CONDITIONS PARTICULIERES DE LOCATION D'UN SERVEUR DEDIE KIMSUFI

Dernière version en date du 07/11/2013

ARTICLE 1 : OBJET

Les présentes conditions particulières, complétant les conditions générales de services KIMSUFI, ont pour objet de définir les conditions techniques et financières dans lesquelles OVH s'engage à louer sur sa plate-forme, le serveur dédié KIMSUFI du Client.

Le Client reconnaît expressément qu'OVH ne participe aucunement au sens des présentes à la conception, au développement, à la réalisation et à la mise en place du site Internet du Client et de ses outils informatiques de gestion et d'administration.

Les présentes conditions particulières prévaudront sur les conditions générales si une contradiction devait apparaître entre ces deux documents.

ARTICLE 2 : MOYENS

La plate-forme serveur KIMSUFI où sera installé le serveur dédié KIMSUFI au Client est accessible pour le grand public par le réseau Internet au moyen de stations connectées au réseau Internet.

Pendant toute la durée de la location du serveur dédié au Client, OVH met à la disposition du Client l'accès à un forum, grâce auquel le Client pourra bénéficier de conseils techniques.

ARTICLE 3 : SUPPORT TECHNIQUE

L'assistance technique intervient exclusivement à partir du forum accessible à l'adresse : http://forum.kimsufi.com/

Il appartient ainsi au Client de faire état de ses problèmes ou dysfonctionnements rencontrés avec le Service sur le forum KIMSUFI.

Lorsqu'il apparait que le dysfonctionnement rencontré par le Client relève de la compétence du Service Incident, alors le conseiller technique KIMSUFI peut procéder à la création d'un ticket incident afin de procéder aux vérifications requises sur le Service.

ARTICLE 4 : CONDITIONS DE REALISATION DES PRESTATIONS

OVH informera par courrier électronique de la mise à disposition du serveur dédié au Client. La mise en ligne effective du serveur dédié détermine la date initiale à laquelle la facturation prendra effet.

La mise à disposition du serveur intervient dans un délai maximal de 7 jours à compter du paiement effectif du bon de commande par le Client.

SAS OVH, 2 rue Kellermann – 59100 Roubaix – France
SAS au capital de 10 000 000 € RCS Lille Métropole 424 761 419 00045 – Code APE 6202A - N° TVA : FR 22 424 761 419

Passé ce délai et à défaut de mise à disposition du serveur par OVH, le Client est en droit de demander l'annulation de la transaction et le remboursement des sommes déjà versées.

Le serveur loué au Client reste la propriété d'OVH. Tout serveur loué auprès d'OVH bénéficie d'une adresse IP fixe.

Les caractéristiques techniques du Service sont détaillées sur le site https://www.kimsufi.com.

Le Client est administrateur du serveur loué à OVH. Il a la possibilité d'installer par lui-même des applications software sur le serveur. Ces installations se font sous son entière responsabilité, et OVH ne pourra être tenu pour responsable d'un défaut de fonctionnement du serveur consécutif à ces installations.

ARTICLE 5 : OBLIGATIONS D'OVH

OVH s'engage à apporter tout le soin et la diligence nécessaires à la fourniture d'un service de qualité conformément aux usages de la profession et à l'état de l'art. OVH s'engage à :

5.1. Maintenir en état de fonctionnement le matériel. En cas de défaillance du matériel loué au Client identifié après la création du ticket incident, OVH s'engage à remplacer la pièce défectueuse dans les meilleurs délais possibles sauf défaillance qui ne serait pas de son fait, ou toute autre intervention qui nécessiterait une interruption du service excédant les délais habituels de remplacement. Dans ce dernier cas, OVH en informe immédiatement le Client.

5.2. Assurer la connexion réseau du serveur via Internet 24h/24 tous les jours de l'année. OVH se réserve la possibilité d'interrompre la connexion réseau du serveur pour procéder à une intervention technique sur le réseau les équipements du réseau OVH.

5.3. Intervenir rapidement en cas d'incident non consécutif à une mauvaise utilisation du serveur par le Client sur demande d'intervention du Client.

5.4. Assurer le maintien au meilleur niveau de la qualité de ses outils conformément aux règles et usage de sa profession.

