

Laatste versie gedateerd 05/12/2013

ARTIKEL 1: ONDERWERP

Deze bijzondere voorwaarden vormen een aanvulling op de Algemene Voorwaarden van de “Dienst So you Start”, om de technische en financiële voorwaarden te bepalen waarop OVH zich verbindt om de Dienst dedicated server “So you Start” te verhuren op het platform van OVH, aan de Klant. De Dienst dedicated server So you Start wordt nader in deze voorwaarden de Dienst genoemd.

De Klant erkent uitdrukkelijk dat OVH geen enkele betrokkenheid heeft voor het ontwerp, de ontwikkeling, de uitvoering en de inbedrijfstelling van het internetsite door de Klant en zijn IT-managementtools en de administratie-tools.

Deze bijzondere voorwaarden prevaleren boven de algemene voorwaarden als er een conflict ontstaat tussen deze twee documenten.

ARTIKEL 2: MIDDELEN

Het server platform So you Start wordt geïnstalleerd op de dedicated server van de Klant die deze heeft in het kader van de Dienst en is toegankelijk voor het grote publiek via het internet door middel van stations aangesloten op het internet.

Gedurende levering van de Dienst aan de Klant, biedt OVH de Klant toegang tot een forum, waarop de klant technisch advies kan ontvangen.

ARTIKEL 3: VOORWAARDEN LEVERINGSPRESTATIES

OVH zal de Klant via e-mail op de hoogte houden over de beschikbaarheid van de Dienst. Het effectieve online gaan van de Dienst bepaalt de aanvangstdatum van de verschuldigdheid van de vergoeding voor de Dienst.

De dedicated server wordt beschikbaar binnen een termijn van maximaal 7 dagen vanaf de effectieve betaling van de bestelling van de Dienst door de Klant. De dienst wordt derhalve vooruit gefactureerd.

Na deze periode, indien OVH in gebreke blijft inzake het verstrekken van de dedicated server, is de Klant gerechtigd tot annulering van de transactie en de terugbetaling van de reeds door OVH ontvangen bedragen.

De dedicated server die verhuurd is aan de Klant, blijft eigendom van OVH. Alle dedicated servers verhuurd door OVH hebben een vast IP-adres.

De technische kenmerken van de Dienst worden vermeld op de site <https://www.soyoustart.com>.

De Klant is de Beheerder van de door OVH verhuurde server. Hij heeft de mogelijkheid om zelf softwaretoepassingen te installeren op de server. Deze faciliteiten zijn onder zijn uitsluitende verantwoordelijkheid, en OVH kan niet verantwoordelijk worden gehouden voor een storing als gevolg van deze server installaties.

ARTIKEL 4: VERPLICHTINGEN VAN OVH

OVH verbindt zich de inspanning te leveren die nodig is voor een goede Dienst in overeenstemming met de gebruiken van haar beroep en de stand van de techniek. OVH verbindt zich:

4.1. Tot onderhoud, zodat de apparatuur blijft functioneren. In geval van storing van aan de Klant verhuurde apparatuur, geïdentificeerd na het aanmaken van een incident-ticket, verbindt OVH zich het defecte onderdeel zo snel mogelijk te vervangen tenzij het falen niet aan OVH is te wijten, of het falen een zodanige handeling vereist die een onderbreking van de Dienst voor een langere dan de gebruikelijke tijd voor vervanging noodzakelijk maakt. In de laatste gevallen, doet OVH onmiddellijk mededeling aan de Klant.

4.2. tot het waarborgen van de netwerkverbinding via internet 24/7, elke dag van het jaar. OVH behoudt zich het recht voor om de netwerkverbinding van de server te onderbreken om technisch onderhoud op het netwerk-apparatuur van het OVH netwerk uit te voeren.

4.3. Snel te reageren in geval van een niet-openvolgend incident van misbruik/slecht gebruik van de server door de Klant op aanvraag voor interventie van de Klant.

4.4. tot handhaven van het hoogste kwaliteitsniveau van zijn tools in overeenstemming met de stand van de techniek en de gebruiken van zijn beroep.

