ANNEXE

Convention de services – Hébergement SecNumCloud

Destinataires :	**Ci-après "Commanditaire" ou "Client"**
Référence du document :	Annexe_Convention de Services Hébergement SecNumCloud_Contrat d'Hébergement SNC

Version du document template	V2
Date de validation du document Template	17 avril 2026
Classification	Diffusion Limitée
Validé par	Lorena ALCALDE GONZALEZ
Durée de validité du document	2 ans
Responsable du document	Emeline CAZAUX

Suivi des modifications du document

Version	Date	Action	Auteur
1	05 .09.2025	Rédaction initiale	Emeline CAZAUX
2	17.04.2026	Enrichissement SNC	Emeline CAZAUX

TABLE DES MATIERES

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

1 Préliminaire, Glossaire et Acronymes

1.1 Préliminaire

Le présent document formalise la Convention de service associée aux divers Services qualifiés SecNumCloud.

Les Services sont qualifiés SecNumCloud, HDS et C5 (cf attestations en Annexe).

La présente Convention de service complète et est complémentaire aux Conditions Générales de Vente et d'Utilisation du Prestataire ou du Contrat. Il est entendu que les documents contractuels s'interprètent de manière cohérente entre eux. En cas de contradiction ou de divergence entre les termes des documents contractuels, les Parties ont convenu de se référer à l'article 2 « Documents contractuels » du Contrat. [OU] les documents prévaudront les uns sur les autres dans l'ordre suivant :

1. Conditions Générales de Vente et Utilisation (CGVU) ou Contrat
2. Convention de Services – Hébergement SecNumCloud
3. Plan d'Assurance Sécurité (PAS)
4. Data Protection Agreement

1.2 Glossaire

Dans la présente Convention de service, le **Commanditaire**, le **Prestataire** ou les **Parties** sont identifiés dans le Contrat auquel est annexe la présente Convention de service.

Les expressions ci-après employées dans la présente Convention de service seront interprétées conformément aux définitions qui leur sont attribuées ci-dessous :

Changement : demande d'ajout, modification ou suppression d'un service ou d'un composant avec les caractéristiques suivantes:

- L'impact et les risques liés au changement sont à évaluer par les parties ;
- Les modalités de mise en production et de validation du changement sont à définir ;
- La mise en production est à planifier à l'avance ;
- Les modalités de retour arrière sont à prévoir ;
- Il y a un impact financier potentiel pour le CLIENT ou pour le PRESTATAIRE (devis complémentaire ou autre) ;
- Une mise à jour de la CMDB est nécessaire suite à la mise en production du changement (mise à jour des informations des éléments de configuration concernés, etc.).

On distingue la gestion du changement de sa réalisation : la gestion du changement correspond au qui, quoi, quand, où, comment et à quel prix. La réalisation du changement est associée à la notion de mise en production (c'est-à-dire la mise en œuvre des actions définies dans la gestion du changement).

Changement standard : Changement faisant l'objet d'une procédure, dont les modalités de mise en production et les impacts (y compris financiers) sont connus et acceptés à l'avance. Il est alors intégré au catalogue des changements standards, et peut selon les cas avoir une GTI et une GTR.

Exemples de changement standard : mise à jour mineure d'une application en pré-production selon un mode opératoire connu et rôdé ; mise à disposition d'une machine virtuelle selon un modèle prédéfini pour un serveur de développement.

Contrat : désigne le contrat souscrit par le Commanditaire auprès du Prestataire pour permettre au Commanditaire de bénéficier du Service auquel la présente Convention de service est annexée.

Convention de service : désigne le document décrivant, notamment, de manière technique et fonctionnelle les Services fournis par le PRESTATAIRE ; ainsi que la liste détaillée des Niveaux de Services, leur méthode de calcul et la périodicité de leur production. La Convention de Services est une Annexe du Contrat.

Demande de service : demande d'évolution faisant l'objet d'une procédure, dont la réalisation :

i) Ne modifie pas la Configuration Management Database (Base de données de gestion des configurations) ;

ii) Le mode opératoire, les coûts et les risques sont connus et acceptés à l'avance et ne nécessitent pas de modalités de retour arrière spécifiques ;

iii) La réalisation est soumise à un accord de niveau de service et incluse dans la redevance du Contrat lorsqu'elle est réalisée en heures ouvrées et jours ouvrés.

Disponibilité : Capacité à assurer la disponibilité et le maintien des performances optimales du Service, en accord avec les critères et engagements définis dans les Accords de Niveau de Service (SLA).

Données techniques : comprend l'ensemble des données manipulées pour délivrer le Service, notablement dont l'identité des bénéficiaires et des administrateurs de l'infrastructure technique, des journaux de l'infrastructure technique, configuration des accès, annuaire, certificats...

Elément de configuration : actif, composant ou autre élément qui est ou sera sous le contrôle de la gestion des configurations. Les éléments de configuration et leurs attributs peuvent varier en complexité pour finalement décrire l'ensemble d'un service, d'un système incluant le matériel, les applications, la documentation, les contrats, les processus ou les organisations jusqu'à un niveau de détail pouvant être riche (composant de matériel, module logiciel, etc.). Les éléments de configurations devraient être définis selon des critères, groupés, classés et identifiés de façon à pouvoir être gérés et tracés tout au long de leur cycle de vie.

Evénement : toute occurrence détectable ou identifiable ayant une signification en ce qui concerne la gestion des infrastructures ou la fourniture d'un service et l'évaluation de l'impact de l'écart qu'elle pourrait causer.

Hyperviseur : Système d'exploitation permettant l'exécution de machines virtuelles sur une lame de calcul.

Incident : désigne tout événement ne faisant pas partie du fonctionnement standard d'un Equipement, et qui cause, ou peut causer, un non-respect d'un ou plusieurs Niveaux de Services, une perturbation ou une interruption d'un Service, et/ou un dommage au CLIENT.

Incident de sécurité : Tout événement dans le périmètre du Service :
- De nature intentionnellement malveillante ;

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

- De nature accidentelle portant atteinte à l'intégrité, la confidentialité ou la traçabilité du Service ou des données du Commanditaire ;
- Portant atteinte aux mesures de sécurité existantes.
- Les atteintes à la Disponibilité d'origine non-malveillante ne sont pas considérées comme un Incident de sécurité (panne matérielle, bug, dysfonctionnement, sinistre naturel...).

Interface Commanditaire : Interface d'administration du Service mise à disposition du Commanditaire par le Prestataire, regroupant une console d'administration web et une API.

Mise en production : action(s) d'administration de réalisation du Changement quand celui-ci est approuvé (le changement, au sens Information Technology Infrastructure Library (Bonnes Pratiques pour la Gestion des SI), ne concernant que la gestion du changement et non sa réalisation/concrétisation).

Problème : cause d'un ou plusieurs Incidents récurrents, cause d'un Incident potentiel (situation à risque) nécessitant une analyse et une résolution pour prévenir sa récurrence.

Région : désigne un ensemble géographiquement délimité de zones de disponibilité cloud, fournissant des services de réseau, de calcul et de stockage pour optimiser la latence, la performance et la conformité réglementaire locale.

Service : Désigne le(s)s service(s)s commandés par le CLIENT dans le cadre du Contrat et soumis à la présente Convention de Services prise en application dudit Contrat.

Secure Temple : désigne le service IaaS qualifié SecNumCloud, proposé par la société Cloud Temple, tel que défini dans l'attestation consultable sur le site de l'ANSSI et fournie en annexe de la présente Convention de service.

Sinistre : désigne un événement grave d'origine naturelle ou humaine, accidentelle ou intentionnelle, occasionnant des pertes et des dommages importants à la Partie sinistrée.

Supervision : Surveillance d'un Système d'Information ou d'un Service, impliquant la collecte de diverses données telles que mesures et alarmes. Cette activité se limite à l'observation et au suivi, sans intervenir directement sur les éléments surveillés, une prérogative qui appartient aux opérations d'Administration.

Tenant : Une instance isolée réservée à un utilisateur ou groupe d'utilisateurs, partageant une infrastructure commune tout en maintenant l'indépendance et la sécurité des données et des applications.

Zone de Disponibilité (AZ) (Availibility zone) : Une section spécifique et isolée de l'infrastructure de cloud computing, conçue pour assurer la haute disponibilité et la résilience des services par une distribution géographique des ressources.

1.3 Acronymes

GTI Garantie de Temps d'Intervention
IaaS Infrastructure as a Service
OS Operating system (système d'exploitation)
OpenIaaS Open Infrastructure as a Service
PaaS Platform as a Service
PAS Plan d'Assurance Sécurité
PASSI Prestataire d'Audit de Sécurité des Systèmes d'Information
RGPD Règlement Général de Protection des Données (personnelles)
SLA Service Level Agreement -- Accord sur les niveaux de services
SNC SecNumCloud
SOC Security Operation Center
VM Virtual Machine (Machine virtuelle)

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

2 Objet de la présente Convention de service

La présente Convention de Service régit les modalités selon lesquelles le Prestataire s'engage à fournir au Commanditaire les services souscrits parmi les offres Infrastructure as a Service (IaaS), OpenIaaS, Bare Metal et Platform as a Service (PaaS), conformes aux spécifications SecNumCloud.

Son objet est de :

- Préciser les exigences de performance attendues par le Commanditaire en termes de fonctionnalité et de fiabilité du Service et de l'infrastructure ;
- Énoncer les obligations du Prestataire afin de satisfaire aux niveaux de service convenus ;
- Identifier les normes réglementaires applicables spécifiquement au Service délivré ;
- Assurer une uniformité et une intégrité dans l'évaluation de la qualité du Service ;
- Garantir l'excellence des services fournis, évaluée au moyen d'indicateurs de performance quantitatifs.

