Conditions Particulières – Services Héberger

Version 03.2025

Article 1. OBJET

Les présentes Conditions Particulières ont pour objet de définir les conditions selon lesquelles Axantis (ci-après « le Prestataire ») fournit à son Client un ou des Services d'hébergement tels que décrits ci-dessous.

Article 2. DEFINITIONS

Les termes suivants assortis d'une lettre majuscule sont définis dans les Conditions Générales de Vente et de Services du Prestataire (ci-après « CGVS ») ou ont la signification qui leur est donnée ci-après :

« **Baie(s)** » désigne l'infrastructure permettant l'hébergement physique des équipements informatiques.

« **Code d'Accès** » désigne le couple constitué d'un nom d'utilisateur et d'un mot de passe pour se connecter à une interface d'administration des services.

« **DataCenter(s)** » désigne un site physique où sont rassemblées des installations informatiques chargées de stocker et distribuer des données sur un Intranet ou sur Internet.

« **Durée de Rétention** » désigne la durée de conservation de la sauvegarde des données en jours calendaires.

« **Firewall** » ou « **Pare-Feu** » désigne selon les prestations souscrites par le Client, un outil de protection du réseau qui surveille le trafic entrant et sortant, et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies.

« **IaaS** » ou « **Infrastructure As A Service** » désigne une infrastructure informatique (stockage, vCPU, mémoire RAM).

« **Machine(s) Virtuelle(s)** » ou « **Virtual Machine** » ou encore « **VM** » est environnement entièrement virtualisé qui fonctionne sur une machine physique. Elle exécute son propre système d'exploitation (OS) et bénéficie des mêmes équipement qu'une machine physique : CPU, mémoire RAM, disque dur et carte réseau. Plusieurs machines virtuelles avec des OS différents peuvent coexister sur le même serveur physique.

« **RAM** » ou « **Random Access Memory** » également appelée mémoire vive. Il s'agit d'un type de mémoire qui équipe tout ordinateur et permettant de stocker des informations provisoirement.

« **Service(s)** » désigne la ou les prestations fournies par le Prestataire et décrites à l'article 3.

« **Supervision** » consiste en la collecte de données (mesures, alarmes) d'un équipement, d'un serveur ou d'une application.

« **Traçabilité** » désigne la situation où l'on dispose de l'information nécessaire et suffisante pour connaitre les actions réalisées sur les données traitées par un système d'information, tout au long de leur cycle de vie.

« **vCPU** » ou « **Virtual Central Processing Unit** » désigne une quote-part de processeur physique alloué à une Machine Virtuelle. Chaque Machine Virtuelle doit disposer au minimum d'un vCPU.

Article 3. DESCRIPTION DES SERVICES

3.1 *Cloud Datacenter*

Le Service Cloud Datacenter permet au Prestataire, depuis une interface d'administration des services (ci-après « l'Interface ») de commander et piloter, pour le compte du Client, un ensemble de ressources telles qu'elles sont détaillées ci-après, au sein d'un DataCenter virtuel. Ce Service proposé en mode IaaS et permet au Prestataire de faire bénéficier le Client de Services composés de ressources modulables telles que :

- vCPU et mémoire RAM ;
- Stockage de données ;
- Prestation de sauvegarde telle que décrite à l'article 3.5 des présentes.
- Bande passante ;
- Souscription de licences.

3.2 *Cloud VM Avancé*

Le Service Cloud VM Avancé permet une gestion par le Prestataire, pour le compte du Client, de Machines Virtuelles grâce à une architecture reposant, si de telles options sont choisies, sur la redondance matérielle des serveurs, du backup et du stockage au sein d'un même site. Ce Service inclut également une redondance géographique optionnelle sur deux sites distincts tels que précisés à l'article 3.4. Le Prestataire gère le paramétrage de

configurations standardisées et préconisées de la Machine Virtuelle, avec la possibilité de modifier à tout moment selon les besoins du Client.