ARTIKEL 5: AANSPRAKELIJKHEID VAN OVH

OVH behoudt zich het recht voor om de verbinding van de aan de Klant verhuurde server met het internet te onderbreken, als de server een gevaar is voor de handhaving van de veiligheid van het OVH platform, hetzij als gevolg van het hacken van de server, of na de ontdekking van een fout in het beveiligingssysteem, of een noodzaak om de server te updaten.

OVH zal zo vroeg mogelijk de Klant op de hoogte stellen en de Klant binnen een redelijke termijn hem informeren over de aard en de duur van de interventie, zodat de Klant voorzorgsmaatregelen kan nemen. OVH verbindt zich om de verbinding te herstellen, zodra eventueel noodzakelijke correctie procedures zijn uitgevoerd door de Klant .

OVH kan niet aansprakelijk worden gesteld voor de informatie, geluid, tekst, afbeeldingen, vormelementen of gegevens beschikbaar gesteld, gehost, verstrekt of geüpload door de Klant op de gehoste websites op de server van de Klant, om welke reden dan ook.

OVH is niet aansprakelijk voor de gehele of gedeeltelijke niet-nakoming van een verbintenis en/of falen van de providers van transmissie-netwerken in de internetwereld en in het bijzonder zijn of haar internetproviders.

ARTIKEL 6: VERPLICHTINGEN EN AANSPRAKELIJKHEID VAN DE KLANT

6.1 De Klant fungeert als een onafhankelijke entiteit en is aansprakelijk voor alle risico's en gevaren van zijn activiteit. De Klant is als enige verantwoordelijk voor de Diensten en websites gehost op zijn dedicated server, de inhoud van de informatie die verzonden, verspreid of verzameld wordt, exploitatie en updates van de informatie, alle bestanden, inclusief mailinglijsten. De Klant verbindt zich om de rechten van anderen, met inbegrip van persoonlijkheidsrechten, intellectuele eigendomsrechten van derden, zoals auteursrechten, octrooirechten of handelsmerken te respecteren. Dienovereenkomstig kan OVH niet aansprakelijk worden gesteld voor de inhoud van de verzonden, verspreide of verzamelde informatie, hun werking en updates, en alle bestanden, inclusief mailinglijsten en soortgelijks, in welke hoedanigheid dan ook .

OVH kan de klant slechts waarschuwen inzake de juridische gevolgen die kunnen voortvloeien uit illegale activiteiten op de server, en distantieert zich van alle hoofdelijke aansprakelijkheid op het gebruik van de gegevens, online ter beschikking gesteld door de Klant.

De Klant verbiedt en – voor zover mogelijk - voorkomt eveneens elke inbraak of poging tot inbraak van de server (zoals, maar niet beperkt tot: port scanning, sniffing, spoofing).

Mochten de hiervoor omschreven gevallen zich onverhoopt voordoen, dan heeft de Klant geen recht op terugbetaling van de reeds aan OVH betaalde bedragen.

6.2 De Klant draagt alleen de gevolgen van een storing van het functioneren van de server volgend op elk gebruik, door haar personeel of elke persoon aan wie de Klant zijn (of haar) wachtwoord (en) heeft verstrekt. Op dezelfde manier, draagt de Klant als enige de gevolgen van het verlies van of de wachtwoorden hierboven.

6.3 Om de veiligheid van de server van de Klant en alle servers op het platform te handhaven, verbindt OVH zich om de klant te verwittigen, via e-mail en of via de OVH site, de beschikbaarheid van updates van door OVH onderhouden besturingssystemen, waarvoor een veiligheidslek is geïdentificeerd. Als de update van deze toepassingen niet is gedaan na verzoeken van OVH, behoudt OVH zich het recht voor om de serververbinding met het internet te beëindigen.