Il est stipulé que, dans l'hypothèse où le Prestataire se verrait retirer sa qualification SecNumCloud, le Contrat pourra être résilié de plein droit, sans encourir de pénalités, par le Commanditaire. Dans une telle éventualité, le Prestataire s'engage à informer le Commanditaire de cette déqualification par envoi d'une notification officielle, au moyen d'une lettre recommandée avec demande d'avis de réception.

Il convient de noter qu'une modification ou un ajustement de la qualification SecNumCloud ne sera pas interprété comme une révocation de la qualification initiale.

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

3 Description du Service et des Infrastructures

3.1 Infrastructures Datacenters

Cette clause ne vaut que si le Commanditaire souscrit à un service IaaS, OpenIaaS ou Bare Metal.

Le Service englobe la mise à disposition, pour chaque Zone de disponibilité, des prestations ci-après :

- Site datacenter situé en France pour la Région FR, conforme aux dernières normes technologiques, avec proposant un niveau de résilience équivalent ou supérieur au niveau Tier 3 du Uptime Institute ;
- Mise à disposition de salles techniques au sein de datacenters dédiés à l'accueil des équipements techniques indispensables à la production du service, incluant calcul, stockage, réseau, câblage, et autres composants nécessaires ;
- Alimentation électrique sécurisée, assurée par deux circuits électriques distincts, garantissant une continuité de service ;
- Fourniture de services de climatisation, ajustés pour respecter les normes et préconisations des fabricants d'équipements, afin de maintenir un environnement optimal pour les dispositifs techniques ;
- Supervision continue et métrologie détaillée, permettant un suivi précis et une gestion proactive des performances et de la sécurité du service fourni.

Le Prestataire assure la mise à disposition de services avancés de détection et d'extinction d'incendie, conçus pour identifier et neutraliser efficacement tout départ de feu au sein des installations. Ces systèmes sont essentiels pour garantir la sécurité des équipements et des données. Ils comprennent des détecteurs de fumée de haute précision et des dispositifs d'extinction qui peuvent agir rapidement sans endommager l'équipement informatique. Ce service est crucial pour prévenir les risques d'incendie, minimiser les dommages potentiels et assurer la continuité des opérations.

Le Commanditaire est informé que toutes les procédures et mesures de sécurité mises en place, y compris les tests annuels de basculement sur les groupes électrogènes, sont essentielles pour garantir la continuité et l'intégrité des services fournis. Ces pratiques sont conçues pour minimiser les risques de panne et assurer une réactivité optimale en cas d'Incident. En acceptant ces conditions, le Commanditaire reconnaît l'importance de ces mesures et s'engage à coopérer pleinement pour faciliter leur mise en œuvre. Le Commanditaire est également encouragé à prendre connaissance des recommandations de sécurité fournies et à les intégrer dans sa propre stratégie de gestion des risques.

3.2 Infrastructure logicielle de pilotage du Service

Le Prestataire fournit au Commanditaire la console d'administration et l'API nécessaire à l'utilisation du Service. Il s'engage également à les maintenir en condition opérationnelle optimale et à en assurer la sécurité de manière continue. Cette console d'administration et l'API sont désignées de manière groupée sous le terme « interface Commanditaire ».

Dans le cadre du service PaaS :

Le Prestataire fournit au Commanditaire la console d'administration et l'API nécessaire à l'exploitation de ses environnements PaaS RedHat OpenShift. Il s'engage également à les maintenir en condition opérationnelle optimale et à assurer sa sécurité de manière continue.

Dans le cadre spécifique du service fourni, le Prestataire met à la disposition du Commanditaire toutes les interfaces et API de la plateforme RedHat OpenShift au sein du tenant sélectionné. Il revient au Commanditaire d'instaurer les dispositifs de sécurité appropriés, tels que les pare-feux (firewall), les pare-feux applicatifs Web (WAF), et autres mesures de protection, ainsi que de définir les règles de filtrage associées pour sécuriser l'accès à sa plateforme conformément à sa politique de sécurité.
Dans le cadre de l'ensemble des services :

Le Prestataire alerte le Commanditaire sur le fait qu'une utilisation anormale de l'interface Commanditaire, notamment en cas de surcharge de ses APIs de commande (hammering), peut déclencher des mesures de sécurité automatiques entraînant le blocage de l'accès aux APIs de commande ou au Service. Il convient de souligner que cette situation ne constitue pas une indisponibilité du Service mais une action de protection du Service et de l'infrastructure du Prestataire ; par conséquent, le Commanditaire ne peut la considérer comme une indisponibilité dans ses calculs.

De plus, le Prestataire précise au Commanditaire que les requêtes parfaitement identiques (doublons) envoyées à ses APIs sont limitées à une par seconde (Throttling). Si le Commanditaire soumet des requêtes identiques à une fréquence supérieure, leur rejet ne pourra être interprété comme une indisponibilité du Service.

3.3 Infrastructures de calcul

Cette clause ne vaut que si le Commanditaire souscrit à un Service IaaS, OpenIaaS ou Bare Metal.

Le Service inclut la fourniture, dans les zones de disponibilité souscrites par le Commanditaire, des équipements nécessaires à l'exécution des charges de travail sous forme de machines virtuelles.
Ceci comprend :

- La fourniture des châssis techniques nécessaires au bon fonctionnement des lames de calcul ;
- La fourniture des lames de calcul dans les quantités spécifiées par le Commanditaire et réparties selon les zones de disponibilité de son choix. Il est à noter que ces lames de calcul sont exclusivement dédiées au Commanditaire.

Le choix du modèle de lame de calcul, sélectionné parmi le catalogue proposé par le Prestataire, relève de la responsabilité du Commanditaire.

3.3.1 Services IaaS et OpenIaaS

Les services IaaS et OpenIaaS incluent :

- La mise à disposition de systèmes d'exploitation de type hyperviseurs, ainsi que la garantie du maintien en condition opérationnelle et de sécurité de l'infrastructure logicielle nécessaire au pilotage de ces systèmes d'exploitation.

Il convient de mettre en évidence que, même si le Prestataire est responsable de la maintenance opérationnelle et de la sécurisation globale du Service, il ne détient pas de connaissances spécifiques concernant les environnements de production du Commanditaire ni des exigences liées à ses charges de travail. Par conséquent, la responsabilité de décider de la mise à jour des systèmes d'exploitation des lames de calcul hyperviseurs, une action susceptible de nécessiter un redémarrage, repose entièrement sur le Commanditaire. Cette opération peut être réalisée via l'Interface Commanditaire.

3.3.2 Bare Metal

Le Service Bare Metal inclut:

- La mise à disposition d'une console type KVM pour piloter la gestion de la ressource de calcul.

3.3.3 Infrastructure de Stockage

Le service IaaS, OpenIaaS et Bare metal comprend la fourniture au Commanditaire d'une infrastructure de stockage partagée de type SAN (Storage Area Network), offrant divers niveaux de performance. Ce service englobe :

- L'implémentation et le maintien en condition opérationnelle et en condition de sécurité du réseau SAN dédié ;
- L'installation et la gestion des baies de stockage mutualisées entre les clients, y compris leur maintien en condition opérationnelle et en condition de sécurité, leur supervision et leur métrologie ;
- La mise en place des systèmes automatisés pour l'allocation des LUNs (Logical Unit Numbers) de stockage dédié à l'usage du Commanditaire, conformément aux volumes souscrits par le Commanditaire.

3.3.4 Infrastructure réseau globale

Cette Clause ne vaut que si le Commanditaire souscrit à un Service IaaS, OpenIaaS ou Bare Metal.

Le Prestataire déploie dans le cadre du Service, un réseau global facilitant au Commanditaire la mise en accessibilité de ses systèmes hébergés. Ce service comprend :

- La fourniture, le maintien en condition opérationnelle et en condition de sécurité de l'ensemble des liaisons en fibres optiques interconnectant les différentes Zones de disponibilité ;
- La fourniture, le maintien en condition opérationnelle et en condition de sécurité des équipements techniques nécessaires au bon fonctionnement du réseau et à l'isolation des différents clients.

L'interconnexion réseau du Tenant Commanditaire, à Internet ou à des réseaux privés, les équipements réseaux, liens opérateurs et autres composants techniques réalisant cette interconnexion, ne font pas partie du périmètre du Service. Cette interconnexion réseau est mise en œuvre conformément aux dispositions prévues dans le Contrat.

3.3.5 Infrastructure de sauvegarde

Le Prestataire met à disposition du Commanditaire un service ou une plateforme de sauvegarde intégré, dédié et géré, destiné à la protection de ses machines virtuelles ou des données de ses environnements RedHat Openshift (dans le cadre du Service PaaS).

Le Prestataire assure le maintien en condition opérationnelle et en condition de sécurité de ce service de sauvegarde. Le Prestataire garantit que les sauvegardes du Commanditaire seront situées en dehors de la Zone de disponibilité des charges de travail sauvegardées, sous réserve que le Commanditaire ait souscrit au Unités d'œuvre adéquates.

Cette prestation de sauvegarde se limite à la sauvegarde des machines virtuelles et des configurations de topologie de l'environnement IaaS ou OpenIaaS des Tenants du Commanditaire dans le cadre du Service. L'élaboration et l'application d'une politique de sauvegarde adéquate par le Commanditaire dépendent de la souscription à des unités d'œuvre spécifiques. Il incombe donc au Commanditaire de s'assurer de la disponibilité des ressources techniques nécessaires auprès du Prestataire pour mettre en œuvre sa politique de sauvegarde ou d'ajuster cette dernière en fonction des moyens disponibles.