Les principales fonctionnalités disponibles incluent, **sans que cette liste soit exhaustive** :

- **Création de la VM pour le compte du Client** ;
- **Gestion de la VM pour le compte du Client :** sélection des ressources (vCPU, RAM, stockage…), arrêt, redémarrage de la VM.
- **Sauvegarde de la VM** : les conditions de sauvegarde sont précisées à 3.5 des présentes.
- **Snapshots :** création et restauration d'états spécifiques des VM, conservés pendant sept (7) jours et dans la limite autorisée de 2 snapshots.
- **Historique des actions** : suivi détaillé des opérations effectuées sur les VM.
- **Console de la VM** : contrôle direct de la VM via l'Interface.
- **Gestion des clés d'accès sécurisées aux VM (clés SSH)** ;
- **Firewall basic intégré** : les conditions dudit Firewall sont précisées à l'article 3.6.
- **Supervision de la VM pour le compte du client en suivant de manière graphique la consommation de ressources VCPU, RAM, Stockage, réseau de la VM concernée**

3.3 *Cloud VM Essentiel*

Le Service Cloud VM Essentiel permet au Prestataire de créer depuis l'Interface, pour le compte du Client, des Machines Virtuelles. Ces VMs sont hébergées dans un DataCenter unique de la société Ikoula (situé en France), **sans redondance matérielle ni redondance géographique**.

Les fonctionnalités disponibles se limitent exclusivement aux suivantes, à l'exclusion de toute autre :

- **Gestion de la VM pour le compte du Client** : sélection des ressources (vCPU, RAM, stockage…).
- **Snapshots :** Création et restauration d'états spécifiques des VM, conservés pendant sept (7) jours et dans la limite autorisée de 2 snapshots.
- **Historique des actions** : suivi détaillé des opérations effectuées sur les VM.
- **Firewall basic intégré** : les conditions dudit Firewall sont précisées à l'article 3.6.

3.4 *Sauvegarde*

La sauvegarde des données, lorsque cette fonctionnalité est disponible pour le Service, consiste pour le Prestataire à mettre à disposition du Client une prestation de sauvegarde des Services, permettant d'effectuer une copie des données contenues sur la ou les VM. Les plateformes de sauvegarde étant situées sur des DataCenters différents de ceux hébergeant les Machines Virtuelles, les données des serveurs sauvegardées sont donc stockées à minima sur deux sites distincts.

L'activation de la sauvegarde pour chaque Machine Virtuelle est optionnelle et nécessite que le Client en formule la demande auprès du Prestataire. La mise en œuvre et la gestion des sauvegardes sont assurées par le Prestataire, le Client demeurant responsable de définir les données à sauvegarder ainsi que les modalités de cette sauvegarde.

Les types de sauvegardes proposés par le Prestataire diffèrent selon les Services sélectionnés. Le Client s'engage à s'informer sur les conditions et modalités applicables afin de s'assurer que les sauvegardes demandées correspondent à ses besoins.

Les sauvegardes, lorsqu'elles seront activées, seront réalisées quotidiennement en dehors des heures ouvrées et avec une administration des moyens de sauvegarde (matériels et logiciels). Les Durées de Rétention disponibles sont de sept (7) jours et (trente-un) 31 jours glissants.

Une Rétention personnalisée peut être mise en œuvre à la demande du Client ayant souscrit au Service Cloud Datacenter, sous réserve de la réception et de l'acceptation d'un devis préalablement établi par le Prestataire.

La gestion des sauvegardes, y compris la sélection des Machines Virtuelles à sauvegarder et la sélection de la Durée de Rétention, est réalisée directement par le Prestataire depuis l'Interface, sur instruction du Client. La volumétrie de sauvegarde pour chacune des VM est affichée sur l'Interface et le portail Cloud Datacenter.

