



BIJZONDERE VOORWAARDEN VOOR VERHUUR VAN EEN DEDICATED SERVER 2023

Ingangsdatum d.d. 01/11/2023

ARTIKEL 1 : DOEL

De onderhavige bijzondere voorwaarden vormen een aanvulling op de algemene voorwaarden voor dienstverlening van OVH en hebben ten doel de technische en financiële voorwaarden te bepalen waaronder OVH zich verbindt de dedicated server van de Klant op haar platform te verhuren en te hosten.

De Klant verklaart uitdrukkelijk dat OVH op geen enkele wijze bijdraagt aan het ontwerp, de ontwikkeling, de uitvoering en de installatie van de website van de Klant en de informaticatools voor het beheer en de administratie daarvan.

Deze bijzondere voorwaarden prevaleren boven de algemene voorwaarden in die gevallen waarin beide documenten met elkaar in strijd mochten zijn.

ARTIKEL 2 : MIDDELEN

Het serverplatform van OVH, waar de dedicated server van de Klant wordt geïnstalleerd, is via Internet voor het grote publiek toegankelijk via computers met een Internetverbinding.

Tijdens de gehele looptijd van de hosting en/of de verhuur van de dedicated server aan de Klant verschaft OVH de Klant toegang tot een aparte mailinglist en/of forum, zodat hij van technische adviezen gebruik kan maken.

ARTIKEL 3 : TECHNISCHE ONDERSTEUNING

OVH verleent de Klant technische bijstand volgens de algemene voorwaarden voor dienstverlening, behalve voor het in bijlage 1 opgenomen Isgenoeg-aanbod.

ARTIKEL 4 : VOORWAARDEN VOOR DE UITVOERING VAN DE DIENSTEN

OVH stelt de Klant per e-mail op de hoogte van de beschikbaarstelling van zijn dedicated server. De aanvangsdatum van de facturering wordt bepaald door het moment waarop de dedicated server daadwerkelijk online gaat.

De server wordt uiterlijk 7 dagen nadat de Klant het bedrag op het bestelformulier heeft voldaan ter beschikking gesteld.

Wanneer de server niet binnen deze termijn door OVH ter beschikking is gesteld, heeft de Klant het recht vernietiging van de transactie en teruggave van de reeds betaalde bedragen te eisen.

De aan de Klant verhuurde server blijft eigendom van OVH. Iedere door OVH verhuurde of gehoste server heeft een vast IP-adres. De server wordt gehost op het serverplatform van OVH.

OVH stelt de Klanten verschillende soorten servers ter beschikking. De hardware- en softwarebasisconfiguraties zijn online te vinden op (https://www.ovh.nl/dedicated_servers/).

De verschillende hiervoor geldende tarieven staan vermeld op de website van OVH (https://www.ovh.nl/dedicated_servers/).

De Klant is de beheerder van de server die hij van OVH huurt. De Klant kan zelf software op de server installeren. Dit gebeurt volledig op zijn eigen verantwoordelijkheid en OVH is niet aansprakelijk voor eventuele storingen van de server als gevolg hiervan.

ARTIKEL 5 : VERPLICHTINGEN VAN OVH

OVH verplicht zich haar uiterste best te doen om een service van hoge kwaliteit te leveren, in overeenstemming met het gebruiken in de branche en de State of the Art. OVH verplicht zich er met name toe:

5.1. De apparatuur in goede staat te houden. In geval van een defect van de aan de Klant verhuurde apparatuur verplicht OVH zich het gebrekkige onderdeel zo spoedig mogelijk te vervangen, tenzij het defect niet aan haar te wijten is, of tot elke andere ingreep over te gaan die een langere onderbreking van de service vereist dan normaal gesproken voor vervanging. In dat laatste geval dient OVH de Klant daarvan onmiddellijk in kennis te stellen;

5.2. De toegang tot de server via Internet 24 uur per dag en het hele jaar door te garanderen. OVH behoudt zich het recht voor de server te onderbreken voor technische ingrepen ter verbetering;

5.3. Storingen die niet te wijten zijn aan een onoordeelkundig gebruik van de server door de Klant op verzoek van deze laatste zo spoedig mogelijk te verhelpen;

5.4. De tools op een zo hoog mogelijk kwaliteitsniveau te houden, in overeenstemming met de regels en gebruiken in de branche.

