiques des systèmes gérés au sein de l'Hébergement. Cette mission est strictement limitée aux couches systèmes (OS) et ne s'étend pas aux applicatifs métiers ou logiciels tiers, dont la maintenance et la compatibilité restent sous la responsabilité exclusive du Client.
Administration des accès et identités	Le Prestataire assure la création, la modification et la suppression des comptes utilisateurs et la gestion des droits associés sur le périmètre défini. Ces interventions sont réalisées exclusivement sur Sollicitation du Client, qui conserve la responsabilité du cycle de vie de ses collaborateurs et de la cohérence des droits d'accès demandés.
Gestion des Ressources de stockage	Les opérations d'ajustement, d'allocation ou d'extension des Ressources de stockage sont effectuées par le Prestataire après validation du Client. Le Client est responsable de la surveillance de ses volumes de données et des coûts induits par toute augmentation des Ressources sollicitées.
Supervision de la sauvegarde	Le Prestataire supervise la sauvegarde, c'est-à-dire qu'il vérifie la bonne exécution du processus de sauvegarde (bonne réalisation ou non des jobs de sauvegarde).
Facturation des services managés	L'ensemble des actes de gestion opérationnelle, de support (N1 à N3) et d'administration est facturé selon les modalités définies entre les Parties à l'Offre commerciale. Toute Sollicitation excédant le périmètre des Prestations (par exemple : intervention sur un environnement non-géré) sera facturée au taux en vigueur chez le Prestataire au moment de la Sollicitation.

Article 3. Options de sécurité

3.1.1 Option d'immuabilité de la sauvegarde

Le Client peut souscrire, en option, à une sauvegarde immuable reposant sur un mécanisme d'immuabilité des sauvegardes pendant une période de sept (7) jours glissants.

Lorsque cette option est activée, chaque sauvegarde concernée est protégée contre toute suppression, modification ou altération pendant une durée de sept (7) jours à compter de sa mise en place. À compter du huitième jour, la sauvegarde la plus ancienne cesse d'être immuable et peut être remplacée, écrasée ou supprimée conformément à la politique de rétention applicable et aux actions administrateurs.

3.1.2 Option PRA

Le Client a la possibilité de réserver des Ressources complémentaires en vue de constituer un plan de reprise informatique (PRI) qu'il pourra activer en cas d'indisponibilité de son infrastructure principale, cette activation étant déclenchée après Sollicitation à destination du Prestataire selon les modalités que le Client a déterminées en matière de reprise d'activités en cas de sinistre. L'activation permettra la bascule de son infrastructure active vers un Hébergement de réplication.

L'infrastructure principale peut être un Hébergement mutualisé, dédié ou une infrastructure non-hébergée chez le Prestataire.

Les modalités opérationnelles d'activation du PRI sont définies entre les Parties. En tout état de cause :
- La quantité maximale de Données (« *Recovery Point Objective* » ou « RPO ») que le Client pourra perdre dépendra du délai s'écoulant entre la dernière sauvegarde valide (si existante) et l'évènement ayant généré l'activation du PRI ;
- Le délai maximal durant lequel le service est indisponible (« *Recovery Time Objective* » ou « RTO ») dépend du temps nécessaire aux opérations de bascule vers l'Hébergement de réplication (incluant le temps de traitement par le Prestataire de la Sollicitation formulée par le Client) et le temps de restauration des éléments contenus dans l'Hébergement.

Le Prestataire informe le Client de la nécessité de prévoir une procédure relative à la gestion des incidents et à la reprise de son activité en cas d'incident générant une indisponibilité. Il revient au Client de s'assurer de l'intégrité des Données et des Contenus sauvegardés ainsi que de la cohérence du contenu desdites sauvegardes et de faire réaliser, en collaboration avec le Prestataire, des tests de PRI ou de PRA à échéances régulières.

