SPECIAL CONDITIONS FOR PUBLIC CLOUD SERVICE

Version date 12/09/2016

ARTICLE 1: APPLICATIONS OF CONDITIONS

1.1 OVH Limited (the "Supplier") shall provide the OVH Public Cloud Service ("Services") to the Customer and the Customer shall pay for the Services in accordance with these Conditions and the General Conditions which shall govern the contract between the parties to the exclusion of any other terms or conditions whether proposed by the Customer, implied by law, trade custom, practice or course of dealing or otherwise (the "Contract").

1.2 These special terms and conditions supplement the Supplier's General Terms and Conditions of Service, and are intended to set out the conditions, in particular the technical and financial conditions, being part of the Services to which the Supplier is committed. In the event of conflict between these Conditions and the General Conditions, these Conditions shall prevail.

1.3 Terms that begin with an upper-case letter are defined in the OVH Glossary, which can be found on the Supplier website.

ARTICLE 2: MEANS

2.1 In the context of the Services, the Supplier shall provide the Customer with Instances, Object Storage Containers and Archive Storage.

2.2 Instances are provided with Local or Remote Storage Space, a portion of RAM and Host Server processor resources and a fixed geolocated IP address in compliance with the physical location of the Instance.

2.3 Resources allocated, the maximum data transfer on the bandwidth and the characteristics of the Storage Space (replication, distribution, localisation) vary, depending on the configuration and type of Instance.

2.4 The volume of RAM and processor resources allocated to the Customer are either guaranteed (RAM Instances and CPU Instances), or shared by the Customer with other users that have one or several Instance(s) installed on the same Host Server. Where resources are shared, performance cannot be guaranteed.

2.5 Depending on the selected type of Storage Space, different features and/or options (eg: public containers, transfer protocols) may be available. Some Storage Spaces are not redundant (for example: Archive Storage).

2.6 Before choosing and using an instance or a Storage Space, the Customer undertakes to carefully examine each Instance configuration and each type of available Storage Space. It is up to the Customer to select Instances, Storage Spaces and operating systems whose characteristics correspond to their needs.

2.7 The different configurations and characteristics of Instances and Storage Spaces are described and available online on the Supplier website. These configurations and characteristics change regularly. It is up to the Customer to pay attention to these developments.

2.8 Resources (Host Server, Storage Spaces, Instances, etc.) available to the Customer remain the exclusive property of the Supplier.

2.9 The Infrastructure capabilities used in connection with the Service may be limited.

2.10 Due to the highly-technical nature of the Service, The Supplier is only subject to an obligation of means.

2.11 For the entire duration of the subscription, the Supplier provides the Customer with a Management Interface that enables them to manage the Services, configure their Instances, Object Storage Containers and Archive Storage (creation, deletion, etc.) and retrieve their usage statements.

2.12 The Customer and the general public may access the Supplier Infrastructures via the internet where Instances, Object Storage Containers, Archive Storage and any other Storage Spaces are made available. The Customer must have an internet connection in order to log in to the Management Interface and access the Service, and is solely responsible for the aforementioned internet connection, in particular its availability, reliability and security.

ARTICLE 3: TECHNICAL SUPPORT

3.1 Where the Supplier is responsible for any disruption to the Service, the Customer has the right to contact the support service via the Management Interface, or by using the contact details available on the Supplier website.
Each request or incident report received results in the creation of a ticket (“incident ticket"). The customer is notified by email of the creation of the ticket and the corresponding number.

3.2 When an incident has been submitted, the Customer provides the Supplier with as much information about the problem, to enable the successful completion of diagnosis.

ARTICLE 4: CONDITIONS OF USE OF SERVICES

4.1 The Customer subscribes to the Services on the Supplier website. The subscription requires the registration of a payment method from which payments shall be executed for invoices issued for the Services, under the conditions provided in Article 13 below.

4.2 From the time of activation of the Services by the Supplier, the Customer has the ability to create Instances in the Management Interface and use the Services.

4.3 The Customer shall be the sole administrator of their Instances. The Supplier shall under no circumstances be involved in the administration of the Customer's Instances. Similarly, the Customer bears sole responsibility for their usage of the Object Storage Containers, Archive Storage and other Storage Space provided to them.