ARTICLE 6 : RESPONSABILITE D'OVH

OVH se réserve le droit d'interrompre la connexion à Internet du Serveur loué au Client, si ce serveur constitue un danger pour le maintien de la sécurité de la plate-forme d'OVH, que ce soit suite à un piratage dudit serveur, ou à la suite de la détection d'une faille dans la sécurité du système, ou à une nécessité de mise à jour du serveur.

OVH informera auparavant, dans la mesure du possible, le Client dans un délai raisonnable en l'informant de la nature et de la durée de l'intervention, afin que le Client prenne ses dispositions. OVH s'engage à rétablir la connexion dès que les interventions de correction auront été effectuées par le Client.

SAS OVH, 2 rue Kellermann – 59100 Roubaix – France
SAS au capital de 10 000 000 € RCS Lille Métropole 424 761 419 00045 – Code APE 6202A - N° TVA : FR 22 424 761 419

OVH ne pourra être tenu responsable du contenu des informations, du son, du texte, des images, éléments de forme, données accessibles sur les sites hébergés sur le serveur du Client, transmises ou mises en ligne par le Client et ce à quelque titre que ce soit.

OVH ne saurait être tenu pour responsable du non-respect total ou partiel d'une obligation et/ou défaillance des opérateurs des réseaux de transport vers le monde Internet et en particulier de son ou ses fournisseurs d'accès.

ARTICLE 7 : OBLIGATIONS ET RESPONSABILITE DU CLIENT

7.1 Le Client agit en tant qu'entité indépendante et assume en conséquence seul les risques et périls de son activité. Le Client est seul responsable des services et des sites Internet hébergés sur son serveur dédié, du contenu des informations transmises, diffusées ou collectées, de leur exploitation et de leur mise à jour, ainsi que de tous fichiers, notamment fichiers d'adresses. Le Client s'engage notamment à respecter les droits des tiers, notamment les droits de la personnalité, les droits de propriété intellectuelle des tiers tels que droits d'auteur, droits sur les brevets ou sur les marques. En conséquence, OVH ne saurait être tenu pour responsable du contenu des informations transmises, diffusées ou collectées, de leur exploitation et de leur mise à jour, ainsi que de tous fichiers, notamment fichiers d'adresses et ce, à quelque titre que ce soit.

OVH ne peut que mettre en garde le Client sur les conséquences juridiques qui pourraient découler d'activités illicites sur le serveur, et dégager toute responsabilité solidaire sur l'utilisation des données mises à la disposition des internautes par le Client.

Le Client s'interdit également toute activité d'intrusion ou de tentative d'intrusion à partir du serveur (à titre non exhaustif : scan de ports, sniffing, spoofing).

Dans ces hypothèses, le Client ne pourra prétendre au remboursement par OVH des sommes déjà versées.

7.2 Le Client supportera seul les conséquences du défaut de fonctionnement du serveur consécutif à toute utilisation, par les membres de son personnel ou par toute personne auquel le Client aura fourni son (ou ses) mot(s) de passe. De même, le Client supporte seul les conséquences de la perte du ou des mots de passe précités.

7.3 Afin de maintenir le niveau de sécurité du serveur du Client et de l'ensemble des serveurs présents sur sa plate-forme, OVH s'engage à annoncer au Client, par courrier électronique et ou par l'intermédiaire du forum http://forum.Kimsufi.com/, la disponibilité des mises à jour des systèmes d'exploitation maintenus par OVH, pour lesquelles un défaut de sécurité a été relevé. Si la mise à jour de ces applications n'est pas effectuée suite aux demandes d'OVH, OVH se réserve le droit d'interrompre la connexion du serveur au réseau Internet.

De même, dans le cas où OVH détecterait que la machine du client est piratée, un courrier électronique sera envoyé au Client, indiquant qu'une procédure de réinstallation s'impose pour maintenir l'intégrité du serveur et de l'ensemble de la plate-forme. Le Client peut alors effectuer une telle procédure via son Interface de gestion, après avoir sauvegardé l'ensemble de ses données. OVH se réserve le droit

SAS OVH, 2 rue Kellermann – 59100 Roubaix – France
SAS au capital de 10 000 000 € RCS Lille Métropole 424 761 419 00045 – Code APE 6202A - N° TVA : FR 22 424 761 419

d'interrompre la connexion du serveur au réseau Internet, en attendant la réinstallation à neuf de la machine. OVH n'est pas tenu à opérer le transfert des données du système piraté au nouveau système, cette manipulation devant être faite par le Client lui-même. OVH s'engage et limite uniquement son intervention à l'installation du nouveau système.