3.1.3 Option EDR

Le Client peut souscrire à une option EDR par le biais d'une Offre commerciale qui précise la Solution SOC mise en place. L'option EDR est associée à un Hébergement (hors Hébergement de sauvegarde). Le détail opérationnel de cette option est repris dans les Conditions particulières « Cyber – Surveillance des évènements de sécurité » (CYBER SOC) disponibles sur le site internet du Prestataire. A des fins de bonne lecture de ces Conditions particulières, il est précisé que :
- La notion de « Périmètre surveillé » désigne les éléments de l'Hébergement du Client sur lesquels un agent est installé,
- Les Niveaux de service s'appliquent à l'alerte émise à destination de l'Hébergeur,
- Le traitement de l'Incident de sécurité est réalisé par les équipes de l'Hébergeur ou du Prestataire lorsqu'il s'agit d'une Remédiation.

3.1.4 Option bastion

Le Client peut souscrire à une option bastion nommée « Citadelle » par le biais d'une Offre commerciale qui précise la configuration du bastion mis en place ainsi que le nombre d'accès administrateurs autorisés. L'option Citadelle est associée à un Hébergement de production et constitue le point de passage obligatoire pour toute action d'administration sécurisée. Le détail opérationnel de cette option est repris dans la Fiche technique. Il est précisé que :

- Le périmètre protégé par le bastion désigne les accès d'administration et les flux critiques de l'Hébergement du Client dont l'étanchéité et la traçabilité sont assurées par la solution Citadelle ;
- Le Prestataire prend en charge les anomalies d'authentification ;
- La gestion des accès et le durcissement du bastion sont réalisés par les équipes de l'Hébergeur ou du Prestataire dans le cadre du maintien en conditions de sécurité.

Article 4. Autres prestations possibles

Les autres prestations possibles sont décrites dans les Fiches techniques.

Article 5. Description de la Solution d'hébergement

Localisation de la Solution d'hébergement – Le Prestataire s'engage à ce que la Solution d'hébergement soit hébergée dans l'Union européenne. La localisation des data centers possibles est détaillée dans les Fiches techniques.

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.

Sécurité – Le Client est informé que la Solution d'hébergement fait l'objet de mesures d'ordre technique et organisationnel définies par l'Hébergeur équivalentes à celles prescrites par le référentiel de la norme ISO 27001. Ces mesures ont pour objectif de limiter et/ou de restreindre les menaces, vulnérabilités et risques ou conséquences associées portant sur l'intégrité, la disponibilité et la confidentialité de la Solution d'hébergement dans son ensemble. Ainsi, en sus des mesures techniques et organisationnelles de sécurité définies par le Client, des mesures techniques et organisationnelles de sécurité, ayant notamment vocation à encadrer l'accès aux Données hébergées, ont été définies par le Prestataire et l'Hébergeur. Le Prestataire ou l'Hébergeur peut modifier, à tout moment et sans préavis, tout ou partie des mesures de sécurité techniques et organisationnelles reprises au présent tableau. Cependant, ces modifications ne peuvent engendrer une diminution du niveau de protection des Données.

MESURES ORGANISATIONNELLES	
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 ISO 27001.
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'actions pour les maîtriser.
Confidentialité	Le Prestataire garantit la confidentialité des Données et plus particulièrement des Données à caractère personnel. Certains traitements peuvent justifier que le Prestataire mette en œuvre des obligations de confidentialité renforcée spécifiques avec certains collaborateurs du Prestataire ou de l'Hébergeur (par exemple : les personnes en charge de l'administration, de l'exploitation ou de la maintenance des systèmes d'information).
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 surveillance 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	L'Hébergeur effectue une surveillance régulière 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 (i) 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 incidents de sécurité et (ii) concevoir, mettre en œuvre et suivre les programmes de sécurité chez le Prestataire. 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.

	L'Hébergeur a mis en place un dispositif de détection et de remédiation des incidents de sécurité. Dans ce cadre, la BU Cybersécurité surveille les systèmes d'information concernés pour détecter les menaces de sécurité et les vulnérabilités potentielles, et de réagir rapidement pour minimiser les risques. **Option :** Le Client peut souhaiter disposer d'un tel dispositif sur la Solution d'hébergement et souscrire, à cette fin, à une Prestation complémentaire dite « EDR/SOC ».
Sensibilisation et formation	L'Hébergeur 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.