4.4 The Supplier is responsible for the administration of the Infrastructure (hardware, network, Host Servers, disks) on which the Instances and Storage Space made available to the Customer are configured.

4.5 The Customer confirms they have all the necessary technical knowledge to ensure the correct administration of resources (Instances, Object Storage Containers, Archive Storage and other Storage Space) provided by the Supplier, and to back up the data stored on these resources. The Customer also undertakes to acquaint themselves with the documentation related to the Services, provided by the Supplier.

4.6 The Customer has the right to install software on their Instances. The Customer bears sole responsibility for these installations, the Supplier shall not be liable for any failure of the proper operation of the Customer Instances resulting from such installations.

4.7 The Customer undertakes to comply with the licence conditions and conditions of use of the operating system on which the Instances are configured by the Supplier, and the licence conditions and conditions of use of the applications, in some cases preinstalled on the Instances by the Supplier. The Supplier reserves the right to modify the operating systems and applications pre-installed by the Supplier, in particular by way of any updates and/or version upgrades that it deems necessary in their sole discretion. If an operation system or application update is necessary while it's being use by the Customer, this update is carried out in consultation with the Customer.

4.8 The Customer may also perform maintenance operations and updates on the aforementioned operating systems and applications pre-installed on their Instances. In such a case, the Customer assumes full responsibility and the Supplier shall not under any circumstances be held responsible, including without limitation where said operations (maintenance, updates, etc.) are performed in violation of the applicable conditions of use/licence conditions, or where there the Instance fails to perform and/or operate correctly following maintenance operations and/or updates performed by the Customer.

4.9 The applicable licence conditions and conditions of use of the aforementioned applications and operating systems are either provided to the Customer at the time of the first order of the Instance configured with these preinstalled systems and/or software, or made available to the Customer via the Supplier website or the Website of the software company.

4.10 The Supplier reserves the right to restrict access to certain ports which it deems to be sensitive in order to protect the Infrastructure. Similarly, the Customer acknowledges that UDP/ICMP flows are limited.

4.11 The Customer has the option, via the Management Interface, to increase and decrease the number of Instances and the volume of data stored in their Storage Spaces. It may also change the Instance(s) provided by the Supplier in order to change configuration. These changes are made asynchronously upon the request of the Customer. The Customer creates the request in the Management Interface or the Supplier API.

4.12 The operations of removal and reinstallation of Storage Spaces (Object Storage Containers, Archive Storage, and others) lead to automatic and irreversible deletion of all data and information stored there. Similarly, operations of removal and reinstallation of Instances lead to automatic and irreversible deletion of (a) operating systems and applications that are installed there, and (b) all data and information stored on Local and Remote Storage Spaces associated with deleted or reinstalled Instances. The Customer is solely responsible for operations (such as backups, transfers, Snapshot, etc.) they deem necessary before removing or reinstalling their Instances and Storage Spaces, to prevent any loss of information, content and data.

4.13 The Supplier reserves the right to limit or restrict certain functionality of the Instance in order to guarantee the security of the Infrastructure. The Supplier shall inform the Customer of the implementation of these restrictions whenever possible.

4.14 The Customer undertakes to use the Service with good mutual understanding.

ARTICLE 5: OBLIGATIONS AND RESPONSIBILITY OF THE SUPPLIER

5.1 The Supplier shall provide the Services with reasonable care and skill and in accordance with good industry practice.

5.2 The Supplier undertakes to:

a) Ensure the administration of the Supplier Infrastructure and Host Servers.

b) Maintain the Host Server in an operational state. The Supplier shall use reasonable endeavours to replace any defective part of the Host Server as soon as reasonably possible except where the Supplier is not directly responsible for the failure or in situations where the repair or replacement procedure requires an interruption of Service which exceeds the usual replacement time. In the latter case, the Supplier will notify the Customer as soon as reasonably practicable.

c) Make the Instances and Object Storage Containers available to the Customer in accordance with the provisions of Article 11 of this Contract. The Supplier reserves the right to interrupt the Services in order to perform a technical intervention to improve the operation of the Services.

d) Upon notification by the Customer of an incident, intervene as soon as possible, provided the incident is not caused by the Customer's misuse of the Instance or

Object Storage Containers and subject to incidents due to improper use of the Service by the Customer.

e) Ensure the quality of its tools is maintained in accordance with good industry practice and in accordance with the rules and customs of the profession.