ARTIKEL 6 : AANSPRAKELIJKHEID VAN OVH

OVH behoudt zich het recht voor de Internetverbinding van de aan de Klant verhuurde server te onderbreken indien deze server een gevaar vormt voor de veiligheid van het hostingplatform van OVH, hetzij als gevolg van hacking van genoemde server, hetzij doordat een zwakke plek in de beveiliging van het systeem is ontdekt, of omdat de server geüpdatet moet worden.

OVH dient de Klant hierover binnen een redelijke termijn, en voor zover mogelijk vooraf, onder vermelding van de aard en de duur van de ingreep te informeren, teneinde de hem in staat te stellen de nodige maatregelen te nemen. OVH verplicht zich de verbinding te herstellen zodra de correctieve ingreep door de Klant is uitgevoerd.

OVH is op geen enkele wijze aansprakelijk voor de inhoud van informatie, geluid, tekst, beelden, vormelementen en gegevens die toegankelijk zijn via de websites die op de server van de Klant worden gehost of die door de Klant worden verzonden of online gezet.

OVH kan evenmin aansprakelijk worden gesteld voor de gehele dan wel gedeeltelijke niet-naleving van een verbintenis en/of het in gebreke blijven van de netwerkproviders en met name van haar toegangprovider(s).

ARTIKEL 7 : VERPLICHTINGEN EN AANSPRAKELIJKHEID VAN DE KLANT

7.1 De Klant handelt als zelfstandige entiteit en draagt derhalve als enige het risico van zijn activiteiten. De Klant is als enige verantwoordelijk voor de diensten en websites die op zijn dedicated server worden gehost, alsmede voor de inhoud van de verzonden, verspreide of verzamelde informatie, de exploitatie en update daarvan, en voor alle bestanden, met name adresbestanden. De Klant dient met name de rechten van derden te eerbiedigen, waaronder persoonlijkheidsrechten en intellectuele eigendomsrechten als het auteursrecht, het octrooirecht en het merkrecht. OVH kan derhalve op geen enkele grond aansprakelijk worden gesteld voor de inhoud van de verzonden, verspreide of verzamelde informatie, de exploitatie en update daarvan, alsmede alle bestanden, met name adresbestanden.

OVH kan de Klant slechts waarschuwen voor de juridische gevolgen die uit onwettige activiteiten op de server kunnen voortvloeien, en wijst alle hoofdelijke aansprakelijkheid voor het gebruik van gegevens die door de Klant aan Internetgebruikers ter beschikking worden gesteld af.

Dit geldt tevens voor het geval dat de Klant aantoonbaar gebruik maakt van spamtechnieken op Internet. In dat geval wordt de dienstverlening zonder opzegtermijn stopgezet en de overeenkomst beëindigd.

Het is de Klant eveneens verboden om vanaf de server in andere computers binnen te dringen of een poging daartoe te doen (poortscans, sniffing, spoofing, enz.).

In deze gevallen kan de Klant geen aanspraak maken op teruggave door OVH van de reeds betaalde bedragen.

7.2 De Klant draagt als enige de gevolgen van de gebrekkige werking van de server als gevolg van het gebruik hiervan door zijn personeelsleden of iedere andere persoon aan wie de Klant zijn wachtwoord(en) heeft verstrekt. De Klant draagt tevens als enige de gevolgen van het kwijtraken van de hierboven bedoelde wachtwoorden.

7.3 Teneinde de beveiliging van de server van de Klant en alle andere servers op haar hostingplatform op niveau te houden, verplicht OVH zich om de Klant via de forum <http://forum.ovh.nl> per e-mail in kennis te stellen van de beschikbare updates van de applicaties van OVH waarvoor een beveiligingsgebrek is geconstateerd. Als de Klant geen gehoor geeft aan het verzoek van OVH om deze applicaties te updaten, behoudt OVH zich het recht voor de verbinding van de server met het Internet te verbreken.