Le Prestataire s'engage à notifier le Commanditaire en cas de contraintes de capacité et à fournir une assistance conseil pour l'optimisation des ressources. Les obligations du Prestataire se limiteront à la mise en œuvre des besoins exprimés par le Commanditaire en matière de politique de sauvegarde, dans le cadre des ressources souscrites.

3.3.6 Mise en œuvre de solutions de reprise d'activité ou de continuité d'activité

Le Prestataire fournit au Commanditaire l'ensemble des solutions techniques nécessaires pour garantir une répartition optimale de ses ressources à travers diverses Zones de disponibilité. Il incombe au Commanditaire la responsabilité de gérer efficacement cette distribution de ressources, pour laquelle il a la possibilité à exploiter les outils du Prestataire disponibles à cet usage.

Dans le cadre du service PaaS :

En particulier, les applications déployées sur la plateforme RedHat OpenShift doivent prendre en charge les mécanismes de redondance proposés par le Prestataire afin de pouvoir bénéficier des solutions de reprise d'activité ou de continuité d'activité associées.

3.4 Modèle de responsabilité partagée

Le Service proposé par le Prestataire se caractérise par la mise à disposition des prestations suivantes, lesquelles s'alignent sur le principe de responsabilité partagée présenté dans le référentiel SecNumCloud :

- Produits IaaS et OpenIaaS : Matrice de responsabilité IaaS | Documentation Cloud Temple
- Bare metal :
- PaaS Openshift SecNumCloud: Matrice de responsabilité PaaS - OpenShift SecNumCloud | Documentation Cloud Temple
- PaaS Openshift standard : Matrice de responsabilité - OpenShift Standard | Documentation Cloud Temple
- Stockage S3 : Matrice de responsabilité IaaS - Stockage Objet S3 | Documentation Cloud Temple
- VM Instances : Modèle de responsabilité partagée — VM instances | Documentation Cloud Temple
- VPC : Modèle de responsabilité partagée — VPC | Documentation Cloud Temple

Il est entendu que le Prestataire mobilisera son expertise pour réaliser les Prestations selon les meilleures pratiques professionnelles et conformément aux exigences du référentiel SecNumCloud.

3.5 Présentation détaillée du périmètre des Services

Les périmètres de service détaillés dans les articles suivants de la présente convention ne sont applicables et ne présentent d'intérêt que dans la mesure où le Commanditaire a effectivement souscrit au service auquel se rapporte chacun de ces périmètres.

3.5.1 Service PaaS

L'offre de services proposée par le Prestataire se caractérise par la mise à disposition des prestations suivantes, lesquelles s'alignent sur le principe de responsabilité partagée détaillé dans les normes établies par le référentiel SecNumCloud :

- La provision d'une plateforme de gestion des conteneurs Redhat Openshift pilotée par le Prestataire.
- La mise à disposition de la plateforme au sein d'une région sur 3 zones de disponibilité.

Il est entendu que le Prestataire mobilisera son expertise pour réaliser les Prestations selon les meilleures pratiques professionnelles, conformément à leurs Spécifications et en respectant les normes de sa certification ISO/IEC 27001 ainsi que les directives du Référentiel SecNumCloud.

3.5.1.1 Mise en œuvre du service

Il est précisé que toutes les opérations et tous les composants physiques impliqués dans la fourniture du service qualifié, dont la présente convention fait l'objet, sont situés dans l'Union Européenne. Cela inclut notamment le support, la supervision opérationnelle et la supervision de sécurité (SOC).

3.5.1.2 Description des composants techniques

Les services PaaS (Platform as a Service) englobent l'intégralité des composants et services requis pour son fonctionnement optimal dans le respect de la qualification SecNumCloud.

À cet égard, leur performance et fiabilité sont intrinsèquement liées aux composants techniques et aux services de **l'infrastructure IaaS** du Prestataire.

3.5.2 Service IaaS et OpenIaaS

Le Service englobe l'ensemble des ressources de calcul, de stockage des données de production, de stockage objet S3, de sauvegarde si le Commanditaire à souscrit au mass storage adéquat, d'infrastructure réseau ainsi que la console Shiva permettant au Commanditaire l'accès et l'administration de son service IaaS ou OpenIaaS. L'accompagnement technique se limite strictement à ces prestations, dans le cadre du périmètre de service qualifié SNC et conformément aux responsabilités contractuelles du Prestataire.

3.5.3 Service Bare Metal

Le Service englobe l'ensemble des ressources de calcul, de stockage des données de production, d'infrastructure réseau ainsi que la console Commanditaire permettant l'accès et l'administration du service Bare Metal. L'accompagnement technique se limite strictement à ces prestations, dans le cadre du périmètre de service qualifié SNC et conformément aux responsabilités contractuelles du Prestataire.

3.5.4 Virtual Private Cloud (VPC)

Le Service VPC permet la création et l'administration, via la console de gestion, de réseaux privés isolés, sécurisés et souverains, interconnectables avec les environnements OpenIaaS, IaaS VMware, Bare Metal et PaaS OpenShift. Il comprend la segmentation des réseaux régionaux, la gestion des flux (nord-sud et est-ouest), ainsi que les fonctionnalités de routage natif, d'IP flottantes et d'adressage dynamique (DHCP/IPAM). Le Service est délivré soit en mode mutualisé pour les instances virtuelles, soit en mode dédié pour une isolation physique maximale, offrant au Client la pleine maîtrise de la configuration de son infrastructure réseau. L'accompagnement technique se limite strictement à ces prestations, dans le cadre du périmètre de service qualifié SNC et conformément aux responsabilités contractuelles du Prestataire.

3.5.5 Virtual Machine Instance

Le Service VM Instances permet le provisionnement et la gestion de machines virtuelles reposant sur l'infrastructure OpenIaaS qualifiée SecNumCloud et mutualisée du Prestataire, exploitant la technologie XCP-NG. Il repose sur une architecture à deux API découplées assurant une séparation stricte entre les plans de gestion (Management) et les environnements clients (Tenants). L'accompagnement technique se limite strictement à ces prestations, dans le cadre du périmètre de service qualifié SNC et conformément aux responsabilités contractuelles du Prestataire.

3.6 Limitations des services dans les modèles IaaS, OpenIaaS et Bare Metal

3.6.1 Services managés en RUN

Il est important de noter que sont écartés du Service :

- L'hébergement de composants physiques du Commanditaire ;
- L'interconnexion réseau du Tenant Commanditaire, à Internet ou à des réseaux privés, incluant les liens opérateur ;
- Tout service de type managé, ou Tiers Maintenance d'Application ;
- Toute assistance sur les machines virtuelles au niveau OS ou sur les système d'exploitation installés et au-dessus dans les matrices de responsabilités même s'il s'agit de simple supervision.

Cela étant, il n'est absolument pas exclu que le Commanditaire ait recours à de tels services auprès de l'offre Managed Services Provider du Prestataire pour intervenir en mode services managés sur ses Tenants. Ces services ne seront alors pas encadrés par la présente Convention de service et ses engagements/clauses bipartites.

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

3.6.2 Configuration du secours

Cette clause ne vaut que si le Commanditaire souscrit à un Service Iaas, OpenIaaS ou Bare Metal

Par défaut, le Prestataire fournit la mise en place des ressources IaaS ou Bare Metal au Commanditaire en réservant des ressources et en configurant les déploiements pour utiliser les Zones de disponibilité. Il incombe au Commanditaire de choisir les Zones de disponibilité via l'interface Commanditaire.

3.6.3 Configuration de la sauvegarde

Cette clause ne vaut que pour le service IaaS et OpenIaaS.

La prestation de sauvegarde s'arrête à la sauvegarde des machines virtuelles et des configurations de topologie représentant l'environnement OpenIaaS des Tenants du Commanditaire dans le cadre du Service.

La prestation de sauvegarde et la complétion de la politique de sauvegarde du Commanditaire est soumise à la souscription d'espace de stockage sur le mass storage (IaaS) ou stockage Objet S3 (OpenIaaS) nécessaire pour assurer le service. Il est donc de la responsabilité du Commanditaire de souscrire auprès du Prestataire les moyens techniques nécessaires pour assurer la politique de sauvegarde sur son périmètre informatique, ou d'ajuster la politique de sauvegarde aux moyens mis en œuvre. Le Prestataire s'engage à informer le Commanditaire en cas de limite de capacité technique.

Le Prestataire mettra en place les moyens techniques et humains nécessaires à la sauvegarde du système hébergé dans la limite des ressources souscrites par le Commanditaire.
Par ailleurs, dans le cas des périmètres non pris en charge par le Prestataire, il appartient au Commanditaire de définir sa propre stratégie de sauvegarde et de paramétrer lui-même les sauvegardes des VM ou d'effectuer une Demande de service auprès du Prestataire pour que le paramétrage des sauvegardes pour les serveurs physiques soit mis en place si le Commanditaire dispose d'un contrat de service managé permettant au Prestataire d'agir via l'interface Commanditaire qui est la console d'administration qui est mise à disposition dans le cadre de cette Convention de service et qui dispose de fonctionnalités pour configurer les sauvegardes.
En outre, ce service n'aura comme engagement que de traduire par le paramétrage via l'interface Commanditaire, la configuration spécifiée clairement par le Commanditaire.

