ARTICLE 1: PURPOSE

These Special Conditions supplement the So You Start General Conditions (the “General Conditions”) and are intended to set out the technical and financial conditions under which the Supplier will provide to the Customer the So You Start dedicated server on its platform.

The Customer expressly acknowledges that save as expressly provided under these Special Conditions, the Supplier has had and shall have no involvement in the design, development, creation or implementation of the Customer's website(s) and the Customer’s IT management and administration tools.

In the event of a conflict between these Special Conditions and the General Conditions of Service, these Special Conditions shall prevail.

ARTICLE 2: RESOURCES

The So You Start server platform on which the Customer's dedicated server will be installed is accessible to the general public by way of stations connected to the internet.

Throughout the period of renting the dedicated server to the Customer, the Supplier shall provide the Customer with access to a forum, which the Customer may use to obtain technical advice.

ARTICLE 3: CONDITIONS OF SERVICE IMPLEMENTATION

The Supplier will inform the Customer by email when their dedicated server has been made available. The Supplier shall invoice the Customer from the date on which the dedicated server is put online.

The server will be made available to the Customer after the Supplier has validated payment from the Customer and not more than 7 days from the date on which the Supplier receives the sums.

If the Supplier does not provide the Customer with access to the server within 7 days of receipt of the sums due, the Customer may request cancellation of the transaction and a refund of the sums already paid.

The server rented to the Customer shall remain the property of the Supplier. Any server rented from the Supplier will have a fixed IP address.

The technical specifications of the Service are detailed on the https://www.soyoustart.co.uk website.
The Customer is the administrator of the server rented from the Supplier. The Customer may install software applications on the server themselves. In this instance, they accept full responsibility for carrying out these installations, and the Supplier shall not be liable for any malfunctioning of the server in relation to these installations.

ARTICLE 4: SUPPLIER'S OBLIGATIONS

The Supplier shall provide the Service with all reasonable care and diligence in accordance with customary professional practices. The Supplier undertakes to:

4.1 use reasonable endeavours to maintain the Service in good working order. In the event of failure of the hardware rented to the Customer after creation of an incident ticket, the Supplier shall replace the defective part as soon as reasonably practicable. This provision shall not apply in relation to any failure for which the Supplier is not responsible, or any other intervention requiring an interruption or suspension of the Service for a period exceeding the usual replacement times. The Supplier shall inform the Customer immediately if the Supplier does not expect to be able to repair or replace the malfunction in the usual replacement times;

4.2. use reasonable endeavours to ensure that the server's connection to the network via the internet is available 24hours a day, every day of the year provided that the Supplier may suspend the servers connection to the network in order to carry out a technical review of the devices on the Supplier network;

4.3. use reasonable endeavours to promptly rectify any incident upon receipt of a request from the Customer provided that the incident has not arisen as a result of any misuse of the server by the Customer; and

4.4. use reasonable endeavours to ensure that its resources comply with good quality standards at all times, in accordance with industry rules and practices.

ARTICLE 5: SUPPLIER'S LIABILITY

The Supplier reserves the right to suspend the internet connection for the server rented to the Customer if the server poses a threat to the security maintenance of the Supplier platform, whether resulting from hacking of the said server, the detection of a security system loophole, or the need to update the server.

The Supplier shall inform the Customer as soon as reasonably practicable if any maintenance, repair or upgrade requires the server to be suspended, and of the likely duration of such suspension, so that the Customer may take appropriate measures. The Supplier shall inform the Customer by email as soon as reasonably practicable if any maintenance, repair or upgrade requires the Dedicated Hosting Services to be suspended and shall inform the Customer of the likely duration of such suspension. The Supplier shall use reasonable endeavours to restore the connection as soon as the issue has been resolved.
In addition, the Supplier shall not be held liable for the content of the information, sound, text, images, shapes and forms and data accessible via the websites hosted on the Customer's server, transmitted or uploaded by the Customer, in any respect whatsoever.

The Supplier shall have no liability to the Customer under the General and Special Conditions in the event of any interruption, suspension or partial or total failure of the server due to any variation of the bandwidth or any failure of the Supplier’s ISP/Access Provider.

ARTICLE 6: OBLIGATIONS AND LIABILITY OF THE CUSTOMER

6.1 The Customer is acting as an independent entity and, as such, accepts full responsibility for all risks and liabilities of their activity. The Customer is solely responsible for the services and internet websites hosted on the dedicated server, its content, use and the updating of information transmitted, distributed or collected and of all files, especially address files. The Customer specifically undertakes to respect the rights of any third parties, especially intellectual property rights such as copyrights, patent rights or trademarks. Therefore, the Supplier shall not be liable for the content, usage or updating of any information transmitted, distributed or collected and of all files, especially address files, in any respect whatsoever.

The Supplier can only warn the Customer of the legal consequences that may arise from illicit activities on the server, and does not accept any responsibility regarding the Customer’s use of the data made available to internet users.

The Customer shall not undertake or attempt to undertake, any intrusive web activities whatsoever through the server, such as, without limitation, port scanning, sniffing and spoofing.

In such situations, the Customer will not be able to claim any reimbursement from the Supplier for amounts already paid.

6.2 The Customer shall be solely liable for the consequences of any malfunctioning of the server resulting from any use by their personnel, or any person to whom the Customer has supplied their password/s. The Customer shall be solely liable for the consequences of losing the above mentioned password/s.