5.3 The Supplier does not back up specific content or data stored on the Instances, Object Storage Containers, Archive Storage or any other of the Customer's Storage Spaces. Any data replication mechanisms implemented by the Supplier within the aforementioned Storage Spaces (including Object Storage Containers and Archive Storage) are under no circumstances a guarantee to the Customer against the loss of their contents and data.

ARTICLE 6: OBLIGATIONS AND RESPONSIBILITY OF THE CUSTOMER

6.1 The Customer acts as an independent entity and shall solely bear all risk associated with its activity when using the Services. The Customer is solely responsible for the services and Websites that they host on the Instance and Storage Spaces provided, as well as the content of transmitted, broadcast or collected data, the processing and updating of data, and all files, especially address files.

6.2 The Customer shall comply at all times with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the "PEC Regulations").

6.3 The Supplier only ensures access to the Services to enable the Customer to store their data and their customers' data.

6.4 The Customer shall take all technical steps available to ensure that it holds and retains connection logs or any data which can allow anyone to identify any person who contributes to the creation of content for the services for which the Customer is the provider, according to the legislation in force and, shall at all times comply with the PEC Regulations.

6.5 The Customer undertakes to respect the rights of third parties, rights of the individual, intellectual property rights such as copyrights, patent rights or trademark rights, database rights and any other intellectual property. The Supplier shall not be held liable for the content of any transmitted, disseminated or collected data, data processing or updating, or any files, namely address files of any kind.

6.6 The Customer is prohibited from making any files or links that breach third party intellectual property rights publicly available via websites hosted on their Instance, deploying services which are intended to enable users to download files in large quantities to and from file hosting platforms, using proven spamming techniques on the internet, any intrusive activity or any intrusion attempt (including, but not limited to: port scans, sniffing, spoofing), and any activity or contentious behaviour such as traffic exchanging (Hitleap, Jingling), Black Hat SEO (downloading and uploading videos from and to online gaming platforms…), crypto-currency mining, video game bots, etc. The customer agrees to fulfill any license that is required if they use a third-party software when using the Service.

6.7 In such events, the Supplier reserves the right to suspend the Service without notice and immediately terminate the Contract, without prejudice to the right to all damages that the Supplier may claim.

6.8 The Supplier shall therefore not be liable, in any way whatsoever, even jointly, for the information, files (especially address files), data and any other of the Customer's content, and the way in which it is used under the Service, including its transmission, broadcasting to internet users, collection, updating etc. The Supplier will only alert the Customer as to the legal consequences that could result from unlawful activities conducted on or from the Service.

6.9 The Customer is solely liable for the consequences of any malfunction of their Instances, Object Storage Containers and/or Archive Storage as a result of any usage, by their staff or any person to which The Customer may have provided their password(s) and any other means of access (such as SSH access keys, OpenStack Tokens, etc…). Similarly, the Customer is solely liable for the consequences of the loss of passwords and any other means of access.

6.10 In order to maintain the security level of the Customer's Instances and all the servers on the Infrastructure, the Supplier reserves the right to request that The Customer update the operating system running on the Instance and any applications pre-installed by the Supplier, where security vulnerability is identified. If The Customer does not act upon such requests, the Supplier reserves the right to disconnect the Instance from the Internet.
Similarly, in the event that the Supplier finds that the Instance, Object Storage Containers, Archive Storage and other Storage Space represents a security risk, the Supplier may send an email to the Customer to inform the latter with a reinstallation or deletion procedure to maintain the integrity of the Service and the Infrastructure. The Supplier reserves the right to disconnect the Instances, the Object Storage Container, Archive Storage and other Storage concerned from the Internet pending the Customer's reinstallation of their Instance. The Customer is solely responsible for backing up and transferring data from the failing system to the new system before any reinstallation and / or deletion of the Service.