3.5 *Firewall*

Le Service Firewall consiste à fournir au Client une solution de sécurité centralisée dans le but d'appliquer une politique d'accès aux ressources réseau de l'entreprise du Client ou aux Machines Virtuelles de ce dernier le cas échéant, en définissant le type de communications autorisées ou interdites en interne ou vers Internet. Aucune déclaration ou garantie n'est faite que le Service Firewall éliminera tout type de menace ou d'accès non autorisé.

- **Dans le cadre du Service Cloud Datacenter**, il appartient au Client de choisir entre les deux (2) options suivantes :
  - L'option « firewall standard » ;
  - L'option « firewall avancé ».

Dans sa version « firewall standard », le Prestataire propose les fonctionnalités suivantes : Pare-feu à états (Firewall Stateful), translation d'adresses et de ports (NAT/PAT), Proxy, VPN IPSec et SSL.

Dans sa version « firewall avancé », le Prestataire enrichit son offre avec les fonctionnalités supplémentaires : IPS (Intrusion Prevention System), antivirus, contrôle des applications, filtrage web. Les différentes modalités et fonctionnalités desdits Firewalls sont détaillées dans la documentation relative au Service fournie par le Prestataire.

Ces offres de Firewall permettent au Client, sous réserve que ce dernier ait souscrit au Service d'infogérance, de déléguer au Prestataire la configuration et à l'administration de sa politique de sécurité. Il appartient donc au Client de définir, avec le Prestataire, les règles d'ouverture et de fermeture des flux entrants et sortants.

- **Dans le cadre du Service Cloud VM Avancé et Cloud VM Essentiel**, le "Firewall basic" est un Firewall logiciel préinstallé sur la VM et permettant la sélection d'un Pare-feu, des ports autorisés et des IP entrantes autorisées pour administrer le Service.

Dans l'hypothèse où le Client a souscrit au Service d'infogérance, le Prestataire assure l'administration et la maintenance du Firewall basic, et notamment sa configuration, sa gestion et la surveillance du Firewall.

3.6 *Supervision des infrastructures*

Le Prestataire assure une Supervision des infrastructures dont il assure la mise en place et l'administration afin de surveiller et de détecter les Incidents. Les systèmes tiers ou non gérés directement par le Prestataire ne sont pas couverts. La Supervision n'inclut pas les interventions correctives, résolution des Incidents sauf stipulation contraire notamment dans le cadre du Service d'infogérance précisé à l'article 3.8.1.

3.7 *Infogérance*

Le Service d'infogérance permet au Client de déléguer tout ou une partie de la gestion technique, de la Supervision et de la sécurité de ses infrastructures au Prestataire, selon les niveaux d'infogérance souscrits qui sont détaillées dans la documentation relative au Service fournie par le Prestataire.

Le Prestataire propose plusieurs niveaux de Service d'infogérance selon les besoins du Client, pour maintenir, administrer et superviser l'environnement des Services. Cela peut inclure la maintenance curative (gestion des alarmes, patchs de sécurité), évolutive (mise à jour de logiciels) et réglementaire (gestion des licences).

3.8.1. Supervision des serveurs

Le Service d'infogérance inclut la mise en place d'une Supervision des serveurs. Son objectif est de définir et contrôler des indicateurs permettant de s'assurer de la disponibilité maximale des ressources.

La Supervision des serveurs consiste à :

- Exercer une surveillance permanente de ces ressources : celle-ci s'appuie sur une surveillance « technique » des composants informatiques (serveurs, éléments actifs, …) basée sur une approche évènementielle (remontée d'alarme) consistant à réagir rapidement à l'apparition d'évènements ou d'alertes,

- Détecter de façon proactive les événements susceptibles d'altérer la bonne marche des applications ou les Incidents,
- Appliquer les actions correctives appropriées qui reposent sur l'application de procédures et consignes fiables et documentées avec pour objectif la restauration des services interrompus dans le respect des niveaux de services,
- Assurer une complète Traçabilité des interventions, notamment dans le but de capitaliser l'expérience acquise en vue de la retranscrire par une évolution des procédures et consignes.