MESURES 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 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.
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.
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 au Client à sa 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 à privilèges	L'usage des programmes utilitaires à privilèges est restreint.
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 intervenants qui n'ont pas besoin d'y accéder. 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.
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 protocoles sécurisés pour les sites web	L'Hébergeur 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.
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.
Chiffrement	Sur les réseaux publics, les flux sont chiffrés. Les Données fournies par le Client doivent être chiffrées avant réception par l'Hébergeur. Ce dernier ne peut s'engager sur ce chiffrement.

Article 6. Niveaux de service spécifiques

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, les opérations techniques préplanifiées (par exemple : les opérations réalisées dans le cadre du maintien en conditions opérationnelles), les évènements de force majeure et les cas d'interruption liés à une obligation faite au Prestataire. Le taux est calculé à partir de la Solution d'hébergement et non pas à partir des équipements du Client.

Si le Prestataire doit interrompre momentanément les Prestations, il s'efforcera, dans la mesure du possible, d'effectuer l'opération de suspension en-dehors des Heures Ouvrées et de limiter la période d'interruption des Prestations. Toutefois, en cas d'urgence ou dans le cas où la suspension est liée au maintien en conditions opérationnelles réalisé par le Prestataire, le Prestataire informera le Client par tous moyens de la réalisation de telles opérations.

Par ailleurs, sans qu'il ne puisse en être tenu responsable, le Prestataire se réserve la possibilité de suspendre partiellement ou complètement les Prestations si le Prestataire y est obligé pour respecter un ordre, une instruction ou une exigence gouvernementale, d'une autorité de régulation ou de contrôle ou de toute autorité administrative ou judiciaire, européenne, nationale ou locale compétente.

Niveaux de service applicables aux services managés – Le Client peut souscrire à des Prestations de services managés pour lesquels les Niveaux de service sont précisés dans l'Offre commerciale ou les Fiches techniques.

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.

ANNEXE C
ACCORD DE SOUS-TRAITANCE RGPD

Article 1. Définitions spécifiques

« **Accord** » désigne la présente Annexe constituant l'accord de sous-traitance RGPD référencé au Contrat ;

« **Données à caractère personnel** » désigne toute information se rapportant à une personne physique identifiée ou identifiable au sens de la Réglementation applicable ;

« **Réglementation applicable** » désigne la réglementation en vigueur applicable au traitement de Données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ;

« **Responsable de traitement** » : désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ;

« **Sous-traitant** » : désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données à caractère personnel pour le compte du Responsable de traitement.

Article 2. Objet

Le présent Accord a pour objet de définir les conditions dans lesquelles le Prestataire, en sa qualité de Sous-traitant, s'engage à effectuer pour le compte du Client, en tant que Responsable de traitement, les opérations de traitement de Données à caractère personnel dont notamment des Données de santé définies ci-après.

Article 3. Description du traitement faisant l'objet de la sous-traitance

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.

Les modalités de traitement sont décrites à la fiche opérationnelle de traitement jointe au présent Accord.

Article 4. Obligations des Parties

4.1. Obligations du Responsable de traitement vis-à-vis du Sous-traitant

Le Responsable de traitement s'engage à (i) respecter la Réglementation applicable, (ii) fournir au Sous-traitant les Données à caractère personnel concernées, (iii) documenter par écrit toute instruction concernant le traitement des Données à caractère personnel par le Sous-traitant, (iv) 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, et (v) superviser le traitement, en compris le fait de réaliser des audits et/ou des inspections du Sous-traitant.

4.2. Obligations du Sous-traitant vis-à-vis du Responsable de traitement

Le Sous-traitant s'engage à (i) ne traiter les Données à caractère personnel que pour les seules finalités qui font l'objet de la sous-traitance, (ii) 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 ou 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, (iii) garantir la confidentialité des Données à caractère personnel traitées dans le cadre du présent Accord, (iv) 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 reçoivent la formation nécessaire en matière de protection des Données à caractère personnel, (v) 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, et (vi) respecter la Réglementation applicable.