6.11 The Customer acknowledges that, for security reasons, some features and protocols (such as IRC or peer-to-peer file sharing) are likely to be restricted under the Services. Anonymisation services (Proxy) and cardsharing (CCCam or equivalent) are prohibited under the Services.

6.12 The Services, especially the Cloud Computing technologies that the Supplier uses for the management of the Customer's Instances, Object Storage Containers, Archive Storage and other Storage do not guarantee Service continuity or the protection or retention of Customer data. The Customer is solely responsible for all measures to ensure the backup of data, especially when the data is sensitive and / or necessary for business continuity. The Customer is responsible for establishing and managing a business continuity plan and / or disaster recovery plan, and more generally all technical and organisational measures likely to enable the Customer to continue operating in the event of a major Services malfunction which may impact business continuity and the availability and integrity of their content and data.

6.13 It is the Customer's responsibility to pay for any licenses or usage rights contracted with the Supplier. Should The Customer fail to do so, The Supplier reserves the right to suspend the Services without prior notification.

6.14 The Supplier reserves the right to carry out checks to ensure that the Customer's use of the Service complies with these conditions. The Supplier reserves the right to suspend the Service without notice, under the conditions stated in the General Conditions of Service, in the event of a breach by the Customer of the Supplier's Special Conditions or General Conditions of Service and, in general, of any applicable statutory and regulatory provisions, or of any third-party rights.

ARTICLE 7: MEASURES FOR THE PREVENTION OF SPAMMING FROM THE SUPPLIER'S NETWORK

7.1 The Supplier shall implement a system of technical measures intended to prevent the dispatch of fraudulent emails and spam from its Infrastructure.

7.2 Further to Article 7.1, the Supplier shall monitor outgoing traffic from the Service towards port 25 (SMTP server) on the internet, which shall involve monitoring traffic by means of automatic tools.

7.3 The outgoing traffic referred to in Article 7.2 shall be monitored by the Supplier with a delay of a few seconds, rather than being filtered or intercepted. These operations shall be conducted by the Supplier concurrently and not, under any circumstances, directly between the Services and the internet.

7.4 The Supplier reserves the right in certain circumstances to block the sending of emails.

7.5 The Supplier shall not conduct any tagging of e-mails, and shall not modify e-mails sent by the Customer in anyway whatsoever. No information shall be stored by the Supplier during these operations aside from statistical data.

7.6 The operation in Article 7.2 shall be conducted regularly and in a fully-automated manner by the Supplier and the Customer acknowledges that no human intervention is involved during the monitoring of traffic to port 25 (SMTP port).

7.7 In the case of outgoing traffic from the Customer's server, including e-mails, being identified as spam or fraudulent e-mails, the Supplier shall inform the Customer by e-mail and block the Server's SMTP port.

7.8 The Supplier shall not keep any copy of e-mails sent from the Service's SMTP port, even when they are identified as Spam.

7.9 The Customer may request unblocking of the SMTP port through their Management Interface.

7.10 Any new e-mail identified as Spam will entail a new blocking of the SMTP port by the Supplier for a longer period to be determined at the Supplier's reasonable discretion.

7.11 On the occurrence of the Supplier blocking the SMTP port for a third time, the Supplier reserves the right to deny any new request for the unblocking of the SMTP port.

ARTICLE 8: MITIGATION (protection against DOS and DDoS attacks)

8.1 The Supplier shall implement protection against DOS and DDoS-type (Distributed Denial of Service) hacking attempts provided that these attacks are conducted in a manner reasonably considered to be serious enough by the Supplier to warrant such protection. In implementing such protection, the Supplier shall use reasonable endeavours to ensure that the operation of the Customer's Services is maintained throughout the duration of a DOS or DDoS attack.

8.2 The function in Article 8.1 involves monitoring the traffic sent to the Customer's Services from outside the Supplier's network. The traffic identified as illegitimate shall then be rejected by the Supplier prior to reaching the Customer's Infrastructure, thus allowing legitimate users to access the applications offered by the Customer in spite of the attack.