3.8.2. Administration des serveurs

Le Service d'infogérance inclut l'administration des serveurs qui se concentre sur la configuration, la gestion et la maintenance des serveurs. Le serveur est entièrement administré par le Prestataire. Dans ce cadre, le Client n'a pas d'accès direct au serveur.

3.8.3. Mises à jour

Le Service d'infogérance inclut l'installation des mises à jour, **à la demande du Client**. Le Client est informé qu'en l'absence de demande, la sécurité et la stabilité des serveurs peuvent être compromises et le Prestataire ne pourra être tenu responsable des éventuels défauts de sécurité.

Si les mises à jour automatiques sont activées, le Client reconnaît qu'elles peuvent provoquer des redémarrages non planifiés, entraînant une indisponibilité des serveurs et des risques d'Incidents. Le Prestataire décline toute responsabilité pour les impacts liés à ces redémarrages ou incompatibilités logicielles. Le délai d'installation des mises à jour est en moyenne de soixante-douze (72) heures ouvrées.

Par ailleurs, dans le cadre de ces mises à jour, toute nouvelle installation d'un matériel informatique doit faire l'objet d'une demande préalable auprès du Prestataire, ce dernier se réservant le droit d'approuver ou non l'installation dudit matériel.

3.8.4. Gestion des changements

Le Service d'infogérance inclut un processus de gestion des changements. Ce dernier a pour objectif d'assurer une coordination centralisée dans la mise en œuvre de tout changement afin de minimiser les éventuelles perturbations et d'assurer la Traçabilité des opérations entreprises.

Les équipes du Prestataire qualifient le changement, lequel peut être :

- **Standard** : il amène une charge de travail faible ou modéré, il est bien maîtrisé, présente peu de risques, n'apporte pas de modification du système, sa validation et son autorisation sont rapides. La réalisation de ce changement est gratuite dans la limite du nombre d'interventions mensuelles précisé dans un devis.
- **Significatif** : la charge de travail et le risque sont significatifs puisque l'évaluation et la mise en œuvre nécessitent l'intervention d'un ingénieur et une organisation spécifique : livrables, tests et recette inclus. La réalisation de ce changement est une prestation payante, selon le catalogue de Services.
- **Majeur** : il nécessite la mise en œuvre d'un projet qui peut être important mobilisant des ingénieurs et un chef de projet. La réalisation de ce changement est une prestation payante, et fera l'objet d'un devis préalable.

Article 4. CONDITIONS PREALABLES A LA FOURNITURE DU SERVICE

4.1 *Cloud Datacenter, Cloud VM Avancé et Cloud VM Essentiel*

Il appartient au Client de choisir, sous sa seule responsabilité, le ou le(s) Service(s) d'hébergement virtuel correspondant à ses besoins. Le Client reconnaît avoir été suffisamment informé de la configuration minimale préconisée par le Prestataire et des modalités liées à l'utilisation desdits Services d'hébergement virtuel. Le Client fait son affaire de la mise en place des moyens informatiques et de télécommunications nécessaires à l'accès au(x) Service(s).

4.2 *Infogérance : prise d'empreinte*

Une prise d'empreinte peut être nécessaire dans certaines hypothèses. A l'issue de la prise d'empreinte débute une phase probatoire d'une durée de trois (3) mois calendaires (ci-après la « **Phase Probatoire**). La prise d'empreinte permet de prendre connaissance de la documentation d'exploitation, de la configuration des applications, des éventuelles spécificités de l'installation, du niveau de sécurité, des documents d'exploitation et du dossier d'architecture, etc… Le Client est expressément informé que durant la Phase Probatoire, le Service d'infogérance est facturé mais les SLA ne sont pas applicables. Si des écarts importants avec les bonnes pratiques sont identifiés, le Prestataire le notifiera au Client. Celui-ci devra procéder aux modifications nécessaires. Le Prestataire pourra également proposer de réaliser les modifications sur devis. En tout état de cause, l'absence des modifications correctrices entraine l'impossibilité de réaliser le Service, de même que l'absence de documentation afférente rend impossible la prise d'empreinte ce qui entraînera une impossibilité de réaliser le Service.