Indien OVH ontdekt dat het systeem van de Klant wordt gehackt, stuurt zij eveneens een e-mail naar de Klant om erop te wijzen dat een herinstallatieprocedure noodzakelijk is om de integriteit van de server en het hele hostingplatform te behouden. De Klant kan OVH dan opdracht geven tot een dergelijke procedure, na een back-up van al zijn gegevens te hebben gemaakt. OVH behoudt zich het recht voor om in afwachting van de herinstallatie van het systeem de verbinding van de server met het Internet te onderbreken. OVH is niet verplicht om de gegevens van het gekraakte systeem naar het nieuwe systeem over te brengen. Deze handeling dient door de Klant zelf te worden verricht. OVH verplicht en beperkt zich uitsluitend tot de installatie van het nieuwe systeem.

7.4 Om veiligheidsredenen, behoudt OVH zich het recht voor, om over te gaan tot de onmiddellijke opschorting zonder mededeling, van elke server waarop een openbare service Proxy, IRC, VPN of TOR staat, welke gratis beschikbaar is of voor een vergoeding, en waarvan OVH kennis heeft van frauduleus of illegaal misbruik.

7.5 Het is aan de Klant om alle noodzakelijke maatregelen te treffen voor de back-up van zijn gegevens.

7.6 De Klant dient de kosten te voldoen voor alle licenties of gebruiksrechten die met OVH of derden zijn overeengekomen. Bij gebreke daarvan behoudt OVH zich het recht voor de service met onmiddellijke ingang stop te zetten.

7.7 OVH behoudt zich het recht voor te controleren of de Klant de aan hem ter beschikking gestelde server in overeenstemming met de onderhavige bepalingen gebruikt.

OVH behoudt zich het recht voor de dienstverlening aan de Klant in overeenstemming met artikel 7 van de algemene voorwaarden voor dienstverlening van OVH met onmiddellijke ingang stop te zetten, indien de Klant zich niet houdt aan de algemene en bijzondere voorwaarden van OVH en, meer in het algemeen, aan de geldende wet- en regelgeving en de rechten van derden.

7.8 De leveranciersverplichting met betrekking tot dedicated servers is beperkt tot het installeren van de server en de mogelijkheid voor de klant om de infrastructuur te huren. De leverancier heeft geen controle over de inhoud van de gegevens gehouden op de gehoste websites. De klant dient voor een periode van 12 maanden vanaf het creëren daarvan, te houden en te bewaren, alle gegevens ("Web Data") die de identificatie mogelijk maakt van enige partij die heeft bijgedragen op welke manier dan ook aan het creëren van enige inhoud, gehouden op enige gehoste website, die bereikt zou kunnen worden via de server. De Klant is als enige verantwoordelijk en aansprakelijk voor het houden en bewaren van alle Web Data.

De Klant zal een gemakkelijk toegankelijke en zichtbare structuur implementeren, die het mogelijk maakt voor enige persoon om aangifte te doen van elke overtreding of mogelijke overtreding dan ook, die heeft plaatsgevonden op enige website of die is bevat in enige data die verzonden werd via het server netwerk, met inbegrip van, maar niet beperkt tot, gegevens die aanzetten tot rassenhaat, kinderporno, aanzetten tot geweld, alsmede schending van de menselijke waardigheid of illegale gokactiviteiten. De Klant zal ervoor zorgen dat alle vereiste kennisgevingen worden uiteengezet op de website en dat het duidelijk is dat de Klant de hosting service provider is in enige juridische mededelingen gepresenteerd door zijn contractspartijen die een website bewerken.

ARTIKEL 8 : MAATREGELEN OM HET VERZENDEN VAN SPAM E-MAILS VIA HET OVH NETWERK TEGEN TE GAAN

OVH implementeert een systeem van technische maatregelen gericht op het tegengaan van het verzenden van fraudulente e-mails en SPAM vanaf haar infrastructuur.