Als OVH detecteert dat de machine van de Klant wordt gehackt, wordt een e-mail verstuurd naar de klant, die aangeeft dat een herstelproces noodzakelijk is om de integriteit van de server en het platform te behouden. De Klant kan dan deze procedure uitvoeren door middel van haar management interface, na het opslaan van alle gegevens. OVH behoudt zich het recht voor om de serververbinding met het internet te onderbreken, in afwachting van de herinstallatie van de machine. OVH is niet verplicht om de gegevensoverdracht van het gehackte systeem naar het nieuwe systeem uit te voeren, deze operatie moet worden uitgevoerd door de Klant zelf. OVH verbindt en beperkt zich slechts tot de interventie van de installatie van het nieuwe systeem.

6.4 Om veiligheidsredenen, behoudt OVH zich het recht voor om over te gaan tot de onmiddellijke onderbreking van de Dienst, zonder voorafgaande kennisgeving, in geval van enige dedicated server die gratis of tegen betaling wordt aangeboden voor gebruik als een open publieke Proxy, IRC, VPN of TOR dienst alsmede in geval OVH kennis krijgt van misbruik, fraude of onwettig gebruik.

6.5 Het is aan de Klant om alle nodige maatregelen te nemen om de gegevens opgeslagen middels of in de Dienst althans dedicated server te beschermen.

6.6 Het is aan de Klant om een licentie of recht van gebruik aan te gaan met OVH of een derde ter zake van de software aanwezig op de dedicated server. Standaard behoudt OVH zich het recht voor om de Dienst op te schorten zonder voorafgaande kennisgeving, indien gebruik wordt gemaakt van niet gelicentieerde software.

6.7 OVH behoudt zich het recht voor om controle uit te voeren inzake de naleving van deze bepalingen inzake het gebruik door de Klant van de Dienst .

OVH behoudt zich het recht voor om de dienst op te schorten zonder voorafgaande kennisgeving, en over te gaan tot beëindiging van de huurovereenkomst van de dedicated server als het handhaven van de Server van de Klant te veel risico inhoudt voor de OVH-

infrastructuur, of bij niet-naleving door de Klant van de bijzondere en algemene OVH voorwaarden en, in het algemeen, van alle wet-en regelgeving, alsmede de rechten van derden.

6.8 De Klant wordt eraan herinnerd dat de Dienst slechts de installatie en het geven van toegang van en tot de dedicated server omvat. OVH waarborgt slechts verhuur van een gespecialiseerde infrastructuur, zonder controle over de inhoud van gehoste sites of de contractuele relatie met de uitgevers van deze sites met hun host, Klant van OVH onder de titel verhuurcontract dedicated server.

De Klant moet dan ook worden beschouwd als een zelfstandige host, die zelfstandig voorziet in de levering aan het publiek van online communicatiediensten, het opslaan van signalen, geschriften, beelden, geluiden of boodschappen van welke aard dan ook die door de ontvangers van deze diensten. De Klant behoort zich dan ook te houden aan alle vereisten die de wet stelt aan een host, zonder dat OVH aansprakelijk kan worden gesteld in dit verband.

ARTIKEL 7 : MAATREGELEN OM HET VERSTUREN VAN SPAM TE BESTRIJDEN OP HET OVH NETWERK

OVH heeft een systeem van technische maatregelen ingesteld in de strijd tegen het verzenden van frauduleuze e-mails evenals tegen SPAM verzonden vanaf haar infrastructuren.

Daartoe voert OVH een controlemaatregel op dataverkeer verzonden vanaf de server die wordt gebruikt door de Klant van port 25 (SMTP-server) op het internet. Dit is om het dataverkeer te controleren door middel van automatische tools.

Zendingen worden noch gefilterd noch onderschept maar gecontroleerd met een vertraging van een paar seconden. Deze handelingen worden parallel uitgevoerd en in geen geval frontaal tussen de server en het internet.

Deze handelingen beïnvloeden de verzonden e-mails niet: OVH bewerkt geen gemarkeerde (tag) e-mails, en wijzigt op geen enkele manier de e-mails van de Klant. OVH slaat geen informatie op tijdens deze activiteiten afgezien van statistische gegevens.

Dit wordt regelmatig en volledig automatisch gedaan. Het controleren van het verkeer naar port 25 (SMTP-poort) wordt zonder menselijke tussenkomst uitgevoerd.