Article 5. CONDITIONS D'UTILISATION DES SERVICES

5.1 *Cloud Datacenter*

Le Firewall du Service Cloud Datacenter est activé par le Prestataire sur instruction du Client. Ce dernier doit notamment communiquer ses besoins s'agissant de la configuration de la politique de sécurité selon l'option retenue. Le Client veillera à informer le Prestataire de façon régulière sur ses besoins concernant lesdites règles de sécurité. La supervision du Firewall est assurée par le Prestataire.

5.2 *Cloud VM Avancé et Cloud VM Essentiel*

Les Services Cloud VM Avancé et Cloud VM Essentiel sont configurés par le Prestataire en fonction des besoins exprimés par le Client. Le Prestataire paramètre le Firewall basic selon les besoins exprimés par le Client pour que soit assuré le niveau de protection souhaité. Il relève de la responsabilité du Client de soumettre au Prestataire toute demande, d'ajout, par exemple, de règles supplémentaires. Les obligations et responsabilités du Client relatives au Firewall basic sont énoncées dans les articles 7 et 8 ci-dessous.

5.3 *Infogérance*

Le Service proposé par le Prestataire et décrit à l'article 3.8, met à disposition du Client différents niveaux d'infogérance. Quel que soit le niveau d'infogérance souscrit par le Client, ce dernier reste responsable des choix en matière de règles de sécurité, de politiques de sauvegarde ou des configurations spécifiques qu'il souhaite mettre en œuvre. Le Client doit fournir au Prestataire les informations nécessaires demandées par celle-ci, notamment en cas d'Incident ou de mises à jour.

Article 6. ENGAGEMENT DE NIVEAU DE SERVICE (« SLA »)

En cas de Notification de Défaillance, le Prestataire s'efforcera sur un (1) mois calendaire, de rendre le Service disponible au moins 99,85% du temps (ci-après désigné l' « **Objectif de Disponibilité du Service** »), pendant la période de couverture du Service du lundi au vendredi, de 8 heures à 18 heures (hors jours fériés et hors périodes de maintenance programmées).

La disponibilité du Service se mesure en pourcentage et est calculée mensuellement (mois calendaire) comme suit :

Disponibilité du Service en pourcent = [Nombre de minutes totales dans le mois – Temps d'indisponibilité en minute hors Evénements Excusables (tel que ce terme est défini ci-après) dans le mois]

/Nombre de minutes totales dans le mois

X 100

Le Client pourra, si un Objectif de Disponibilité du Service n'est pas atteint durant trente (30) jours calendaires, sur demande, bénéficier auprès du Prestataire d'un avoir égal à un pourcentage, décrit ci-dessus :

Objectif de Disponibilité du Service	**Montant de l'Avoir du montant mensuel facturé**
De 99,85 à 99,5%	5%
De 99,5 à 97%	10%
Moins de 97%	20%

Les pénalités libératoires mentionnées ci-dessus ne s'appliquent pas, et aucun avoir ne sera émis, pour la période au cours de laquelle le Service fait l'objet d'une Défaillance en raison d'un cas de force majeure ou de l'une des causes suivantes (ci-après individuellement désignées un « **Evénement Excusable** ») : (i) un équipement ou un service non fourni par le Prestataire (ii) les actes ou omissions du Client (iii) une maintenance planifiée (iv) un trafic du réseau qui excède la capacité du Service (v) les actes ou omissions de tout autre opérateur de télécommunication (vi) l'indisponibilité du Client, ou autre manquement de celui-ci, à coopérer raisonnablement avec le Prestataire afin de rétablir le Service.

L'émission par le Prestataire d'avoirs est soumise à la limite suivante : le montant d'avoirs pour le taux de disponibilité du Service émis sur toute période de trente (30) jours calendaires consécutifs sera plafonné à 20% des frais mensuels dus au titre du Service défaillant.