7.4 Pour des raisons de sécurité, OVH se réserve la possibilité de procéder à la suspension immédiate et sans préavis de tout Serveur sur lequel serait proposé à titre gracieux ou onéreux, un service ouvert au public de Proxy, IRC, VPN, TOR, pour lequel OVH aurait connaissance d'une utilisation malveillante, frauduleuse ou illicite.

7.5 Il appartient au Client de prendre toutes mesures nécessaires à la sauvegarde de ses données.

7.6 Il appartient au Client de s'acquitter de toute licence ou droit d'utilisation contracté auprès d'OVH ou d'un tiers. A défaut, OVH se réserve le droit de suspendre sans préavis le Service.

7.7 OVH se réserve la possibilité d'exercer des contrôles sur la conformité de l'utilisation par le Client du Service à ces dispositions.

OVH se réserve le droit de suspendre sans préavis le Service, et de procéder à la résiliation du contrat de location du serveur dédié dès lors que le maintien du Serveur du Client constitue un risque trop important pour l'Infrastructure OVH, ou encore en cas de non-respect par le Client des conditions particulières et générales d'OVH et, de manière générale, de l'ensemble des lois et règlements en vigueur, ainsi que des droits des tiers.

7.8 Il est rappelé au Client que l'intervention d'OVH dans le cadre de la souscription d'un contrat portant sur un serveur dédié se limite à l'installation du serveur. OVH n'assure à ce titre que la location d'une infrastructure spécialisée, sans aucune maîtrise du contenu des sites hébergés ou de la relation contractuelle des éditeurs de ces sites avec leur hébergeur, client d'OVH au titre d'un contrat de location de serveur dédié. Le Client doit dès lors être considéré comme un hébergeur au sens de l'article 6.I.2 de la loi pour la Confiance dans l'Economie Numérique du 21 juin 2004, puisqu'il assure, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par les destinataires de ces services. Il lui appartient dès lors de détenir et conserver, en application de l'article 6.II de la loi précitée, l'ensemble des données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont il est prestataire et ce pour une durée de 12 mois, sans que la responsabilité d'OVH puisse être à cet égard engagée.
Il appartient également au Client, en application de l'article 6.I.7 de la loi pour la Confiance dans l'Economie Numérique du 21 juin 2004, de mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à sa connaissance toute infraction constitutive d'apologie de crime contre l'humanité, d'incitation à la haine raciale, de pornographie enfantine, d'incitation à la violence, ainsi que d'atteinte à la dignité humaine, ou encore d'activités illégales de jeux d'argent. Enfin, l'attention du Client est attirée sur le fait qu'il doit apparaître en qualité d'hébergeur dans les mentions légales indiquées par les éventuels éditeurs des sites Internet hébergé sur son serveur KIMSUFI.

ARTICLE 8 : MESURES DE LUTTE CONTRE L'ENVOI DE SPAM DEPUIS LE RESEAU OVH

SAS OVH, 2 rue Kellermann – 59100 Roubaix – France
SAS au capital de 10 000 000 € RCS Lille Métropole 424 761 419 00045 – Code APE 6202A - N° TVA : FR 22 424 761 419

OVH met en place un système de mesures techniques destiné à lutter contre les envois de courriels frauduleux ainsi que la pratique du SPAM émis depuis ses infrastructures.

A cette fin, OVH procède à une mesure de vérification du trafic émis depuis le serveur utilisé par le Client à destination du port 25 (serveur SMTP) sur internet. Cette opération consiste à vérifier le trafic par le biais d'outils automatiques.

Les envois ne sont ni filtrés ni interceptés mais vérifiés avec un décalage temporel de quelques secondes. Ces opérations sont faites en parallèle et en aucun cas de manière frontale entre le serveur et le réseau internet.

De même, aucune opération n'est effectuée sur les courriels émis : OVH ne procède pas au marquage (Tag) des courriels, et ne modifie d'aucune manière les courriels envoyés par le Client. Aucune information n'est stockée par OVH lors de ces opérations en dehors de données statistiques.