8.3 As a result of the high technicality of the Service, certain attacks may not be detected by the protection measures implemented by the Supplier. The protection measures outlined in Articles 8.1 and 8.2 shall not apply in the case of attacks such as SQL injection, brute-force, abuse of security vulnerabilities, or attacks of a similar nature to the latter. In such cases, the Infrastructure and the Service may be temporarily suspended and unavailable.

8.4 Given the nature of a potential DOS or DDoS attack and their complexity, the Supplier shall implement different levels of traffic protection in order to preserve their Infrastructure and the Services.

8.5 The mitigation of a DOS or DDoS attack is activated only at the time of the detection of the attack by the Supplier's tools and for a non-fixed period, and deactivated only once the attack and illegitimate traffic are no longer present. Thus until the mitigation is activated, the Service shall handle the attack directly, which may lead to the temporary unavailability of the Service.

8.6 While mitigation is activated, the Supplier shall not guarantee the accessibility of the Customer's applications but it shall endeavour to limit the impact of a DOS or DDOS attack on the Customer's Services and on the Supplier's Infrastructure.

8.7 If, in spite of the activation of mitigation, a DOS or DDOS attack is of such a nature as to adversely affect the integrity of the Supplier's Infrastructure or the infrastructure of the other customers of the Supplier, the Supplier shall strengthen its protection measures which may lead to the deterioration of the Customer's Services or impact its availability for which the Supplier shall not be liable.

8.8 Where part of the traffic generated by a DOS or DDOS attack is not detected by the Supplier's equipment and reaches the Customer's Services, the effectiveness of the mitigation shall also depend on the appropriate configuration of the Customer's Services. In this regard, the Customer must ensure that it has the adequate resources to administer the configuration of the Customer's Services properly.

8.9 The Customer shall be solely responsible for ensuring it secures its Services, implementing security tools (firewall, etc.), periodically updating their system, backing up their data and for ensuring the security of their software (scripts, codes etc.).

ARTICLE 9: GEOLOCATION

9.1 At the time of the creation of the Instance, an Object Storage Container or Archive Storage, the Customer chooses where they wish to locate their Service, from the available datacentres.

9.2 The Customer acknowledges and accepts that they are also subject to the legislation applicable on the territory where their hardware is installed and data is stored.

9.3 The Customer therefore acknowledges the ability of the Supplier to suspend the Service should it be used for a prohibited activity in the physical location of the hardware provided by the Supplier.

9.4 Similarly, regarding geolocated IP addresses, the Customer undertakes to ensure that they do not use the Service to breach legislation applicable in the country for which the IP address is declared. If the Customer uses the Service in this way, the Supplier may be forced to suspend every one of the Customer's geolocated IP addresses.

ARTICLE 10: SNAPSHOTS

10.1 The Supplier provides a feature enabling the Customer to make "instantaneous" copies (or "Snapshots") of the Instance.

10.2 The Supplier reminds the Customer that a Snapshot is not a perennial backup of the data of the Instance. It is rather an "instantaneous" copy of the Instance. As a result, a Snapshot does not, under any circumstances, exempt the Customer from its obligation to back up their data in accordance with Article 6 in this contract.

10.3 By default, Snapshots are of unlimited duration and invoiced under the conditions set out below in Article 13.

10.4 The Customer may restore their Instance from any Snapshot. In this case, any data on the Instance will be deleted and the data on the selected Snapshot will be restored.

ARTICLE 11: SERVICE LEVEL AGREEMENT (SLA)

11.1 The Supplier shall use its reasonable endeavours to meet the following Service level targets:

(a) CLOUD Instances:
Monthly availability rate: 99.999%

(b) VPS-CLOUD Instances:
Monthly available rate: 99.99%

(c) VPS-SSD Instances:
Monthly available rate: 99.95%

(d) Object Storage Containers:
Monthly availability rate: 99.9%
Monthly resilience rate of data: 100%.

"Monthly availability rate" means the total number of minutes in the month minus the number of minutes of Unavailability in the month in question, divided by the total number of minutes in the month in question.