Pour des raisons de flexibilité de l'offre du Prestataire, le Commanditaire a l'option d'associer une politique de non-sauvegarde sur certaines de ses VM. Dans ce cas, il appartient au Commanditaire d'assumer ce choix. Le Prestataire ne sauvegardera pas les VM associées à la politique "no backup". Le Prestataire alerte le Commanditaire que choisir la politique "no backup" ou choisir de sauvegarder manuellement expose le Commanditaire à une perte de données définitive en cas d'Incident sur les couches basse ou sur les couches dépendant de sa responsabilité dans le modèle IaaS. Dans un tel cas, il sera impossible de tenir le Prestataire responsable de restaurer les données car il n'y aura rien à restaurer. Le Prestataire recommande de toujours sauvegarder les VM.

Pour tout sujet concernant l'OS installé sur une machine virtuelle et tout logiciel ou programme exécuté « par-dessus l'OS », il est de la responsabilité du Commanditaire de réaliser les opérations d'administration et de supervision au sein de l'Union Européenne s'il souhaite garantir que toute la verticalité des couches du SI soient opérées et gérées depuis l'Union Européenne. Les opérations d'administration hors du périmètre de responsabilité du Prestataire dans le cadre de la présente Convention de service sont indiquées dans la section « Modèle de responsabilités partagées » de la présente Conventions de Service.

La stratégie de sauvegarde déployée pour le Commanditaire, est conditionnée par la souscription aux unités d'œuvre adéquates.

Le Prestataire s'engage sur la mise à disposition d'une solution de sauvegarde qui permettra au Commanditaire d'appliquer les politiques de sauvegardes souhaitées.

Il est précisé que le périmètre du Prestataire s'arrête à la mise à disposition d'un service de sauvegarde et c'est au Commanditaire de superviser via l'interface Commanditaire la bonne exécution des politiques associées.

Il est précisé que la gestion de capacités de stockage de l'espace de stockage dédié aux sauvegardes, reste à la charge et responsabilité du Commanditaire. Le Prestataire met à disposition le taux d'utilisation via la console.

Exemple : Non sauvegarde d'une machine virtuelle :

Le Commanditaire a la charge de vérifier / superviser la bonne exécution des politiques des sauvegardes, dans le cas où le Commanditaire constate qu'une machine virtuelle n'est pas sauvegardée, il lui appartient d'en vérifier la cause, le Commanditaire pourra solliciter le Support du Prestaire selon le niveau de support souscrit pour être assisté.

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

3.7 Mise en œuvre du service

3.7.1 Prérequis techniques

Pour la mise en œuvre du Service, le Commanditaire reconnait qu'il devra :

- Déclarer des IP fixes depuis lesquelles le Prestataire l'autorisera à accéder à l'interface Commanditaire (Filtrage par liste blanche). Les modifications de cette liste d'IP devront être réalisées via le menu prévu à cet effet dans la console ou via des Demandes de service pour les modifications ultérieures. A l'initialisation du service, le Prestataire aura été informé à minima d'au moins 1 adresse IP telle que décrite.

3.7.1.1 Pour les modèles IaaS et OpenIaaS

Pour la mise en œuvre du Service, le Commanditaire reconnaît qu'il devra :

- Fonctionner avec une virtualisation de type VMware pour le modèle IaaS ou de type Xen pour le modèle OpenIaaS dans les versions supportées par l'éditeur et fournies par le Prestataire dans le cadre du Service;
- Recourir via le Prestataire à l'utilisation de l'outil de sauvegarde.

3.8 Localisation du service en France

Il est précisé qu'aucune des opérations et aucun des composants physiques impliqués dans la fourniture du Service, dont la présente Convention de service fait l'objet, n'est situé hors de l'Union Européenne.

Cela inclut notamment le support, la supervision opérationnelle et la supervision de sécurité (SOC) de l'infrastructure technique délivrant le Service. De fait, tout le stockage, toutes les tâches d'administration, de supervision et tous les traitements sont réalisés en France.

3.8.1 Localisation des Datacenters hébergeant le Service

A défaut des opérations des collaborateurs et des agences du Prestataire, l'ensemble des opérations de production (comprenant le stockage et le traitement des données) et composants techniques délivrant le Service sont situés dans les Datacenters basés en France.

3.8.2 Localisation des agences Cloud Temple opérant le service

Les collaborateurs de Cloud Temple intervenant sur le périmètre du Service opèrent depuis les agences de Cloud Temple toutes situées exclusivement en France. Ces agences sont situées en France, à Tours, Lyon, Caen et Paris La Défense.

Le Commanditaire est informé de la possibilité des salariés de Cloud Temple de travailler à distance. Toutefois, le Prestataire garantit le même niveau de sécurité concernant les accès à distance, notamment concernant les accès VPN. Ces accès distants sont mis en œuvre conformément aux exigences du référentiel SecNumCloud.

3.9 Support

Cet article ne vaut que si le Commanditaire à souscrit à un Service IaaS, OpenIaaS ou Bare Metal.

3.9.1 Nature du support accompagnant le service

Le Prestataire fournit un service de support technique visant à assister le Commanditaire dans la gestion, le dépannage et l'optimisation de leurs ressources déployées. Ce service couvre une gamme étendue d'activités, depuis l'aide à la configuration initiale des services jusqu'au soutien technique avancé pour résoudre des problèmes spécifiques.

Voici une description des caractéristiques et fonctionnalités du service de support :

- Assistance à la mise en œuvre initiale de l'utilisation du Service ;
- Assistance à la résolution d'incidents ;
- Assistance à la résolution de problèmes ;
- Suivi et conseil sur l'optimisation du socle technique.

Dans le cadre du service de support, le Prestataire ne se substitue pas au Commanditaire dans l'usage du Service. Le Commanditaire reste entièrement responsable de la configuration, de l'exploitation de ses VM et de ses Tenants, et de la gestion de tous les éléments (données et applications incluses) qu'il a stockés ou installés sur les infrastructures du Prestataire. Le service de support technique est fourni en accord avec les Conditions Générales de Vente et d'Utilisation, le Prestataire étant tenu à une obligation de moyens.

Le Commanditaire s'engage à utiliser le service de support technique de manière raisonnable, s'abstenant notamment de solliciter des services non souscrits auprès du Prestataire et de faire intervenir les équipes du Prestataire auprès de ses propres clients ou de tiers non inclus dans le Contrat. Le Prestataire se réserve le droit de rejeter toute demande de service ne respectant pas ces critères.

Le niveau d'engagement du support est conditionné à la souscription des unités d'œuvre de support associées.

3.9.2 Solicitation du service support technique

Le support technique est accessible par le biais d'un système de tickets via la console Commanditaire et est disponible durant les heures normales de bureau hors jours fériés (8h - 19h ; Lundi -- Vendredi ; calendrier et horaires français). Pour les urgences survenant en dehors des heures ouvrées, notamment les incidents affectant significativement la production, le service d'astreinte peut être joint via un numéro communiqué au Commanditaire à l'initialisation du Service

Pour chaque demande ou Incident, il est impératif de générer un ticket auprès du support du Prestataire. L'initialisation de ce ticket, comprenant toutes les informations nécessaires, est essentielle et marque le début de l'évaluation des engagements du Prestataire.

Dès que le Prestataire reçoit une demande ou une notification d'Incident, que ce soit par le biais de la console de gestion ou à la suite d'un appel téléphonique, un ticket est automatiquement créé. Lors de la déclaration d'un Incident, il est essentiel que le Commanditaire fournisse au prestataire un maximum de détails sur le problème rencontré. Cette démarche est cruciale pour permettre une évaluation adéquate de la situation, sa priorisation et un diagnostic efficace.

Le Commanditaire reçoit alors une confirmation par courriel, indiquant la création du ticket et son numéro unique. Le Commanditaire peut consulter le statut et l'historique de ses demandes et déclarations d'Incidents directement depuis la console de gestion.

3.9.3 Processus de gestion des Incidents

Lors d'une déclaration d'un Incident, l'équipe de support technique du Prestataire initie une investigation pour identifier la cause du problème et établir un diagnostic. Le Commanditaire doit collaborer activement avec le Prestataire en fournissant toutes les informations nécessaires et en effectuant les tests requis. Le Prestataire peut accéder au Service du Commanditaire pour diagnostiquer l'Incident.

Si les Services du Prestataire sont jugés fonctionnels et que l'Incident ne lui est pas imputable, le Commanditaire en sera informé. À la demande du Commanditaire, le Prestataire peut proposer des Services Professionnels pour identifier l'origine du problème, facturable sur accord préalable par tranche de 30mn.

Dans le cas où l'Incident est de la responsabilité du Prestataire ou de l'un de ses sous-traitants, celui-ci complète le diagnostic et s'attèle à la restauration du Service sans frais supplémentaires. Le diagnostic s'appuie sur les échanges entre les Parties et les données du Prestataire, ces éléments étant considérés comme probants par accord des Parties.