Cette opération est effectuée de manière régulière et totalement automatique. Aucune intervention humaine n'est réalisée lors de la vérification du trafic vers le port 25 (port SMTP).

Dans l'hypothèse d'envois depuis le serveur du Client de courriels identifiés comme SPAM ou frauduleux, OVH en informe le Client par courriel et procède au blocage du port SMTP du Serveur.

OVH ne conserve aucune copie des courriels émis depuis le port SMTP du Serveur même lorsqu'ils sont identifiés par SPAM.

Dans l'hypothèse de blocage du port SMTP, le Client devra se rendre sur le forum Kimsufi et demander le déblocage.

Tout nouveau courriel identifié comme SPAM entrainera un nouveau blocage du port SMTP pour une durée plus importante.

A compter du troisième blocage, OVH se réserve la possibilité de refuser toute nouvelle demande de déblocage du port SMTP.

ARTICLE 9 : MITIGATION (PROTECTION CONTRE LES ATTAQUES DOS ET DDOS)

OVH met en place une protection contre les attaques informatiques de type DOS et DDOS (Attaques par déni de service) et sous réserve qu'elles soient effectuées de manière massive. Cette fonctionnalité vise à permettre le maintien en fonctionnement du Service du Client pendant toute la durée de l'attaque.

Cette fonctionnalité consiste à vérifier le trafic à destination du Service du Client et provenant de l'extérieur du réseau OVH. Le trafic qualifié d'illégitime est alors rejeté en amont de l'infrastructure du Client, permettant ainsi aux utilisateurs légitimes de pouvoir accéder aux applications proposées par le Client malgré l'attaque informatique.

Ces mesures de protection ne peuvent pas intervenir pour les attaques informatiques telles qu'injection SQL, Bruteforce, exploitation de failles de sécurité etc…

SAS OVH, 2 rue Kellermann – 59100 Roubaix – France
SAS au capital de 10 000 000 € RCS Lille Métropole 424 761 419 00045 – Code APE 6202A - N° TVA : FR 22 424 761 419

En raison de la très grande complexité du Service de protection, OVH n'est soumis qu'à une obligation de moyen, il est possible que l'attaque ne soit pas détectée par les outils mis en place, et que les outils mis en place ne permettent pas le maintien en fonctionnement du Service.

En fonction de la nature de l'attaque et de sa complexité, OVH procèdera à différents niveaux de protection du trafic afin de préserver son infrastructure et le Service du Client.

La mitigation n'est activée qu'à compter de la détection de l'attaque par les outils d'OVH, et pour une durée minimale de 26 heures. Par conséquent jusqu'à l'activation de la mitigation, le Service supporte l'attaque de manière frontale ce qui peut entrainer son indisponibilité.

Dès lors que l'attaque informatique est identifiée et que la mitigation est activée automatiquement, la mitigation ne pourra pas être désactivée jusqu'au terme du délai de 26 heures.

Pendant toute la durée de l'activation de la mitigation, OVH ne peut garantir l'accessibilité des applications du client mais s'efforcera de limiter l'impact de cette attaque sur le Service du Client et sur l'Infrastructure d'OVH.

Si malgré l'activation de la mitigation, l'attaque informatique est de nature à porter atteinte à l'intégrité des infrastructures OVH ou aux autres clients OVH, OVH renforcera les mesures de protection ce qui peut entraîner une dégradation du Service du Client ou impacter sa disponibilité.

Enfin, il est possible qu'une partie du trafic généré par l'attaque informatique puisse ne pas être détectée par les équipements d'OVH et atteindre le Service du Client. L'efficacité de la mitigation dépend également de la configuration du Service du Client, à ce titre il appartient au Client de vérifier qu'il dispose de compétences nécessaires pour en assurer la bonne administration.

Pour rappel, la mitigation ne dispense en aucun cas le Client de procéder à la sécurisation de son Service, de mettre en place des outils de sécurité (pare-feu…), de procéder régulièrement à la mise à jour de son système, sauvegarde de ses données, ou encore de veiller à la sécurité de ses programmes informatiques (scripts, codes etc…).

SAS OVH, 2 rue Kellermann – 59100 Roubaix – France
SAS au capital de 10 000 000 € RCS Lille Métropole 424 761 419 00045 – Code APE 6202A - N° TVA : FR 22 424 761 419