Article 5. Aide du Sous-traitant au Responsable de traitement

5.1. Assistance du Sous-traitant

Le Sous-traitant fournira les informations nécessaires et assistera le Responsable de traitement en cas d'opérations de contrôle et/ou de la mise en œuvre de mesures imposées par une autorité de contrôle, dès lors que ces opérations se réfèrent aux Prestations confiées.

Dans le cas où une autorité compétente le demanderait au Sous-traitant (par exemple : dans le cadre d'une procédure de recherche d'infraction ou une procédure relative au traitement de Données à caractère personnel couvert par l'Accord), le Sous-traitant s'engage à en informer le Responsable de traitement, dès qu'il y est autorisé. En tout état de cause, le Sous-traitant s'engage à ne fournir que les informations strictement pertinentes à la demande formulée par l'autorité compétente.

5.2. Analyse d'impact et consultation préalable

Si le Responsable de traitement lui en fait la demande, le Sous-traitant contribue, dans la mesure des Prestations qui ont été confiées et qui sont concernées, 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.

5.3. Droit d'information des personnes concernées

Dans le cadre de ses obligations, il revient au Responsable de traitement de définir la base légale du / des traitement(s) concerné(s) par la présente Annexe et notamment de prévoir une base légale supplémentaire pour le traitement de Données à caractère personnel sensibles au sens de la Réglementation applicable.

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. Lorsque cela est applicable, la formulation et le format de l'information doivent être convenus avec le Responsable de traitement avant la collecte de Données à caractère personnel. En sus de cette obligation générale, le Responsable de traitement doit, conformément à la Réglementation applicable, avoir préalablement informé les personnes concernées que leurs Données de santé à caractère personnel seront hébergées sur support numérique.

5.4. Exercice de droits par une personne concernée

Dans le cas où une personne concernée exerce l'un de ses droits en vertu de la Réglementation applicable (accès, rectification, limitation, opposition, effacement et/ou portabilité), le Responsable de traitement doit répondre, en son nom et pour son compte, et dans les délais prévus par la Réglementation applicable. Lorsque la demande porte sur des Données à caractère personnel faisant l'objet de la sous-traitance prévue par le présent Accord, le Sous-traitant doit aider, dans la mesure du possible, le Responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées, notamment en informant le Responsable de traitement dans les meilleurs délais lorsque la personne concernée a exercé son droit auprès du Sous-traitant.

Dans le cas spécifique de la présence de Données de santé dont la durée de vie n'excède pas cinq (5) ans (cette information doit être connue du Sous-traitant) et uniquement dans le cas où les personnes concernées exercent leur droit d'accès et souhaitent obtenir communication de leurs informations (médicales), 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 de la Réglementation applicable.

5.5. Violation de Données à caractère personnel

Le Sous-traitant notifie au Responsable de traitement, dans les meilleurs délais et au plus tard dans les quarante-huit (48) heures sur les Jours Ouvrés, toute violation de Données à caractère personnel dont il a connaissance. 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 qu'il transmet 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.

La notification est réalisée par téléphone ou par e-mail, au point de contact désigné conformément à l'article 8 POINTS DE CONTACT du présent Accord. 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.

Il est rappelé qu'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.

5.6. Aide du Sous-traitant dans le cadre du respect par le Responsable de traitement de ses obligations

Sur le Périmètre qui lui est confié, le Sous-traitant aide le Responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des Données.

Le Sous-traitant aide le Responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

Le Sous-traitant garantit l'information (et son assistance) au Responsable de traitement concernant des opérations de contrôle et des mesures de l'autorité de contrôle, dès lors qu'elles se réfèrent aux Prestations confiées. 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. Dans ce cadre, le Sous-traitant en informe immédiatement le Responsable de traitement, sauf à ce qu'une telle notification soit interdite.

Article 6. Sous-traitance

Le Sous-traitant peut faire appel à un autre sous-traitant (ci-après, le ***« Sous-traitant Ultérieur »***) pour mener des activités de traitement spécifiques. Dans ce cas, et conformément à l'article 28.4 RGPD, 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 Sous-traitant 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, pour tout ou partie des Prestations, faire appel :
- A ses Affiliés ;
- Aux Sous-traitants Ultérieurs mentionnés dans le tableau des garanties mis en ligne sur le site Internet du Prestataire ;
- A tout Sous-traitant Ultérieur mentionné sur un document validé entre les Parties.