3.9.4 Processus de priorisation des traitements

La détermination du niveau de priorité d'un dossier repose sur une analyse matricielle qui évalue l'impact de l'Incident et son degré de criticité :

- Les niveaux d'impact sont définis de la manière suivante :

Niveau d'impact	Description
Impact I1	Le ou les services du Prestataire sont interrompus
Impact I2	Le ou les services du Prestataire sont dégradés
Impact I3	Le ou les services du Prestataire sont actuellement stable, mais montrent des signes de potentiel déclin à long terme

- Les niveaux de Criticités sont définis de la manière suivante :

Niveau de criticité	Description
Criticité C1	Le ou les services du Prestataire se dégrade à une vitesse préoccupante
Criticité C2	Le ou les services du Prestataire se détériore progressivement au fil du temps
Criticité C3	Le ou les services du Prestataire présentes un ou plusieurs inconvénient sans conséquence significative

- Sur la base d'une analyse approfondie de la situation, prenant en compte les éléments déterminant l'Impact et la Criticité, une priorité est attribuée au ticket conformément à la matrice de décision ci-après :

Niveau d'impact / Niveau de criticité	Impact I1	Impact I2	Impact I3
Criticité C1	Priorité P1	Priorité P2	Priorité P4
Criticité C2	Priorité P2	Priorité P3	Priorité P5
Criticité C3	Priorité P3	Priorité P4	Priorité P6

Les engagements de niveau de service correspondant à chaque niveau de priorité sont détaillés dans le chapitre suivant.

3.9.5 Langue et localisation du service de support

Cette clause vaut pour l'ensemble des Services, dont il est fait mention dans cette Convention de Service, qui peuvent être souscrits par le Commanditaire

Le support est fourni par le Prestataire au Commanditaire a minima en langue française. Le support peut être également fourni en langue anglaise.

Les opérations du service de support du Prestataire pour l'offre de service d'infrastructure qualifiée SecNumCloud sont situées dans l'Union Européenne.

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

4 Engagements et niveaux de services

Le Prestataire s'engage à garantir une surveillance continue de la performance et de l'intégrité sécuritaire de son infrastructure technique délivrant le Service, veillant à leur fonctionnement optimal.

L'indisponibilité d'un service, faisant l'objet d'un indicateur de performance, est reconnue dès son identification par le système de supervision du Prestataire, ou suite à une notification par un utilisateur du Commanditaire. Le début de l'indisponibilité est fixé au moment le plus précoce entre ces deux événements, afin de garantir un décompte précis et juste du temps d'indisponibilité.

La fin de l'indisponibilité est officiellement marquée par la restauration complète du service, confirmée soit par les outils de supervision du Prestataire, soit par un retour utilisateur, assurant ainsi une reprise effective des opérations et une mesure fidèle de la durée de l'interruption.

4.1 Engagements de disponibilité de l'infrastructure

Le Prestataire s'engage à maintenir un niveau de disponibilité et de performance conforme aux standards définis pour chaque période spécifiée. Les engagements de niveau de service (Service Level Agreements, SLAs) s'appliquent sous réserve que le Commanditaire implémente ses systèmes à travers au moins deux des Zones de disponibilité présentes dans la Région concernée.

En l'absence de respect de ces conditions par le Commanditaire, celui-ci se verra dans l'incapacité de revendiquer l'application des SLAs concernés, lesquels sont spécifiquement identifiés par un astérisque (*). L'accessibilité aux SLAs se fait via l'interface Commanditaire.

Les mesures s'entendent calculées mensuellement :

- ****SLA 1 (*) : IC-INFRA_SNC-01**** -- Disponibilité de la puissance de calcul (Compute) : taux de disponibilité garanti de 99,99%, calculé sur une base 24h/24, 7j/7.
- ****SLA 1.1 (*) : IC-PAAS_SNC-01**** -- Disponibilité de la plateforme RedHat OpenShift : taux de disponibilité garanti de 99,9%, calculé sur une base 24h/24, 7j/7.
- ****SLA 2 (*) : IC-INFRA_SNC-02**** -- Disponibilité du stockage : taux de disponibilité garanti de 99,99%, calculé sur une base 24h/24, 7j/7.
- ****SLA 3 : IC-INFRA_SNC-03** **-- Fiabilité de la sauvegarde pour les Services IaaS et OpenIaaS : taux de disponibilité garanti de 99,99%, calculé sur une base 24h/24, 7j/7.
- ****SLA 4 (*) : IC-INFRA_SNC-04**** -- Disponibilité de l'infrastructure réseau : taux de disponibilité garanti de 99,99%, calculé sur une base 24h/24, 7j/7.
- ****SLA 5 : IC-INFRA_SNC-05**** -- Accès Internet : taux de disponibilité garanti de 99,99%, calculé sur une base 24h/24, 7j/7.

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

Remarques :

En réponse à une attaque par déni de service distribué (DDoS), le Prestataire se réserve le droit d'ajuster sa configuration de routage internet pour limiter l'impact de cette attaque et sauvegarder son infrastructure. En particulier, si une adresse IP appartenant au Commanditaire est ciblée, le Prestataire peut recourir à la technique de blackholing via la communauté BGP pour bloquer tout le trafic vers l'adresse IP visée en amont chez ses fournisseurs, dans le but de protéger les ressources du Commanditaire ainsi que celles d'autres Commanditaires et de l'infrastructure du Prestataire. Le Prestataire encourage vivement le Commanditaire à adopter des mesures similaires, telles que l'utilisation de logiciels de pare-feu d'applications web disponibles sur le marché, et à configurer soigneusement ses groupes de sécurité via l'API de commande.

*Le Prestataire insiste sur la nécessité pour le Commanditaire de minimiser les ouvertures de flux, en évitant notamment de rendre accessibles les ports d'administration **SSH** (port TCP 22) et **RDP** (port TCP 3389) depuis l'ensemble d'Internet (sous-réseau 0.0.0.0/0), ainsi que les protocoles internes tels que **SMB** (port TCP/UDP 445) ou **NFS** (port TCP/UDP 2049).*

4.2 Engagement de disponibilité de l'interface Commanditaire

SLA 6 : IC-INFRA_SNC-06 -- Accès à la console d'administration du Service : une disponibilité garantie de 97%, assurée en continu, 24 heures sur 24 et 7 jours sur 7.

SLA 7 : IC-INFRA_SNC-07 -- Accès aux APIs de pilotage du Service : une disponibilité de 99.9%, calculé sur une base 24h/24, 7j/7.

4.3 Engagements de disponibilité du support

****SLA 8 : IC-INFRA_SNC-08**** -- Voici les engagements de performance du support technique du Prestataire pour les incidents, hors maintenances programmées :

Priorité	Garantie de temps d'intervention (GTI)	Objectif de performance
P1	30mn	95%
P2	2h	90%
P3	4h	90%
P4	24h	85%
P5	48h	85%

****SLA 9 : IC-INFRA_SNC-09**** -- Voici les engagements de performance du support technique du Prestataire pour les demandes de service :

	Garantie de temps d'intervention (GTI)	Objectif de performance
Demande de service	4h	90%

Le SLA 8 et SLA 9, seront exclusivement applicable dans le cas d'un Incident du service sauvegarde.

Nota :

- *Le délai pour la Garantie de Temps d'Intervention (GTI) est calculé à partir de la différence entre le moment où le Commanditaire ouvre le ticket et la première intervention du support du Prestataire.*
- *L'investigation d'incidents concernant les Commanditaires ne comprendra pas d'intervention à distance sur les serveurs hébergés du Commanditaire. Cette assistance se limitera à l'explication des métriques disponibles relatives à l'environnement du Commanditaire, afin de faciliter la compréhension des incidents ou des problèmes de performance rencontrés. Sur la base des résultats de cette analyse, des recommandations pourront être suggérées.*

4.4 Engagement de disponibilité du stockage objet S3

****SLA 10 : IC-INFRA_SNC-10**** -- Voici les engagements de disponibilité pour le stockage objet S3 :

Indicateur	Engagement	Objectif de performance
IC-INFRA-SNC-10.1	Durabilité du stockage d'un objet sur une région	99. 9999999% / an
IC-INFRA-SNC-10.2	Disponibilité de l'API Stockage Objet S3	99.99%
IC – INFRA-SNC-10.3	Latence maximale d'accès à un objet sur une région	150ms

Remarques :

- Le Service de Stockage Objet est spécifiquement conçu pour le stockage d'objets et doit être employé dans ce seul but, **excluant catégoriquement son utilisation en mode bloc**. Recourir au mode bloc par des méthodes détournées, incluant par exemple l'utilisation de *"FUSE" dans un environnement Linux*, constitue une infraction aux termes d'utilisation énoncés. Aucun incident, dysfonctionnement ou dommage découlant de cet usage non conforme ne sera couvert par les Accords de Niveau de Service (SLA) définis dans cette convention de services.
- La garantie de durabilité est conditionnée à une utilisation des services conforme aux meilleures pratiques et standards actuels, et exclut explicitement toute modification des données, qu'elle soit intentionnelle ou accidentelle, résultant d'actions entreprises par le Commanditaire.

4.5 Engagement de disponibilité de la VM Instance

Le Prestataire s'engage à un taux de disponibilité garanti de 99,95%, calculé sur une base 24h/24, 7j/7.

Le présent SLA ne constitue pas un engagement sur la disponibilité des éléments qui sont sous le contrôle exclusif du Client. Par conséquent, ne sont **pas** considérées comme des Périodes d'Indisponibilité les coupures, pertes d'accès ou pannes résultant de :

1. **Défaillances du Système d'Exploitation (OS) ou logicielles** : Plantage de l'OS invité (ex : *Kernel Panic*, *Blue Screen of Death*), surcharge de la CPU ou de la RAM causée par les processus du Client, ou corruption du système de fichiers interne.
2. **Configurations du Client** : Règles de pare-feu réseau ou local (iptables, firewalld) bloquant les accès, erreurs de configuration réseau au sein de l'OS via Cloud-init ou en post-déploiement.
3. **Pannes applicatives** : Arrêt ou crash d'un service hébergé sur la VM Instance (serveur web, base de données, conteneurs, etc.).
4. **Maintenance programmée** : Interventions matérielles ou logicielles sur l'infrastructure physique de Cloud Temple ayant fait l'objet d'une notification préalable dans le cadre des fenêtres de maintenance prévues par votre contrat de support.
5. **Comportement abusif ou violation** : Suspension de la VM Instance par Cloud Temple suite à une violation des Conditions Générales ou des exigences de sécurité (ex : compromission, non-respect des règles de la Marketplace Cloud Temple).
6. **Force majeure** : Événements hors du contrôle raisonnable de Cloud Temple.