"Unavailability" means the loss of access to the Customer's Object Storage Container, or the loss of connectivity to the Customer's active Instance, for more than three (3) consecutive minutes. The Supplier implements ARP PING (Address Resolution Protocol), monitoring requests to establish loss of connectivity. The Supplier calculates the downtime from the moment an incident ticket has been opened by the Customer. If due to some configurations made by the Customer on its Instances, the Supplier is not able to realise the above monitoring techniques to check the availability of Services, the commitment of availability set out above shall not apply.

"Resilience" means the capacity of the Supplier to again provide the Customer with access to the data that was stored in the Object Storage Container prior to an incident of unavailability that has been duly notified (see the following conditions). The resilience commitment only applies to the Object Storage Service, to the exclusion of other Storage offered by the Supplier within the Supplier's Public Cloud Service. The Supplier's resilience commitment is under no circumstances a guarantee to the Customer against the loss of their contents and data. The Customer remains responsible for their data backup and business continuity as stated in article 6.6 above.

The Service level targets described above are in place; subject to the exclusions listed below and provided that the Customer works with the Supplier, in the event of unavailability, to restore the Service as described as follows.

In the event of unavailability, the Customer shall declare the incident and shall provide the Supplier with all relevant information useful for the diagnosis and intervention by the Supplier. The Customer undertakes to remain constantly available in order to collaborate with the Supplier including by providing further information and carrying out all the necessary tests and checks. If necessary, the Customer agrees to give access to its Management Interface. If the Customer is not available or does

not cooperate with the Supplier, it cannot benefit from the Service level targets defined.

The above commitment does not under any circumstances apply to the availability of components that are under the responsibility of the Customer, in particular the software or applications installed and used by the Customer on the Instance. In the event of a change of Instance following an incident, the Customer is responsible for reinstalling or reinitialising their software and applications, and restoring the data and information that were stored on it.

11.2 If The Supplier ascertains that the Instance or Object Storage Container is available and fully operational, the Supplier shall be absolved of this SLA. However, under these circumstances, the Supplier, at the request of the Customer, undertakes to assist the Customer in identifying the source of any difficulties found by the Customer.
If the Supplier ascertains an Unavailability, it will complete the diagnostic and work in collaboration with the Customer to re-establish availability.

11.3 If the Service level targets defined above in Article 11.1 are not achieved, the Customer may, apart from the cases of exclusion numbered below, request the following Service credits:

· Non-compliance with availability rate:
Credit equal to 0.5% of the monthly fee paid for the month concerned by the Customer for the unavailable components (Instances or Object Storage Containers) per consecutive sequences of one (1) minute (beyond the first three (3) consecutive minutes of lost access or connectivity), up to a maximum of 50% of the monthly amount for Instances and up to 100% of the monthly amount invoiced with respect to the said unavailable Object Storage Containers

· Non-compliance with data Resilience rate (Object Storage Containers):
Credit equal to 100% of the monthly fee, for the month in question, paid by the Customer for the affected Object Storage Container components.

The funds are credited directly to the Supplier account belonging to the Customer, on The Customer's request. The Customer must make their request in their Management Interface, in the month following the month in which the Supplier recorded the downtime. Otherwise, the Customer is no longer able to obtain such compensation. The credit must be used by the Customer under the Public Cloud Service in the calendar month following the month when they were credited to the Supplier account belonging to the Customer. Otherwise, the credit is lost and cannot be used. Credit can under no circumstances be refunded to the Customer in cash.

It is expressly agreed that the aforementioned Service credits are the Customer's sole remedy for all damages, losses, liabilities, costs and expenses resulting from the Supplier's failure to comply with its obligations. As such, the Customer will renounce any further requests, claims and/or action.

If an event leads to the failure of several Service level agreements, the credits cannot be combined. The Customer will receive the most favourable credit amount.

11.4 The Customer may not claim for aforementioned Service credits where the unavailability or Resilience breach results, in whole or in part from (i) events or factors beyond control of the Supplier, including but not limited to events of force majeure, actions of a third-party, internet connection issues, the malfunction of the internet, the malfunction or misuse of hardware or software under the control of the Customer (in particular applications running on the Instance), (ii) a breach of the obligations of the Customer pursuant to this Contract (in particular failure to collaborate with the Supplier to resolve the incident), (iii) the misuse or inappropriate use of the Service by the Customer (in particular the misuse of the Instance or the Supplier Management Interface), (iv) scheduled maintenance, (v) an interruption caused by the Supplier's intervention under the Conditions set out in Article 6 of this document, or (vi) computer hacking or piracy.