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 afin que le traitement réponde aux exigences de la Réglementation applicable. L'Hébergeur, lorsqu'il a recours à des prestataires externes assure un niveau de protection équivalent de garantie au regard des obligations pesant sur l'Hébergeur. 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. 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 décrit spécifiquement les mesures qui sont mises en œuvre dans le cadre des Prestations au sein de l'**Annexe 2A** du Contrat. Celles-ci sont définies de façon à lui permettre de mettre en œuvre les :
- 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. A ce titre, le Sous-traitant est autorisé à mettre en œuvre des mesures alternatives, à la condition que ces mesures continuent à assurer un niveau de sécurité équivalent à celui assuré par la mesure initiale.

Le Sous-traitant s'engage à fournir au Responsable de traitement, à sa demande, toutes 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 8. 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 par le Contrat, ou éventuellement, selon les modalités convenues entre les Parties à :
Renvoyer toutes les Données à caractère personnel au Responsable de traitement ; ou
Détruire toutes les Données à caractère personnel.

Article 9. Points de contact

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. En l'absence d'une telle communication, le Sous-traitant contactera les points de contact désignés par le Client dans le cadre des Prestations.

Article 10. Registre de traitement

Chaque Partie déclare tenir par écrit un registre de traitement conforme à la Réglementation applicable. Le Sous-traitant y répertorie les catégories d'activités de traitement effectuées pour le compte du Responsable de traitement.

Article 11. 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 Ultérieur est « importateur de Données à caractère personnel ». C'est le cas notamment lors du recours à certains Sous-traitants Ultérieurs (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.

En tout état de cause, le Sous-traitant s'engage à mettre à disposition du Responsable de traitement les informations portant sur les possibilités d'accès à des Données de santé par le biais de réglementations extraterritoriales applicables à l'Hébergeur ou à ses sous-traitants.

Article 12. Audit

Le Responsable de traitement (ou l'auditeur mandaté par lui ne concurrençant pas les activités du Sous-traitant) peut procéder à toute vérification qui lui paraîtrait utile pour s'assurer du respect des obligations du Sous-traitant fixées au 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-traitant Ultérieurs (par exemple : interdiction de réaliser un audit physique) et dans la limite d'un (1) audit par an. A cette fin, le Sous-traitant met à sa disposition la documentation nécessaire aux vérifications menées pour démontrer le respect de ses obligations, permet la réalisation d'audits, y compris des inspections, par le Responsable de traitement et y contribue. Les informations du Sous-traitant seront considérées comme des Informations confidentielles.

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 Responsable de traitement prend à sa charge tous les frais occasionnés par l'audit et rembourse au Sous-traitant ou au Sous-traitant Ultérieur 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 Ultérieur ayant collaboré à l'audit. 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 Ultérieur concerné, ni leur causer une quelconque désorganisation au-delà de la mise à disposition par le Sous-traitant ou du Sous-traitant Ultérieur 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 à la Réglementation applicable seraient constatés durant l'audit, les Parties s'engagent à échanger et collaborer de bonne foi pour la mise en œuvre des mesures nécessaires.

FICHE OPERATIONNELLE RELATIVE AU TRAITEMENT

Eu égard à l'article 2 « DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DE LA SOUS-TRAITANCE » de l'Accord, 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. Les opérations réalisées sur les Données à caractère personnel sont fonction des Prestations souscrites par le Client et décrites au Contrat. Dans ce cadre, les opérations réalisées peuvent être 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. 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) : il peut s'agir de solutions logicielles et prestations associées et/ou de 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. Conformément aux dispositions du 11° de l'article R. 1111-11 du Code de la santé publique, il est rappelé que le Sous-traitant n'est pas autorisé à utiliser les Données de santé à caractère personnel à d'autres fins que l'exécution de l'activité d'hébergement des Données de santé à caractère personnel. 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 7 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).