5 Organisation de la relation contractuelle

5.1 Responsabilités du Prestataire

Le Prestataire s'engage :

- à informer son Commanditaire de manière adéquate (par exemple en cas de limite de capacité de ressources techniques délivrant le Service).
- à informer formellement le Commanditaire et dans un délai d'un mois, de tout changement juridique, organisationnel ou technique pouvant avoir un impact sur la conformité du Service aux exigences de protection contre les lois extra-européennes (19.6 du référentiel SNC v3.2).
- à fournir au Commanditaire des interfaces et des interfaces de service qui sont en langue française a minima.
- à prendre en compte les exigences sectorielles spécifiques liées aux types d'informations confiées par le Commanditaire dans le cadre de la mise en œuvre du Service et dans la limite des responsabilités du Prestataire d'une part, et des dispositions prévues au Contrat d'autre part ;
- à étudier les exigences sectorielles spécifiques liées aux types d'informations confiées par le Commanditaire dans le cadre de la mise en œuvre du Service, ultérieurement exprimées par le Commanditaire, et à indiquer à ce dernier les actions nécessaires pour leur prise en compte
- à ne divulguer aucune information relative à la prestation à des tiers, sauf autorisation formelle et écrite du Commanditaire.
- à mettre à disposition toutes les informations nécessaires à la réalisation d'audits de conformité conformément aux dispositions de l'article 28 du RGPD.
- à rendre compte auprès du Commanditaire, par la présente Convention de service, de tout Incident de sécurité impactant le Service ou l'utilisation faite par le Commanditaire du Service (incluant les données du Commanditaire).
- à autoriser un prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié, mandaté par le Prestataire, à auditer le service ainsi que son système d'information, conformément au plan de contrôle du SecNumCloud du Prestataire. De plus, le Prestataire s'engage à fournir toutes les informations nécessaires pour mener à bien les audits de conformité aux dispositions de l'article 28 du RGPD, menés par le commanditaire ou un tiers mandaté.
- à fournir, en qualité de sous-traitant, conformément à l'article 28 du Règlement général sur la protection des données (RGPD), assistance et conseils au Commanditaire en l'alertant dès lors qu'une instruction émise par ce dernier est susceptible de constituer une violation des règles de protection des données.
- à notifier le Commanditaire dans un délai raisonnable, à travers la console Commanditaire ou par courriel au contact Commanditaire, lorsqu'un projet impacte ou est susceptible d'impacter le niveau de sécurité ou la disponibilité du Service, ou à engendrer une perte de fonctionnalité, des potentiels impacts, des mesures d'atténuation mises en place, ainsi que des risques résiduels qui le concernent. Cette notification devra impérativement préciser :
    - La nature des opérations prévues ;
    - Le calendrier (date et heure programmées de début et de fin) ;
    - Les impacts identifiés sur la sécurité, ou la disponibilité, ainsi que les risques résiduels associés ;
    - Les mesures d'atténuation mise en place pour limiter ces impacts ;
    - Les coordonnées du contact responsable au sein du Prestataire.
- à documenter et à mettre en œuvre l'ensemble des procédures nécessaires pour respecter les exigences légales, réglementaires et contractuelles applicables au service, ainsi que les besoins de sécurité spécifiques du Commanditaire, définis par ce dernier et prévus au Contrat.
- à ne pas utiliser les données du Commanditaire issues de la production pour réaliser des tests, à l'exception d'en obtenir préalablement l'autorisation explicite du Commanditaire, auquel cas le Prestataire s'engage à anonymiser ces données et à en assurer la confidentialité lors de leur anonymisation.

- à supprimer les données et Données techniques relatives au Commanditaire, conformément à la « procédure d'effacement des données en fin de Contrat » décrite dans la présente Convention de service lors d'une fin ou résiliation de Contrat.
- à assurer un effacement sécurisé de l'intégralité des données du Commanditaire par réécriture complète de tout support ayant hébergé ses données dans le cadre du Service.

Sur demande du Commanditaire formelle et écrite, le Prestataire s'engage à :

1. Rendre accessible sur consultation au Commanditaire le règlement intérieur et la charte d'éthique du Prestataire ;
2. Rendre accessible sur consultation au Commanditaire les sanctions encourues en cas d'infraction à la politique de sécurité ;
3. Fournir au Commanditaire l'ensemble des événements le concernant dans les éléments de journalisation du Service. le Commanditaire pouvant par ailleurs consulter en autonomie les événements relatifs à son utilisation du Service au travers des interfaces web et API du Service ;
4. Rendre accessible au Commanditaire les procédures permettant de respecter les exigences légales, réglementaires et contractuelles en vigueur applicables au Service, ainsi que les besoins de sécurité spécifiques du Commanditaire prévus au Contrat ;
5. Fournir, les éléments d'appréciation des risques relatifs à la soumission des données du Commanditaire au droit d'un état non-membre de l'Union Européenne ;
6. Informer le Commanditaire des sous-traitants ultérieurs intervenants dans la fourniture du Service, et à l'informer de tout changement l'impactant relatif à ces sous-traitants.

Le Prestataire et l'ensemble de ses filiales s'engagent à respecter les valeurs fondamentales de l'Union européenne, à savoir la dignité humaine, la liberté, la démocratie, l'égalité, l'état de droit, ainsi que le respect des Droits de l'homme. Le service fourni par le Prestataire est conforme à la législation en vigueur en matière de droits fondamentaux et aux valeurs de l'Union européenne relatives au respect de la dignité humaine, à la liberté, à l'égalité, à la démocratie et à l'État de droit.

5.1.1 Responsabilité et Obligations du Prestataire réservées au service PaaS

Le Prestataire s'engage à mettre à la disposition du Commanditaire des interfaces utilisateur en langue française et anglaise, facilitant ainsi l'accès et la gestion des services fournis. Le Commanditaire, de son côté, s'engage à respecter les contraintes légales et réglementaires en vigueur relatives aux données qu'il confie au Prestataire pour traitement.

En cas de transmission de données sujettes à des exigences légales spécifiques, le Prestataire collaborera avec le Commanditaire pour identifier et mettre en œuvre les mesures de sécurité nécessaires, conformément aux obligations du Prestataire et dans le cadre de la prestation de services.

Le Prestataire prend également l'engagement d'examiner et de prendre en considération les besoins spécifiques liés aux secteurs d'activité du Commanditaire, en respectant les limitations de sa responsabilité, pour garantir un niveau de sécurité adapté aux informations traitées.

Si un projet est susceptible d'impacter la sécurité du Service offert ou la disponibilité dudit Service ou encore à engendrer une perte de fonctionnalité, le Prestataire s'engage à informer à travers la console ou par courriel au contact du Commanditaire et dans un délai raisonnable le Commanditaire des impacts potentiels, des mesures correctives envisagées et des risques résiduels qui le concerne, assurant une transparence totale.

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

Le Prestataire s'engage à ne pas utiliser les données du Commanditaire issues de la production pour réaliser des tests, à l'exception d'en obtenir préalablement l'autorisation explicite du Commanditaire, auquel cas le Prestataire s'engage à anonymiser ces données et à en assurer la confidentialité lors de leur anonymisation.

En cas de changement de sous-traitant pour l'hébergement, Le Prestataire informera le Commanditaire en amont, s'assurant que cette transition n'affecte pas négativement le service fourni.

À la demande du Commanditaire, le Prestataire fournira l'accès à son règlement intérieur, à sa charte d'éthique, aux sanctions applicables en cas de non-respect de sa politique de sécurité, aux événements le concernant, aux procédures relatives au service et aux exigences spécifiques de sécurité.

Le Prestataire s'engage à informer le Commanditaire de tout changement à venir sur des éléments logiciels sous la responsabilité du Prestataire dès lors que la compatibilité complète ne peut être assurée.

5.2 Limitation des responsabilités du Prestataire

Cette Clause ne vaut que si le Commanditaire souscrit à un Service IaaS, OpenIaaS ou Bare Metal.

Du fait de l'ensemble des définitions et conditions mentionnées dans la présente Convention de service, les responsabilités du Prestataire sont limitées ainsi :

1. Le modèle de responsabilité partagée, décrit dans la section « Modèle de responsabilités partagées » de la présente Convention de service, limite de fait l'implication du Prestataire dans les couches de fonctionnement allant "au-dessus" de la mise à disposition de ressources de calcul, de réseau, de stockage et de sauvegarde. Ceci exclut en particulier sans s'y limiter :
    - La gestion de ce qui est installé sur les machines virtuelles (OS, middlewares, applicatifs, etc.) ;
    - La tenue à jour des OS et autres logiciels installés par le Commanditaire sur ses machines dans ses Tenants ;
    - La sécurité des programmes, logiciels et applicatifs installés sur les machines virtuelles ;
    - La mise à jour des machines virtuelles ;
    - La sauvegarde des données au niveau applicatif.
2. Le Prestataire ne peut prendre d'engagements de sauvegarde des Tenants du Commanditaire sans que le Commanditaire n'ai au préalable souscrit aux unités d'œuvres adéquates
3. Le Prestataire ne peut se prévaloir de la propriété des données transmises et générées par le Commanditaire. En effet, celles-ci relèvent de la propriété du Commanditaire.
4. Le Prestataire souligne qu'il ne peut en aucun cas exploiter et/ou disposer des données transmises et générées par le Commanditaire sans validation préalable de ce dernier, étant entendu que leur disposition est réservée au Commanditaire.
5. Le Prestataire dégage toute responsabilité sur les composants physiquement hébergés et infogéré par le Prestataire, mais étant la propriété directe du Commanditaire ou d'un tiers avec lequel le Commanditaire a contractualisé. L'hébergement de composants physiques des clients ne fait pas partie du Service et est de fait hors du cadre de la présente Convention de service. Il incombe au Commanditaire d'évaluer le niveau d'adhérence ou de dépendance qu'introduisent ces composants vis-à-vis du Service IaaS qualifié SecNumCloud.