Les Objectifs de Disponibilité du Service ne s'appliquent pas et le Client ne pourra engager la responsabilité du Prestataire, pour quelque cause que ce soit, s'agissant d'éléments non fournis par le Prestataire.

Article 7. OBLIGATIONS DU CLIENT

En sus des dispositions énoncées dans les CGVS, le Client s'engage à :

- Utiliser les Services conformément aux lois et réglementations en vigueur et aux usages de l'internet ;
- S'abstenir de toute activité illégale, frauduleuse ou portant atteinte aux droits d'un tiers, notamment :
- Le stockage ou la diffusion de données violentes, obscènes ou incitant à la haine raciale ou religieuse ;
- Toute activité liée au phishing, d'emails non sollicités (SPAM) ou des attaques informatiques de quelque sorte que ce soit.
- Ne pas modifier tout élément ne relevant pas strictement de ses propres données ;
- Garantir que ses équipements utilisés sont conformes aux normes applicables (marquage CE, compatibilité électromagnétique) et qu'ils n'entrainent aucun risque pour les infrastructures du Prestataire ou pour des tiers.
- Ne pas réaliser ou faire réaliser toute action susceptible de porter atteinte à l'intégrité ou au bon fonctionnement de l'infrastructure du Prestataire (test d'intrusion, recherche de vulnérabilité, usurpation de droits d'accès, …) sans l'accord préalable écrit du Prestataire.

Le Client est responsable de la sauvegarde régulière des données, fichiers et programmes lorsqu'il n'a pas donné la charge au Prestataire ou lorsqu'il a choisi le Service Cloud VM Essentiel. Le Client s'obligera ainsi, pendant toute la durée du Contrat, à procéder à la sauvegarde régulière des données. En cas de perte ou de dommage des données, le Prestataire pourra réinstaller les données uniquement sur la base des sauvegardes fournies par le Client. Avant l'expiration du Contrat, le Client s'assurera que les données ont été sauvegardées intégralement, sauf si le Client a confié au Prestataire la réversibilité des données.

Il s'engage également à réaliser régulièrement les mises à jour nécessaires pour maintenir la sécurité et le bon fonctionnement des infrastructures, sauf si ces mises à jour relèvent explicitement des prestations assurées par le Prestataire.

Le Client s'engage à ne pas porter atteinte aux droits de tiers et à respecter les droits de propriété intellectuelle ; il est responsable de la bonne conformité des usages des licences et des logiciels.

Le Prestataire met à disposition du Client des solutions de sauvegarde, des Firewalls et des licences acquises auprès de différents fournisseurs. Le Client est responsable de la consultation de la documentation technique fournie par le Prestataire ou l'éditeur pour une utilisation correcte desdites solutions. Le Prestataire ne saurait être tenu responsable en cas d'utilisation non conforme ou de dysfonctionnements liés à l'absence de consultation de cette documentation.

De manière générale, le Client, quelle que soit l'option de Firewall sélectionnée, a une obligation de coopération avec le Prestataire et doit l'informer de tout changement dans l'infrastructure, le réseau concernés ainsi que l'évolution des besoins de sécurité. Le Client s'engage à signaler sans délai les Incidents ou problèmes de sécurité qu'il aurait lui-même détectés.

Dans le cadre du Firewall basic, le Prestataire gère, pour le compte et sur instruction du Client :

- La configuration initiale et la gestion continue des règles de sécurité ;
- Toute modification ou ajout d'équipement, lignes, programmes ou configurations sur les systèmes concernés demandés par le Client;
- La Supervision en continue des alertes générées par le Firewall et la réalisation de mises à jour régulières;
- La prise toutes les mesures adéquates pour limiter les risques liés aux accès non autorisés, cyberattaques;
- Les actions correctives sur le Firewall en cas d'Incident.