Daartoe voert OVH een verificatie uit op het e-mail verkeer verzonden vanaf de door de Klant gebruikte server naar poort 25 (SMTP-server) op het internet. Deze bestaat uit het verifiëren van e-mails of ze door middel van automatische tools verstuurd zijn.

Verzonden e-mails worden noch gefilterd noch onderschept maar geverifieerd met een vertraging van enkele seconden. Deze operaties worden parallel uitgevoerd en in elk geval frontaal tussen de server en het internet.

Evenzo wordt er geen bewerking uitgevoerd op de verzonden e-mails: OVH zal de e-mails niet markeren (labelen), en ook niet op een andere manier de e-mails, verzonden door de Klant, wijzigen. Geen enkele informatie wordt door OVH opgeslagen tijdens deze operaties behalve de statistische gegevens.

Dit wordt regelmatig en volledig automatisch gedaan. Er is geen menselijke tussenkomst tijdens de verificatie van het verkeer naar poort 25 (SMTP-poort).

In het geval dat e-mails, verzonden vanaf de server van de Klant, geïdentificeerd worden als spam of frauduleus, zal OVH de Klant via e-mail op de hoogte brengen en overgaan tot blokkering van de SMTP-poort op de server.

OVH zal geen kopieën van e-mails, verzonden vanaf de SMTP-poort van de server, behouden, zelfs niet als ze geïdentificeerd zijn als SPAM.

De Klant kan om het deblokken van de SMTP-poort vragen dmv zijn beheerinterface.

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

Na de derde blokkering, behoudt OVH zich het recht voor om nieuwe verzoeken om deblokking van de SMTP-poort te weigeren.

ARTIKEL 9: MITIGATIE (BESCHERMING TEGEN DOS EN DDOS AANVALLEN)

OVH heeft beveiliging geïmplementeerd tegen computer aanvallen van DOS en DDOS (Denial of Service), onder de voorwaarde dat ze massaal worden uitgevoerd. Deze functie wordt ingeschakeld om de operationele Service van de Klant voor de duur van de aanval te behouden.

Deze functie, verder “mitigatie” genaamd, is om het verkeer te verifiëren naar de Klant en van buiten het OVH netwerk. Het onwettig gekwalificeerde verkeer wordt vervolgens afgewezen voor de infrastructuur van de Klant, waardoor legitieme gebruikers toegang hebben tot applicaties van de Klant ondanks de cyberaanval.

Deze beveiligingsmaatregelen kunnen niet interveniëren bij cyberaanvallen zoals SQL indringing, brute kracht, exploitatie van gaten in de beveiliging, etc. ...

Vanwege de grote complexiteit van beveiliging, is OVH niet gehouden aan een verplichting, het is mogelijk dat de aanval niet wordt ontdekt door de middelen die voorhanden zijn, en de geïmplementeerde middelen niet in staat zijn om het functioneren van de Service in stand te houden.

Afhankelijk van de aard van de aanval en de complexiteit, opereert OVH op verschillende niveaus bescherming van het verkeer om zijn infrastructuur en de Service van de Klant te behouden.

Mitigatie wordt alleen geactiveerd na het detecteren van de aanval door OVH instrumenten, en gedurende minimaal 26 uur. Als consequentie totdat de mitigatie wordt geactiveerd, ondersteunt de Service de aanval frontaal die tot zijn onbeschikbaarheid kan leiden.

Totdat de cyberaanval wordt geïdentificeerd en mitigatie automatisch wordt geactiveerd, kan mitigatie niet worden uitgeschakeld tot het einde van de 26-uursperiode.

Tijdens de gehele duur van de mitigatie activering, kan OVH niet de toegankelijkheid van de Client applicaties garanderen, maar zal trachten de impact van deze aanval op de Service van de Klant en de Infrastructuur van OVH te beperken.

Indien, ondanks de activering van mitigatie, de cyberaanval waarschijnlijk de integriteit van de infrastructuur van OVH of haar Klanten zal ondermijnen, versterkt OVH de beschermende maatregelen, deze kunnen de Service van de Klant aantasten of haar beschikbaarheid.

