Convention de Service PaaS

**Table des matières**

* [1. Cadre](#X09af6387e1d2792b8edc09fc15abd136a837db5)
* [2. Acronymes](#Xc79d173393c04b42ba8cdf223cca3c0202f4dee)
* [3. Glossaire](#X0c9d1d82fdc5fcc3d01a320dd2dd3715a6900b4)
* [4. Objet de la convention de service PaaS du Prestataire](#X23ec3c3767539f9e69acc7cbf5af8aa8c1b6ad7)
* [5. Evolution de la convention de service PaaS](#Xa7161677dcf9a35d02c20807040326b39d55881)
* [6. Audit](#X910e2801262de94af715f54b8fb509cc70cc79a)
* [7. Description du service](#X3d12a6c93683f0122f5f9a8e21e7c12fc92490b)
* [8. Mise en œuvre du service](#Xc98fb6da582d483e300add6a80df6e3eb76498a)
  + [8.1. Description des composants techniques](#Xa61c340e3fdf14082cef411d3a913fc4bdeeb4c)
    - [8.1.1. Plateforme de service REDHAT OpenShift](#Xf81d22ed0abca8eab163c160107fa228901d82c)
    - [8.1.2. Infrastructure logiciel de pilotage de la plateforme Redhat Openshift](#Xf11ec2e6a431ae11852fe3129245b4d0fd0747b)
    - [8.1.3. Infrastructure de sauvegarde associée](#X77b1112fa2c2a53eb0cf09b416962164b77b437)
    - [8.1.4. Mise en œuvre de solutions de reprise d'activité ou de continuité d'activité](#Xae1394210f1c9bee4293a93160d2d11cc70ebdd)
* [9. Engagements et niveaux de services](#Xad2b4ae071a52a99b502c4e84cbba3f15ac78f8)
  + [9.1. Engagements de disponibilité de la plateforme RedHat OpenShift](#X273341276df81e9f6fad2000ac84216560e59fa)
* [10. Modèle de responsabilités partagées applicable](#Xa90d4e180ca2ae1d92e4e4cf00f20aca5061eac)
  + [10.1. Responsabilité et Obligations du Prestataire](#Xe5cf73850ea2189ab60f41560bf52e97d3019f9)
  + [10.2. Limitation de responsabilité du Prestataire](#X8856c8f606130116944398b24484722823c023c)
  + [10.3. Limitation d'accès](#X902763258f1242326933ce46892d3f549e73e30)
* [11. Effacement des données en fin de contrat](#Xbe642a80027ce4ad88cc932e98b8661c2a0d3a6)
* [12. Droit applicable](#Xa219184d62eb90dfeec612801fd05c5d816c331)

## 1. Cadre

|  |  |
| --- | --- |
| Référence | CT.AM.JUR.ANX.PAAS 2.1 |
| Date | 21 janvier 2025 |

## 2. Acronymes

| Acronyme | Description |
| --- | --- |
| CAB | Change Advisory Board – Comité consultatif sur les changements |
| CMDB | Configuration Management Database – Base de données de gestion des configurations |
| COPIL | Comité de pilotage |
| COSTRAT | Comité stratégique |
| DB | Database (base de données) |
| DRP | Disaster Recovery Plan (Plan de reprise d'activité) |
| GTI | Garantie de Temps d’Intervention |
| GTR | Garantie de Temps de Résolution |
| GTE | Garantie de Temps d’Escalade |
| HYPERVISEUR | Système d'exploitation permettant l'execution de VM sur une lame de calcul |
| ITIL | Information Technology Infrastructure Library - Bonnes pratiques pour la gestion des systèmes d'information |
| IAAS | Infrastructure as a Service |
| MCO | Maintien en condition opérationnelle |
| MOA | Maitrise d’Ouvrage |
| MOE | Maitrise d’Œuvre |
| OS | Operating system |
| PAQ | Plan d’Assurance Qualité |
| PAAS | Platform as a Service |
| SDM | Service Delivery Manager |
| RFC | Request For Change – Demande de changement |
| RGPD | Règlement Général de Protection des Données (personnelles) |
| RPO | Recovery Point Objective – Fraicheur des données restaurées en cas de sinistre |
| RTO | Recovery Time Objective – Délai de rétablissement du service en cas de sinistre |
| SLA | Service Level Agreement – Accord sur les niveaux de services |
| UO | Unité d’Œuvre |
| VABF | Validation d’Aptitude au Bon Fonctionnement |
| VABE | Validation d’Aptitude à la Bonne Exploitabilité |
| VM | Virtual Machine (Machine virtuelle) |
| VSR | Validation de Service Régulier |
| SNC | SecNumCloud |

