OCI INFORMATIQUE & DIGITAL

CONDITIONS PARTICULIERES

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

Version en vigueur à compter du 18 mai 2026

Le présent document décrit les Conditions particulières applicables aux Prestations spécifiques d'hébergement 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.

Article 2. Définitions spécifiques

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

« **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 ;

« **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** ») 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

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.

Article 4. Périmètre des Prestations

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 A** des présentes Conditions particulières.

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* : o La mise à disposition d'un NAS avec capacité suffisante par le Client, qui sera réinitialisé par l'Hébergeur. o 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.

ANNEXE A
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 de mise en œuvre du PRI dépendent de l'infrastructure-source et sont définies par les Parties. Le Client tient compte des éléments suivants :

- 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 qui correspond à l'activation du PRI) et le temps de restauration des éléments contenus dans l'Hébergement de destination (dépendant d'éléments extérieurs au Prestataire, à savoir la volumétrie des Contenus et Données à reprendre).

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.