Tenslotte is het mogelijk dat een gedeelte van de data gegenereert door de aanval niet kan worden ontdekt door de OVH apparatuur en de Service van de Klant bereikt. De effectiviteit van de mitigatie hangt ook af van de configuratie van de Service van de Klant, als zodanig is het aan hen om te controleren of zij over de nodige competenties beschikken om een goed beheer te waarborgen.

Ter samenvatting, de mitigatie is geen vrijstelling voor de Klant om niet door te gaan met: het veiligstellen van zijn Service, om security tools (firewalls, ...) te implementeren, om regelmatig de systeemback-up bij te werken, zijn gegevens op te slaan, of om de veiligheid van zijn computerprogramma's (scripts, codes, enz ...) te waarborgen.

Mitigatie met de PRO-optie

Indien de Klant gebruikmaakt van de PRO-optie op haar Service, zijn er nieuwe functies beschikbaar. De Klant kan daardoor vooraf de mitigatie activeren op zijn Service, echter OVH herinnert eraan dat de activering van mitigatie een direct impact kan hebben op de kwaliteit van haar Service. Daarom moet het gebruik van mitigatie met volledige kennis van de feiten gedaan worden.

De Klant kan wanneer hij wil verschillende beschermingsprofielen testen om de impact op de Service te meten, en aldus het beschermingsprofiel vinden die het meest geschikt is voor het type Service die hij biedt. Het profiel gekozen door de Klant zal dan automatisch gebruikt worden door OVH bij het activeren van de mitigatie.

De Klant kan ook een firewall aanschaffen die direct verbonden zal zijn langs het OVH netwerk. Wanneer mitigatie op de Service van de Klant wordt geactiveerd, worden standaard Firewall-regels automatisch toegepast. Het is aan de Klant te zorgen voor de relevantie van de regels die de firewall integreert, om te voorkomen dat zijn activiteit gestoord wordt bij het activeren van de mitigatie.

ARTIKEL 10 : TARIEF, DUUR, VERLENGING EN OPZEGGEN VAN DE SERVICE

Het tarief is afhankelijk van de reeks server en de duur van de huurperiode (de „Beginduur“) die de Klant tijdens de bestelling gekozen heeft. Alleen het tarief dat op de door OVH uitgegeven bestelbon vermeld is, stemt overeen met het totale, door de Klant te betalen bedrag.

Tijdens de bestelling en bij elke verlenging van de Service wordt een factuur gepubliceerd en voldaan middels automatische incasso met de betalingsmethode die de Klant opgeslagen heeft. De Klant belooft een geldige betalingsmethode te kiezen uit de beschikbare betalingsmethoden en deze in zijn OVH-Account op te slaan.

De Klant dient precies te bepalen welke oplossing het beste aan zijn behoeften voldoet. Deze kan vervolgens niet meer veranderd worden tijdens de looptijd van het contract.

De Beginduur begint op de dag van effectieve levering van de dedicated server. Aan het einde van de Beginduur wordt de huurperiode automatisch verlengd voor opeenvolgende periodes met dezelfde duur (de „Verlengingsperiode(s)“), behalve bij veranderde verlengingsduur of bij opzeggen van de Service conform de hierna vermelde voorwaarden of de geldende Algemene Servicevoorwaarden.

De Klant kan de duur van toekomstige Verlengingsperiodes van zijn Services aanpassen via zijn Managementinterface, ten minste 24 uur voor het einde van de Beginduur of de lopende Verlengingsperiode.

Als de Beginduur niet op de eerste dag van een kalendermaand begint (aanvang tijdens de maand), dan zal de verlengingscyclus van de Service met een maandelijkse cyclus uitgelijnd worden bij de eerste verlenging, opdat de volgende Verlengingsperiodes op de eerste dag van een kalendermaand aanvangen. (Bijvoorbeeld: De automatische verlenging aan het einde van de Beginduur voor een Service die aanvankelijk voor een (1) jaar afgesloten werd op 24 mei 2019, leidt tot een verlenging van deze Service vanaf 24 mei 2020 tot en met 31 mei 2020).