## 3. Glossaire

Les expressions ci-après employées dans le présent document seront interprétées conformément aux définitions qui leur sont attribuées ci-dessous :

| Expression | Définition |
| --- | --- |
| "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. |
| Région | Une "région" dans le contexte du cloud computing 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. |
| Zone Disponibilité(AZ)(Availability 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. |
| 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. |

| Expression | Définition |
| --- | --- |
| Incident | Un "incident" désigne tout événement imprévu qui perturbe le fonctionnement normal d'un système ou compromet la sécurité des données. |
| Problème | Un "problème" est une cause fondamentale d'un ou plusieurs incidents, identifiée ou suspectée, nécessitant une analyse et une résolution pour prévenir sa récurrence |
| Changement | Un "changement" désigne tout ajout, une modification ou suppression impactant le Service, ayant été autorisé, planifié ou pris en charge. |
| Changement standard | Un "changement standard" est un 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 par les Parties. Il est alors intégré au catalogue des changements standards, et peut selon les cas avoir une GTI et une GTR. |
| Mise en production | action(s) d’administration de réalisation du changement quand celui-ci est approuvé (le changement, au sens ITIL, ne concernant que la gestion du changement et non sa réalisation/concrétisation). |
| Demande de service | demande d’évolution faisant l’objet d’une procédure, dont la réalisation: i) ne modifie pas la CMDB,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. |
| Element de configuration | Un "élément de configuration" est un composant identifiable du système d'information, tel qu'un logiciel, un matériel ou un document, sujet à gestion dans le cadre de la gestion des services IT |
| Service | Un "service" désigne le service qualifié SecNumCloud, délivré au COMMANDITAIRE par le Prestataire, tel que décrit dans la section « Description du Service » de la présente Convention de service. |
| Evenement | Un "événement" est toute occurrence détectable ou identifiable pouvant avoir une importance pour la gestion du Service. |
| Sinistre | Un « sinistre » désigne un événement grave d’origine naturelle ou humaine, accidentelle ou intentionnelle, occasionnant des pertes et des dommages importants à la Partie sinistrée. |
| Convention de service | Ce document, établi dans le cadre d'un contrat spécifique ou des Conditions Générales de Vente et d’Utilisation (CGVU), et ce, en conformité avec les exigences du Référentiel SecNumCloud. |
| Disponibilité | Capacité à assurer la disponibilité et le maintien des performances optimales d'un service, en accord avec les critères et engagements définis dans les Accords de Niveau de Service (SLA) |
| 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. |

## 4. Objet de la convention de service PaaS du Prestataire

La présente Convention de Services établit les termes et conditions selon lesquels le Prestataire s'engage à délivrer au COMMANDITAIRE une infrastructure conforme aux spécifications de l'offre « Platform as a Service – PaaS », dûment qualifiée SecNumCloud.

Objet de la Convention de Services :

1. Préciser les exigences de performance attendues par le COMMANDITAIRE en termes de fonctionnalité et de fiabilité de l'infrastructure.
2. Énoncer les obligations du Prestataire afin de satisfaire aux niveaux de service convenus.
3. Identifier les normes réglementaires applicables spécifiquement à l'infrastructure proposée.
4. Assurer une uniformité et une intégrité dans l'évaluation de la qualité des services rendus.
5. 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 présent 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.

## 5. Evolution de la convention de service PaaS

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 au sein du comité stratégique, seule instance habilitée à déterminer les aspects nécessitant une formalisation écrite.

Il est convenu que toute évolution de la convention, 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 incluent, sans s'y limiter :

* L'adaptation de la plateforme PaaS orchestrée par le Prestataire.
* 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 des services auxquels le COMMANDITAIRE a souscrit.

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

## 6. Audit

Le Prestataire s'engage à permettre au COMMANDITAIRE, ou à tout auditeur tiers 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 aux standards définis par le Référentiel SecNumCloud.
2. **Un prestataire d'audit en sécurité des systèmes d'information**, dûment qualifié et expressément désigné par le Prestataire, pour mener à bien des audits de sécurité portant sur le Service délivré par le Prestataire.