6.3 In order to maintain the security level of the Customer's server and all servers present on its platform, the Supplier shall inform the Customer, by email or via the Supplier Website, of the availability of updates to the operating systems maintained by the Supplier, for which a security fault has been raised. If the update of these applications is not carried out according to the Supplier requests, the Supplier reserves the right to suspend or terminate the server's connection to the internet.

In the event of the Supplier detecting that the Customer's machine has been hacked, an email will be sent to the Customer, indicating that a reinstalation procedure is essential in order to maintain the integrity of the server and the entire platform. The Customer may then carry out the reinstalation procedure via their management Interface, after having made a backup of all of

OVH LIMITED 3 Southwark Street LONDON SE1 1RQ
Registration number: 5519821 – VAT number GB 918 7594 74
their data. The Supplier may suspend the server's connection to the internet, pending installation of the new machine. The Customer shall be responsible for carrying out any transfers of the data from the hacked system to the new system. Any intervention carried out by the Supplier shall be limited to installation of the new system only.

6.4 For security reasons, the Supplier reserves the right to suspend any server without giving notice to the Customer, in relation to which there is a public service Proxy, IRC, VPN or TOR which is available free of charge or for a fee, and which the Supplier knows has been subject to fraudulent or illegal misuse.

6.5 The Customer shall be responsible for taking all the necessary measures to back up its data stored using the Supplier’s server.

6.6 In the event that the Customer does not pay any licence or subscription fees when they become due to the Supplier or any third party, the Supplier reserves the right to suspend the Services without prior notice.

6.7 The Supplier reserves the right to carry out checks to ensure that the Customer’s use of the Service is in compliance with these Special Conditions.

The Supplier reserves the right to suspend the Services without prior notice, and to terminate the server agreement:

i) Where, in the Supplier’s reasonable opinion, the Customer’s server poses a significant risk to the Supplier’s infrastructure;

ii) in the event of any non-compliance by the Customer of the Special and General Conditions; or

iii) in accordance with any applicable statutory and regulatory provisions, and pursuant to any contract it has with any third party.

6.8 The Customer is reminded that any intervention by the Supplier of the Customer’s dedicated server is limited to the installation of the server. For this reason, the Supplier only provides rental of the specialised infrastructure and does not assume any control over the contents of the websites hosted or the contractual relationship of the editors of these sites and their hosting provider, or the Customer under the dedicated server rental contract. In relation to the Customer’s server, the Customer shall be a hosting provider and shall retain and preserve any data that will enable the identification of any third party who contributes to the content creation or to one of the contents of the services that he provides, for a period of 12 months, without engaging the liability of the Supplier in this respect.

The Customer shall implement an easily accessible and visible structure that enables any person to notify it of any offence or potential offence whatsoever that may have occurred on any website or contained in any data transmitted across the server network, including, but not limited to, data which constitutes incitement to racial hatred, child pornography, incitement to violence, violation of human dignity or illicit gambling activities. The Customer shall ensure that all required notices...
are set out on the website and that it is clear that the Customer is the hosting service provider in any legal notices presented by their contracting parties on their So You Start server.

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

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

The Supplier shall monitor outgoing traffic from the Server towards port 25 (SMTP server) on the internet, which shall involve monitoring traffic by means of automatic tools.

The Supplier shall not tag any 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.

The operation 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).

The Supplier shall inform the Customer by email in respect of any outgoing traffic from the Customer’s server, including e-mails which the Supplier identifies as spam or fraudulent e-mails. In the event that the Supplier identifies any such outgoing traffic, the Supplier shall block the Server’s SMTP port.

The Supplier shall not keep any copy of e-mails sent from the Server’s SMTP port, even when they are identified as spam.

The Customer must request unblocking of the SMTP port by the So You Start Technical Assistance.

Whenever a new email is identified as spam the SMTP port will be blocked again for a period of time to be determined at the Supplier’s reasonable discretion. In the event that the SMTP port is blocked 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)

The Supplier shall implement protection against DOS (Denial of Service) and DDOS-type hacking attempts in the event that such attacks are reasonably considered by the Supplier to be
serious enough 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.

This function 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.

The protection measures shall not apply in the case of attacks such as SQL injection, brute-force, abuse of security flaws or other types of attack that the Supplier considers are similar. The Supplier shall take all reasonable care and diligence to protect the Service and the Customer acknowledges that the tools installed may not detect the attack and may not enable service operations to be maintained.

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 its infrastructure and the Services.

Once the attack is identified and mitigation is automatically activated by the Supplier, mitigation shall not be deactivated for a period of 26 hours. The Customer acknowledges that the Services may be unavailable immediately following the attack and until the mitigation is activated.

The Supplier shall not guarantee the accessibility of the Customer’s applications but it shall use reasonable endeavours to limit the impact of a DOS or DDOS attack on the Customer’s Services and on the Supplier’s infrastructure.

If, in spite of mitigation, a DOS or DDOS attack adversely affects, or the Suppliers reasonably believes could 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. The Supplier shall not be liable in respect of any losses caused as a result of any deterioration of the Customer’s Services or any impact on the availability of the Service.

Where traffic or part of traffic generated by a DOS or DDOS attack reaches the Customer’s Services, the effectiveness of the mitigation shall also depend on the appropriate configuration of the Customer’s Services. The Customer shall at all times ensure that it has correctly administered the configuration of the Customer’s Services.

The Customer shall be solely responsible for ensuring its Services are secure and shall implement security tools (firewall, etc.), update its system from time to time, back up its data and ensure the security of their software (scripts, codes etc.).