5.2.1 Limitation des responsabilités du Prestataire dans le cadre d'un service PaaS

La structure de responsabilité partagée réduit efficacement l'étendue de l'intervention du Prestataire aux aspects liés à la fourniture d'une plateforme RedHat OpenShift fonctionnelle, comprenant :

- La gestion de l'infrastructure IaaS qui prend en charge la plateforme RedHat OpenShift et son provisionnement,
- La gestion des systèmes nécessaires au bon fonctionnement de la plateforme,
- Le maintien en conditions de sécurité,
- La mise à jour de la plateforme RedHat OpenShift,
- La sauvegarde des données de configuration essentielles de cette plateforme, à l'exception des données et des applications du Commanditaire qui relèvent de sa responsabilité.

Elle exclut notamment, mais sans s'y limiter :

- La mise à jour des systèmes d'exploitation et des logiciels installés par le Commanditaire sur ses environnements OpenShift dans ses espaces locatifs,
- La sécurité des programmes, logiciels et applications installés au sein de l'environnement OpenShift par le Commanditaire,
- La sauvegarde des données au niveau applicatif,
- La configuration des politiques de sauvegarde.

5.3 Limitation d'accès

Dans le cadre du Service, le Prestataire est formellement interdit d'accéder aux Tenants appartenant au Commanditaire sans autorisation préalable. Il est de la responsabilité du Commanditaire de fournir les accès nécessaires au personnel du Prestataire, selon les besoins spécifiques de l'hébergement et, le cas échéant, des services professionnels de support, si cette option a été choisie par le Commanditaire.

Le Commanditaire reconnaît que ces accès sont accordés exclusivement pour les besoins liés à la prestation de services convenus, assurant ainsi une gestion sécurisée et conforme aux termes de l'accord.

L'accès distant par des tiers impliqués dans la prestation de service du Prestataire est strictement interdit. Dans l'éventualité où une exigence technique spécifique nécessiterait un tel accès, celui-ci ne pourrait être établi qu'après avoir clairement notifié le Commanditaire, fourni une justification détaillée et obtenu son accord écrit.

Cette mesure garantit le contrôle et la sécurité des données du Commanditaire, en s'assurant que toute exception à la règle est dûment autorisée et documentée.

5.4 Responsabilités des tiers participant à la fourniture du Service IaaS, OpenIaaS et Bare Metal

Le Prestataire maîtrise la liste des tiers partenaires participant à la fourniture du Service. Ces tiers sont les éditeurs, prestataires (du Prestataire) et autres fournisseurs participant de la fourniture du Service. Le Prestataire applique les mesures suivantes à ces tiers :

- Le Prestataire exige des tiers participant à la mise en œuvre du service, dans leur contribution au Service, un niveau de sécurité au moins équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité applicable au service ;

- Le Prestataire contractualise, avec chacun des tiers participant à la mise en œuvre du service, des clauses d'audit permettant à un organisme de qualification de vérifier que ces tiers respectent les exigences légales et les exigences SNC, permettant au Prestataire de respecter ses engagements dans la présente Convention de Service.
- Le Prestataire met en œuvre une procédure permettant de contrôler régulièrement les mesures mises en place par les tiers participant à la mise en œuvre du service pour respecter les exigences au Prestataire de respecter ses engagements dans la présente Convention de service.
- Le Prestataire assure un suivi des changements apportés par les tiers participant à la mise en œuvre du service susceptibles d'affecter le niveau de sécurité du système d'information du service.

5.5 Responsabilités et obligations du Commanditaire

Le Commanditaire dispose des obligations suivantes dans le cadre du Service :

- Pour rappel, dans le cadre des Services IaaS ou OpenIaaS, Le PRESTATAIRE fournit au Commanditaire une plateforme d'exécution de machines virtuelles, la configuration de celles-ci est à la charge du Commanditaire. Chaque machine virtuelle ne peut fonctionner sans une politique de sauvegarde associée. Le Prestataire définit via ses interfaces des politiques de sauvegarde automatiques mais c'est à la charge du Commanditaire d'activer ces politiques de sauvegarde et donc d'activer les machines virtuelles.
- Pour rappel, dans le cadre du Service Bare Metal, Le Prestataire fournit au Commanditaire une plateforme de calcul (serveur sans OS) dont la configuration de celle-ci est à la charge du Commanditaire.
- Le Commanditaire autorise l'ANSSI et l'organisme de qualification SNC à auditer le Service et l'infrastructure technique délivrant le Service.
- Le Commanditaire est responsable d'indiquer au Prestataire les éventuelles exigences sectorielles spécifiques liées aux types d'informations confiées par le Commanditaire et nécessitant d'être prises en compte par le Prestataire.
- Le Commanditaire accepte de ne pas demander au Prestataire des exigences ou actions faisant déroger le Prestataire aux exigences du référentiel SecNumCloud dans sa version courante d'une part, ou abaissant le niveau de sécurité établi par le respect des exigences de ce même référentiel d'autre part.

5.6 Droit du Commanditaire

À tout moment au cours de la relation contractuelle, le Commanditaire peut déposer une réclamation relative au service qualifié auprès de l'ANSSI.

À tout moment, le Commanditaire peut demander au Prestataire de lui rendre accessible son règlement intérieur et sa charte d'éthique.

6 Disponibilité, continuité et restauration du service

6.1 Gestion des Incidents

6.1.1 Types d'incidents traités dans le cadre de cette Convention de service

- Sinistres ;
- Pannes et défaillances ;
- Incidents de sécurité impactant la disponibilité, la confidentialité ou l'intégrité du Service.

6.1.2 Traitement des Incidents

Le Prestataire informe le Commanditaire dans les meilleurs délais, des Incidents et interruptions, au moyen d'une une notification dans la console Commanditaire ou par courriel au contact du Commanditaire. Le Prestataire informe le Commanditaire du traitement de l'Incident par le canal utilisé pour notifier l'Incident, ou par le canal indiqué dans la notification de l'Incident.

6.1.3 Niveau de notification des Incidents de sécurités

Le Commanditaire a la responsabilité de choisir les niveaux de gravité des Incidents de sécurité pour lesquels il souhaite être informé, par exemple via leur formalisation dans un PAS applicable au Service.

Par défaut, le Commanditaire est informé :

- Des incidents de sécurité avec impact (impacts I1 et I2 selon l'échelle d'impact définie dans le processus de priorisation des traitements de la présente Convention de service) ;
- Des incidents de sécurité impactant la confidentialité ou l'intégrité des données du Commanditaire confiées dans le cadre du Service ;
- Des violations de données à caractère personnel pour lesquelles le Commanditaire est responsable du traitement conformément à l'article 8 de l'Annexe DPA dans le cadre du Service ;

6.2 Maintenance du Service

6.2.1 Nature de la maintenance

Cette clause ne vaut que si le Commanditaire à souscrit à un Service IaaS, OpenIaaS ou Bare Metal.

Des violations de données à caractère personnel pour lesquelles le Prestataire est responsable du traitement et comportant des données personnelles du Commanditaire, conformément à l'article 8 de l'Annexe DPA. La maintenance assurée consiste en la mise en œuvre :

- Du plan de maintien en condition opérationnelle du Service pour assurer de bons indicateurs de disponibilité tels que s'y engage le Prestataire plus haut ;
- Du plan de PCA/PRA si souscrit par le Commanditaire déclenché selon les éventuels incidents qui surviendraient.

6.2.2 Accès distants du Prestataire sur le périmètre du Commanditaire

Le Prestataire s'interdit, dans le cadre de la présente Convention de service, tout accès aux Tenants et à l'espace de l'interface du Commanditaire.

Il incombera au Commanditaire de donner les accès nécessaires au personnel du Prestataire. Le Commanditaire reconnaît que les accès seront utilisés dans le cadre de l'hébergement et in fine dans l'opération de Services Managés (si souscrit par le Commanditaire).

6.2.3 Accès distants de tiers participant à la fourniture du service sur le périmètre du Commanditaire

Aucun accès distant de tiers participant à la fourniture du Service n'est autorisé.

Si un besoin technique rendait ce cas de figure nécessaire, alors ce type d'accès ne serait réalisé qu'après notification du Commanditaire justification et obtention de son accord écrit.

7 Audit

Le Prestataire s'engage à permettre au Commanditaire, ou à tout auditeur tiers et non concurrent du Prestataire que ce dernier aurait désigné, de consulter l'ensemble des documents nécessaires à l'attestation du respect intégral des obligations liées à la conformité avec les dispositions de l'article 28 du Règlement Général sur la Protection des Données (RGPD), facilitant ainsi la réalisation d'audits.