In such cases, excluding point (iv), the Supplier reserves the right to invoice the Customer for the cost of the work done to re-establish the availability of the Services. The Supplier shall provide a quotation for such work, which shall be sent to the Customer for approval.

The Supplier shall use all reasonable endeavours to establish the cause of the unavailability, and confirm which exclusion set out above applies. The Supplier shall be permitted to use components in its information system (such as connection data) for this purpose.

ARTICLE 12: DURATION OF CONTRACT AND SERVICE

12.1 The Contract shall commence from the date it is subscribed to by the Customer, and shall remain in force for an indefinite period. It may be terminated in accordance with the Supplier's general terms and conditions.

12.2 The Customer may choose, based on their requirements, to create and delete all or part of the Service (in particular Instances and Object Storage Containers and Archive Storage) via their Management Interface.

12.3 There is no minimum duration of use. However, any hour or month started shall be invoiced by the Supplier and paid in full by the Customer, in accordance with the conditions set out in Article 13 below.

12.4 Instances, Object Storage Containers and Archive Storage on which the data of the Customer is stored shall remain available from month to month, unless the Customer requests the deletion of the Service via the Management Interface.

ARTICLE 13: PRICES, PAYMENT METHODS AND BILLING

The prices are available at http://www.ovh.co.uk. These prices are quoted in pounds sterling and exclusive of VAT.

13.1 Instances and associated components

The price of Instances and, where necessary, associated components (such as the operating system, Storage Space) depends on the pricing model chosen by the Customer and the period during which the Instances and associated components are provided to the Customer.

The Customer may choose from two pricing models:

- An hourly payment plan
- A fixed-rate monthly payment plan

The fixed-rate monthly payment plan allows the Customer to use an Instance (and where necessary the associated components) during the full calendar month during which the Instance was created.

If the Customer creates an Instance during the month, the aforementioned fixed-rate monthly payment plan shall be invoiced on a pro-rata basis for the number of hours that remain in the month, starting from the date of creation of the Instance to the end of the month in question. The hour of creation of the Instance is counted as a full hour.

The fixed-rate monthly payment plan (in full or on a pro-rata basis under the conditions detailed above) shall be paid in full by the Customer. This also applies where the Instance is deleted before the end of the calendar month in question. Any component (Instance and associated components) that is invoiced at the fixed-rate monthly payment plan and not deleted shall continue to be invoiced from month to month by the Supplier to the Customer at the fixed-rate monthly rate that applies in the above conditions.

With regards to the hourly payment plan, any hour started shall be invoiced by the Supplier and paid in full by the Customer. This also applies where the Instance is created and/or deleted during the same hour.

Any created Instance (including any associated components) is invoiced to the Customer in accordance with the conditions set out in this Contract, even if the Instance is not used. An Instance, including any associated components, is deemed to be created as soon as the Customer validates it in the Management Interface or the API. Once it is created, it will appear in the Management Interface. The provision of the Instance will come to an end once it is deleted. It shall be stated that any Instance that has been deactivated but not deleted shall continue to be invoiced by the Supplier. The status of the Instance may be seen in the Customer's Management Interface.

13.2 Object Container Storage and Archive Storage

The price of using distributed Storage Spaces (Object Storage Containers, Archive Storage and SNAPSHOT Storage Space) varies depending on the quantity of Storage Space used, duration of use of the Storage Space and the volume of incoming and outgoing traffic.

With regards to the provision of the Storage Space:

Storage Space shall be charged on hourly rate basis, charged per gigabyte.

The gigabyte of Storage Space is always charged as a whole, even if it is not fully used (rounded to the superior gigabyte).

Any hour during which a gigabyte of Storage Space is used, is charged and due in full by the Customer, even if the use of a gigabyte of Storage Space starts and/or is deleted during the hourly time slot.