Indien verstuurde e-mails vanuit de server van de Klant als spam of frauduleus worden aangemerkt, zal OVH de Klant op de hoogte stellen via e-mail en de SMTP-server port blokkeren.

OVH bewaart geen kopieën van e-mails verzonden vanaf de SMTP-server port, zelfs niet als ze worden geïdentificeerd als SPAM.

In het geval van blokkering van de SMTP-port, moet de klant contact opnemen met de technische ondersteuning So you Start en om deblokkering vragen.

Elke nieuwe e-mail geïdentificeerd als spam zal resulteren in een nieuwe blokkering van de SMTP-port voor een langere duur.

Bij de derde blokkering, behoudt OVH zich het recht voor om nieuwe verzoeken om de SMTP-port te deblokken te weigeren.

ARTIKEL 8: BESCHERMINGSSERVICE (BESCHERMING TEGEN DOS-EN DDOS-AANVALLEN)

OVH heeft beveiliging tegen DOS-en DDOS-computeraanvallen (Denial of Service) geïmplementeerd, welke beveiliging ingeschakeld kan worden bij massale aanvallen. Deze functie is bedoeld om de verdere werking van de Dienst van de Klant zoveel mogelijk te handhaven gedurende de aanval.

Deze functie bestaat uit het controleren van het dataverkeer naar de Dienst van de Klant en van buiten het OVH netwerk. Het niet-legitiem gekwalificeerde verkeer wordt afgewezen op een andere plek in de infrastructuur van de Klant, waardoor legitieme gebruikers toegang blijven hebben tot de Klant ondanks de cyberaanval.

Deze beschermingsmaatregelen kunnen niet ingrijpen bij computeraanvallen zoals SQL-injectie, bruteforce, het misbruik van beveiligingsproblemen, etc. Vanwege de grote complexiteit van de beschermingsservice, is OVH op geen enkele wijze gehouden de werking van deze service te garanderen of zelfs maar werkend te hebben. Het is mogelijk dat de aanval niet wordt ontdekt door de voorhanden zijnde instrumenten, en de geïmplementeerde instrumenten niet kunnen zorgen dat het functioneren van de Dienst gehandhaafd blijft.

Afhankelijk van de aard en de complexiteit van de aanval, behandelt OVH op verschillende beschermingsniveaus het dataverkeer teneinde zijn infrastructuur en de Dienst van de Klant te behouden.

De beschermingsservice wordt alleen geactiveerd na het ontdekken van de aanval door OVH middelen, en voor minimaal 26 uur.

Nadat de cyberaanval wordt geïdentificeerd en de beschermingsservice automatisch wordt geactiveerd, kan die service niet worden uitgeschakeld tot het einde van de 26 uren-periode.

Tijdens de gehele duur dat de service is geactiveerd, kan OVH de toegankelijkheid van de Klant applicaties niet garanderen, maar zal trachten de impact van deze aanval op de Dienst van de Klant en OVH's infrastructuur te beperken.

Indien, ondanks de activering van de beschermingsservice, de cyberaanval de integriteit van de infrastructuur van OVH of andere klanten van OVH ondermijnt, versterkt OVH de beschermende maatregelen wat kan leiden tot aantasting van de Dienst van de Klant of de beschikbaarheid hiervan.

Tenslotte is het mogelijk dat delen van het dataverkeer, doordat de aanval niet kan worden ontdekt door OVH's apparatuur, de Dienst van de Klant bereikt. De effectiviteit van de beschermingsservice hangt ook af van de configuratie van de Dienst van de Klant, als zodanig is het aan de Klant om te controleren of zij over de nodige competenties beschikt om goed beheer te waarborgen.

Samenvattend, de beschermingsservice ontslaat de Klant van zijn verplichting om zijn eigen Dienst veilig te stellen, om security tools (firewalls, etc.) te implementeren, om regelmatig het systeem bij te werken, zijn gegevens te back-uppen, of om de veiligheid van zijn computerprogramma's (scripts, codes, etc.) te waarborgen.