Le Prestataire s'engage notamment à tenir à disposition du Commanditaire la liste de l'ensemble des tiers qui peuvent accéder aux données et l'informer de tout changement de sous-traitants.

Par l'acceptation de la présente Convention de service, le Commanditaire confère son autorisation explicite à :

1. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ainsi qu'à l'entité de qualification compétente pour entreprendre la vérification de la conformité du Service et de son système d'information au référentiel SecNumCloud.
2. Un prestataire d'audit de la sécurité des systèmes d'information, dûment qualifié PASSI et expressément désigné par le Prestataire, pour mener à bien des audits de sécurité portant sur le Service.

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

8 Cycle de vie de la présente Convention de service

8.1 Entrée en effet de la Convention de service

La présente Convention de service entre en effet le jour de sa signature par le Commanditaire.

La collecte, la manipulation, le stockage et le traitement des données faits dans le cadre de l'avant-vente, la mise en œuvre, l'arrêt du Service, sont faits dans le respect de la législation en vigueur.

8.2 Evolutions de la Convention de service

Les modifications ou ajouts apportés à la présente Convention de service découlent exclusivement des requêtes formulées par les organes de gouvernance désignés à cet effet. Ces propositions de changement seront examinées par les Parties, habilitées à déterminer les aspects nécessitant une formalisation écrite.

Il est convenu que toute évolution de la Convention de service, après validation, qui altère les conditions financières initialement établies, nécessitera l'établissement et la signature d'un avenant au Contrat en cours.

Les facteurs pouvant induire une révision de cette Convention de service incluent, sans s'y limiter :

- L'évolution de l'infrastructure technique délivrant le Service IaaS, OpenIaaS ou Bare Metal ;
- L'adaptation de la plateforme PaaS orchestré par le Prestataire (dans le cas où le Commanditaire aurait souscrit au service PaaS) ;
- Les ajustements apportés aux services déployés par le Prestataire ;
- Les variations des engagements pris et des sanctions applicables ;
- Les reconfigurations organisationnelles au sein du Commanditaire ou du Prestataire ;
- L'expansion ou la réduction du champ d'application du Service auxquels le Commanditaire a souscrit.

La gestion des versions et des révisions de la Convention de service est consignée en préambule du document pour en faciliter le suivi.

8.2.1 Evolutions déclenchées par le Commanditaire

Les évolutions de la Convention de service peuvent avoir, notamment, pour origine :

- Une évolution de l'infrastructure gérée par le Prestataire ;
- Une modification des services mis en œuvre par le Prestataire ;
- Une modification des engagements de niveaux de services par le Prestataire.

8.2.2 Evolutions déclenchées par le Prestataire

Toute modification de la Convention de service est soumise à acceptation du Commanditaire. Il est entendu que toute modification ou complément validés modifiant les éléments financiers du Contrat, pourra impliquer la signature d'un avenant à celui-ci.

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

8.3 Réversibilité

Les Services ne comprennent pas d'obligation de réversibilité (à savoir, l'aide au Commanditaire pour qu'il puisse migrer son système vers un autre Prestataire) à l'exception de la mise à disposition du Commanditaire par le Prestataire de l'interface Commanditaire permettant au Commanditaire de sauvegarder et récupérer ses données y compris notamment les données de configuration de leur système d'information via l'une des modalités techniques suivantes au choix du Commanditaire : la mise à disposition de fichiers suivant un ou plusieurs formats documentés et exploitables en dehors du service fourni par le Prestataire ou bien via la mise en place d'interfaces techniques permettant l'accès aux données suivant un schéma documenté et exploitable (API).

En tant que seul maître de son système, le Commanditaire doit mettre en œuvre tous les moyens nécessaires pour faciliter cette opération, ce qui inclut notamment l'établissement d'une documentation rigoureuse ainsi que l'élaboration de plans de réversibilité. Dans le cas où le Commanditaire aurait besoin d'une prestation complémentaire, le Prestataire peut proposer une mission de conseil à cet égard dans le cadre d'un contrat spécifique à négocier.

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

9 Procédure d'effacement des données en fin de Contrat

À la fin du Contrat, quel qu'en soit le motif, le Prestataire procède à l'effacement sécurisé de l'intégralité des données traitées. Cette obligation couvre tant les données opérationnelles que les données à caractère personnel liées à l'exécution du Service.

9.1 Périmètre de suppression des données personnelles

L'effacement porte sur l'ensemble des informations permettant d'identifier directement ou indirectement les personnes physiques rattachées au Commanditaire, notamment :

- **Données de contact et d'identité :** Noms, prénoms, adresses email professionnelles, numéros de téléphone et fonctions des interlocuteurs du Commanditaire.
- **Comptes techniques nominatifs :** Identifiants de connexion, profils utilisateurs, journaux d'accès individuels et droits d'administration associés aux consoles de gestion ou APIs.

9.2 Modalités et Délais

Le Prestataire adressera un préavis formel au Commanditaire en respectant un délai de vingt et un (21) jours calendaires.
L'intégralité des données, y compris les copies de sauvegarde (backups) et les données techniques, sera définitivement supprimée dans un délai maximum de trente (30) jours suivant la notification, rendant toute récupération impossible.

9.3 Obligations de conservation légale

Par dérogation au paragraphe précédent, le Prestataire est autorisé et tenu de conserver certaines données sous forme d'archives intermédiaires, dont l'accès est strictement limité, pour répondre à ses obligations légales :

Type de donnée	Durée de conservation	Finalité
Journaux d'événements (logs)	6 mois	Obligations "Hébergeur" (LCEN)
Logs des activités SHIVA	18 mois	RGPD
Données de facturation / Contrats	10 ans	Code de commerce / Code civil
Pièces comptables	10 ans	Obligations fiscales et comptables
Données fiscales	6 ans	Contrôle de l'administration fiscale
Données de contact	5 ans	Archivage en base intermédiaire pour gestion des litiges contractuels

9.4 Certificat de suppression

À l'issue de l'opération, le Prestataire délivrera au Commanditaire un **certificat de suppression définitive**. Ce document atteste de la destruction irréversible des données sur les supports de stockage primaires et de la purge des systèmes de sauvegarde à l'issue de leur cycle de rotation.

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

10 Droit applicable

10.1 Disposition Générale

Le droit applicable et auquel est soumise la présente Convention de service est le droit français.

10.2 Respect du droit et des réglementations applicables

Le Prestataire s'engage sur les points suivants :

- L'identification des contraintes légales et réglementaires applicables dans le cadre du Service ;
- Le respect des contraintes légales et réglementaires applicables aux données confiées au Prestataire dans la limite des responsabilités de ce dernier d'une part, et des dispositions prévues au Contrat d'autre part. ;
- Le respect de la Loi informatique et liberté et du RGPD ;
- La mise en œuvre de moyens de protection des données personnelles ;
- La mise en œuvre d'un processus de veille légale et réglementaire ;
- De disposer et maintenir des relations appropriées ou une veille avec les autorités sectorielles en lien avec la nature des données traitées dans le cadre du Services. Cela inclus notamment l'ANSSI, le CERT-FR et la CNIL.

10.3 RGPD

Agissant en qualité de sous-traitant au sens de l'article 28 du Règlement général sur la protection des données (RGPD), le Prestataire s'engage :

- A assurer la transparence et la traçabilité ;
- A désigner un DPO en charge de définir et mettre en œuvre les mesures de protection des données à caractère personnel ;
- Apporter une assistance et du conseil au Commanditaire en l'alerte si une instruction de ce dernier constitue une violation des règles de protection des données personnelles si le Prestataire a le moyen d'en identifier ;
- Une garantie de sécurité sur les données traitées (du fait de la qualification SecNumCloud).

10.4 Protection vis-à-vis du droit extra-européen

Le siège statuaire du Prestataire est établi au sein d'un État membre de l'Union Européenne. Le capital social et les droits de vote dans la société du Prestataire ne sont pas, directement ou indirectement :

- individuellement détenus à plus de 24% ;
- et collectivement détenus à plus de 39% ;

par des entités tierces possédant leur siège statutaire, administration centrale ou principal établissement au sein d'un État non-membre de l'Union européenne.

En cas de recours par le Prestataire, dans le cadre du Service, au service d'une société tierce - y compris un sous-traitant - possédant son siège statutaire, administration centrale ou principal établissement au sein d'un État non-membre de l'Union Européenne ou appartenant ou étant contrôlée par une société tierce domiciliée en dehors l'Union Européenne, le Prestataire s'engage :

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

- à ce que cette susdite société tierce ne disposera d'aucun accès aux données opérées;
- à disposer d'une autonomie d'exploitation à travers la possibilité de faire appel à un autre sous-traitant ou de mettre rapidement en œuvre une alternative technologique.

Il est à noter que les données visées comprennent celles confiées au Prestataire par le Commanditaire, ainsi que toutes données techniques telles que les identités des bénéficiaires et des administrateurs de l'infrastructure technique, les données manipulées par les réseaux, les journaux de l'infrastructure technique, l'annuaire, les certificats; la configuration des accès, etc.., contenant des informations sur le Commanditaire.

Pour les besoins du présent article, la notion de contrôle est entendue comme étant celle mentionnée au II de l'article L233-3 du code de commerce.

CLOUD TEMPLE SAS CAPITAL 13 729 971€ ● SIRET 825 400 336 00095 ● TVA FR 55 825 400 336 ● LE BELVEDERE, 1 – 7 COURS VALMY SPACES 92800 PUTEAUX ● TEL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78

11 Signatures

Fait à _____, le _____

Pour Cloud Temple, le PRESTATAIRE

Pour _____, le Commanditaire