Dans le cadre du Firewall standard ou avancé, le Client doit :

- Informer le Prestataire de ses besoins spécifiques en matière de sécurité et de toutes les modifications qu'il souhaiterait que le Prestataire apporte aux infrastructures ;

En cas d'Incident, le Client doit suivre les recommandations émises par le Prestataire. Le Client s'engage à collaborer étroitement avec le Prestataire en lui communiquant toute information pertinente pouvant impacter la gestion ou la sécurité des infrastructures protégées par le Firewall.

Dans le cadre de l'infogérance, le Client s'engage à respecter les responsabilités définies pour chaque niveau d'infogérance souscrit. Dans le cadre d'une infogérance complète, le Client s'engage à suivre les instructions du Prestataire pour garantir la sécurité et le bon fonctionnement des infrastructures infogérées. Le Client s'engage à informer le Prestataire sans délai de tout changement ou Incident susceptible d'affecter les Services, notamment en matière de sécurité.

Article 8. RESPONSABILITE

Le Prestataire n'a aucun contrôle ni connaissance des données transmises, stockées ou utilisées par le Client ou les Utilisateurs dans le cadre des présents Services. Par voie de conséquence, en sus des exclusions et limitations de responsabilité prévues dans les CGVS, le Prestataire décline toute responsabilité dans les cas suivants :

- La transmission, le stockage ou l'utilisation de données prohibées, illicites, illégales, contraires aux bonnes mœurs ou à l'ordre public (telles que mais s'y limiter les données à caractère violent, obscène, incitatif à la haine, au crime, au suicide, au terrorisme ou enfreignant toute législation relative à la protection des mineurs) ;
- Toute utilisation des Services à des fins illicites, en violation de droits de tiers ou en violation de la réglementation en vigueur ;
- Intrusion ou piratage malgré les mesures de sécurité mises en place comme les anti-virus.

Le Prestataire pourra retirer tout contenu manifestement illicite transmis et/ou stocké via les Services sur réquisition de l'autorité judiciaire et/ou administrative. Une telle intervention ne saurait engager la responsabilité du Prestataire ou de ses fournisseurs vis-à-vis du Client ou de tiers.

Le Client reconnaît être l'unique responsable :

- Du respect de l'étendue des droits concédés et des conditions d'utilisation des Services ;
- De l'utilisation des Services conformément à leur destination ;
- De la sécurité du système d'information et la sauvegarde des données lorsqu'il n'a pas confié ces prestations au Prestataire ;

Article 9. SUSPENSION DES SERVICES

En sus des dispositions exposées dans les CGVS, le Prestataire se réserve le droit de suspendre immédiatement les Services en cas de non-respect des obligations légales ou contractuelles par le Client énoncées aux articles ci-dessus dans les présentes Conditions Particulières.

Article 10. REVERSIBILITE DES SERVICES

En cas de cessation des relations contractuelles, pour quelque cause que ce soit, le Prestataire fera ses meilleurs efforts pour continuer à fournir les Services concernés pendant un délai de trente (30) jours ouvrés maximum à compter de la réception de la lettre recommandée avec avis de réception indiquant la cessation desdites relations

contractuelles, étant précisé que la réversibilité des Services ne peut pas bénéficier au Client en cas de défaut de paiement de ce dernier.

Le Client disposera donc d'un délai de trente (30) jours ouvrés pour effectuer à distance la copie du contenu hébergé et plus généralement de l'ensemble des données, se trouvant sur la Machine Virtuelle, dont il souhaite conserver ledit contenu. Passé ce délai, le Prestataire pourra librement disposer de la Machine Virtuelle et effacera l'intégralité des données s'y trouvant, sans que le Client puisse lui en faire grief ni invoquer quelque préjudice que ce soit.

Le Prestataire indique au Client qu'ils pourront définir les conditions et modalités pratiques de la réversibilité dans un plan de réversibilité élaboré par le Prestataire et validé par le Client. Les prestations d'assistance feront l'objet d'un devis en fonction du périmètre de réversibilité confié par le Client au Prestataire.

Signature