With regards to Storage Space's incoming and outgoing traffic

The Supplier shall charge for this on a pay-per-use rate, charged per gigabyte of incoming and outgoing data. "Gigabyte of incoming data" means gigabyte of data received from the Storage Space, whatever its origin (from the internet and/or the network of the Supplier and/or a third-party private network).
"Gigabyte of outgoing data" means gigabyte of data sent from the Storage Space, whatever its destination (towards the internet and/or the network of the Supplier and/or a third-party private network).

Any incoming or outgoing traffic resulting query is charged, except for an HTTP error. The queries are free.

Notwithstanding the foregoing, the traffic entering the Object Storage Containers is not charged to the Customer.

The provision of the "local" Storage Space (directly attached to the Instance) and the incoming and outgoing traffic sent from the "local" Storage Space is included in the price of the Instance.

13.3 General Information

The Customer may create and delete Instances via the Management Interface. Where several payment plans exist, the applicable rate is determined by the Customer in the Management Interface at the moment of creation of the component concerned (for example the creation of an Instance).

Where the fixed-rate monthly payment plan is applied, the Service shall be invoiced for the remainder of the calendar month a few moments after the creation by the Customer of the component (Instance and associated components).

Where the hourly payment plan or pay-per-use is applied, the Services shall be invoiced on a monthly basis in arrears at the start of the calendar month that follows the month of use, based on the consumption evaluated by the Supplier. The Supplier reserves the right to invoice the cost of these Services to the Customer before the end of the said calendar month of use in the event that the Services used by the Customer reach a significant total amount during the calendar month.

The provisioning time is evaluated by the Supplier based on the data available on its operating system. The data is considered binding and fully enforceable on the Customer.
The payments shall be made by the Customer three (3) days from the invoice date, by automatic transfer from the Customer's credit/debit card, Paypal® account or Customer's Supplier Account.

The Customer undertakes to always retain a sufficient amount, in the bank account and their chosen payment method, to pay for their invoices within the agreed deadlines.

If the Supplier is unable to take payment from the payment method, an email shall be sent to the Customer requesting settlement of the outstanding amount as soon as possible. In the absence of prompt payment, the Service will be suspended by the Supplier for non-payment.

ARTICLE 14: TERMINATION, LIMITATION AND SUSPENSION OF SERVICE

14.1 Each party may terminate the Contract without liability to the other party in an event of force majeure as stated in the Supplier General Terms and Conditions.

14.2 In other cases, the Customer is free to terminate the Contract upon 30 days' notice by sending a termination request in writing via the Management Interface, by using the contact details available on the Supplier website or to the following address: OVH LTD New London House LONDON EC3R 7LP.

14.3 In all cases where the Customer breaches the provisions of Article 6 in these special terms and conditions, particularly by carrying out any expressly prohibited activity using the Supplier's servers and/or publishing expressly prohibited content on the Supplier's servers and/or any activity that could potentially give rise to civil and/or criminal liability and/or affect the rights of third parties, the Supplier has the right to disconnect and/or interrupt the Customer's services immediately and without prior notification and to terminate the Contract with immediate effect and without notice to the Customer, without prejudice to the right to damages that the Supplier may claim.

14.4 Under the terms of this Contract, in the event of termination under Article 14.3 and regardless of the reason for termination, the Customer's Instances, Object Storage Containers and any associated components and stored data shall be deleted.

14.5 In the event of any Customer breach and where the Supplier elects not to terminate for breach, Services will be either restricted, limited or suspended depending on the gravity and the frequency of the breach. The measures will be determined based on the nature of the breach(es) established.

14.6 The Customer accepts in advance that the Supplier shall implement restriction, limitation or suspension measures of the Service where the Supplier receives a notification accordingly from a competent administrative, arbitration or judicial authority, pursuant to the appropriate applicable laws.

BY PLACING AN ORDER ONLINE, THE CUSTOMER SIGNIFIES THEIR UNCONDITIONAL ACCEPTANCE OF THIS CONTRACT. If the Customer has any questions after reading this contract, they should contact the Supplier at New London House 6 London Street London EC3R 7LP.