## 7. Description du service

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.

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.

## 8. 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).

### 8.1. Description des composants techniques

Les service 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, comme spécifié dans le document [Convention de Service IaaS](../Working%20in%20progress%20-%20not%20use/iaas/sla_iaas.md) du Prestataire.

#### 8.1.1. Plateforme de service REDHAT OpenShift

Le service englobe la mise à disposition au sein d'une région, sur 3 zones de disponibilité,

#### 8.1.2. Infrastructure logiciel de pilotage de la plateforme Redhat Openshift

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.

Le Prestataire alerte le COMMANDITAIRE sur le fait qu'une utilisation anormale de sa console d'administration, notamment en cas de surcharge de ses APIs de commande (hammering), peut déclencher des mesures de sécurité automatiques entrainant le blocage de l'accès aux APIs de commande ou à certains services du Prestataire. Il convient de souligner que cette situation ne constitue pas une indisponibilité du service mais une action de protection 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 doit pas être interprété comme une indisponibilité du service.

#### 8.1.3. Infrastructure de sauvegarde associée

Le Prestataire met à disposition du COMMANDITAIRE une plateforme de sauvegarde intégrée, dédiée et gérée, destinée à la protection des données de ses environnements RedHat Openshift. Le Prestataire assure le maintien en condition opérationnelle et en condition de sécurité de cette plateforme intégrée de sauvegarde. Indépendamment du nombre de zones de disponibilité souscrites par le COMMANDITAIRE, le Prestataire garantit que la plateforme de sauvegarde du COMMANDITAIRE sera située en dehors de la zone de disponibilité des charges de travail sauvegardées.

La prestation de sauvegarde se limite à la sauvegarde des machines virtuelles et des configurations de topologie de l'environnement IaaS des tenants SecNumCloud du COMMANDITAIRE. 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.

#### 8.1.4. 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.

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.

## 9. Engagements et niveaux de services

Le Prestataire s'engage à garantir une surveillance continue de la performance et de l'intégrité sécuritaire de ses plateformes et services, 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.

### 9.1. Engagements de disponibilité de la plateforme RedHat OpenShift

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-PAAS\_SNC-01\*\* – Disponibilité de la plateforme RedHat OpenShift : taux de disponibilité garanti de 99,9%, calculé sur une base 24h/24, 7j/7.

***Remarques*** :

* *En réponse 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).*

## 10. Modèle de responsabilités partagées applicable

### 10.1. Responsabilité et Obligations du Prestataire

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.

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 de Cloud Temple dès lors que la compatibilité complète ne peut être assurée.

### 10.2. Limitation de responsabilité du Prestataire

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 exclue 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.

### 10.3. Limitation d'accès

Dans le cadre de cette convention de 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.

## 11. Effacement des données en fin de contrat

À l'issue du contrat, qu'il arrive à échéance ou qu'il soit résilié pour quelque raison que ce soit, le Prestataire s'engage à procéder à l'effacement sécurisé de l'intégralité des données du COMMANDITAIRE, y compris les données techniques. Le Prestataire s'assurera de communiquer au COMMANDITAIRE un préavis formel, respectant un délai de vingt et un (21) jours calendaires. Les données du COMMANDITAIRE seront alors supprimées dans un délai maximum de trente (30) jours suivant cette notification.

Pour attester de cette suppression, le Prestataire remettra au COMMANDITAIRE un certificat confirmant l'effacement des données.

## 12. Droit applicable

Le droit applicable pour la presente convention de service est le droit français.

En cas de recours par le Prestataire, dans le cadre des services fournis au COMMANDITAIRE, à une société tierce, y compris un sous-traitant, dont le siège social, l'administration centrale ou le principal établissement est situé dans un État non membre de l'Union Européenne, ou qui est propriété ou sous le contrôle d'une société tierce domiciliée en dehors de l'Union Européenne, le Prestataire s'engage à garantir que ladite société tierce n'aura aucun accès aux données traitées par le service du Prestataire.

Il est à noter que les données visées comprennent celles confiées au Prestataire par le COMMANDITAIRE, ainsi que toutes les 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 précision, la notion de contrôle est définie conformément au II de l'article L233-3 du code de commerce.