Als de Klant niet wenst dat de huurperiode van een dedicated server verlengd wordt aan het einde van de Beginduur of de lopende Verlengingsperiode („Verlengingsdatum“), dan deactiveert hij de automatische betaalfunctie in zijn Managementinterface minstens 24 uur voor het einde van de Beginduur of de lopende Verlengingsperiode.

Indien de automatische betaling volgens de hierboven vermelde voorwaarden gedeactiveerd is, dan zal de betreffende Service automatisch opgezegd en verwijderd worden bij afloop van de Beginduur of de lopende Verlengingsperiode („Afloopdatum“). Alle Inhoud en door de klant in het kader van de Service opgeslagen gegevens zullen binnen maximaal zeven (7) dagen na de Afloopdatum van deze Service verwijderd worden. Dit

gebeurt ook bij een onmiddellijke of geplande opzegging. De klant dient alle noodzakelijke maatregelen te treffen om het behoud van de voornoemde Inhoud en gegevens te garanderen voordat de Service wordt opgezegd.

Desalniettemin behoudt de Klant de mogelijkheid de betreffende Service te verlengen door de automatische betalingsmethode te reactiveren tot aan 24 uur voor de Afloopdatum of door de volgende Verlengingsperiode vooruit te betalen.

De duur plus de verlengings- en opzegvoorwaarden van bepaalde opties of functies die aan de Service gekoppeld kunnen zijn, kunnen verschillen van diegene die op de Service van toepassing zijn. De Klant dient hierop te letten.

BIJLAGE1: ISGENOEG SERVERS

De OVH Isgenoeg 2013 is beperkt tot natuurlijke personen of rechtspersonen met zetel in de Europese Unie, Noorwegen en Zwitserland. De Klant mag niet meer dan drie Isgenoeg servers 2013 gelijktijdig gebruiken.

Het gebruik van de Isgenoeg 2013 servers is strikt voor persoonlijk gebruik. Elke aankoop van deze soort voor het doel van doorverkoop, is verboden en zal resulteren in de onmiddellijke beëindiging van de overeenkomst van de betrokken server (s).

Als onderdeel van de OVH offerte, wordt de Klant geïnformeerd dat hij, in plaats van technische ondersteuning, zoals gedefinieerd in artikel 3, een support forum beschikbaar heeft via het volgende adres: <http://forum.ovh.nl/>.

BIJLAGE 2 – BACK-UP SERVICE

DOEL

De services wekelijkse back-up / incrementele back-up / FTP back-up zijn opslagruimten waar de gegevens van de dedicated server van de Klant geheel of gedeeltelijk kunnen worden opgeslagen.

De services wekelijkse back-up / incrementele back-up / FTP back-up kunnen als optie worden verkregen wanneer reeds een overeenkomst is gesloten voor de verhuur en/of de hosting van een dedicated server onder Linux of FreeBSD. Tenzij anders wordt overeengekomen zijn deze services niet toegankelijk voor Klanten die een hosting-aanbod met client access hebben ondertekend. Er zijn opslagruimten van verschillende omvang beschikbaar.

De FTP back-upservice kan in bepaalde aanbiedingen voor de verhuur van een dedicated server worden opgenomen.

De Klant verklaart uitdrukkelijk dat OVH in het kader van deze overeenkomst geen enkele bijdrage levert aan het ontwerp, de ontwikkeling, de uitvoering en de installatie van de website van de Klant en van diens beheers- en administratietools.

VOORWAARDEN VOOR DE UITVOERING VAN DE DIENSTEN

- Wekelijkse back-up

In het kader van de wekelijkse back-upservice kan één (1) keer per week een back-up worden gemaakt van de gegevens op de dedicated server, mits in het ondertekende aanbod voldoende opslagcapaciteit is opgenomen. De volgende directory's worden steeds van de back-up uitgesloten: /proc /sys /tmp /home/ovh/src.

- Incrementele back-up

Met de incrementele back-upservice kunnen bepaalde gegevens van de dedicated server worden opgeslagen. De Klant kan data en tijdstippen voor zijn back-ups reserveren (op voorwaarde dat deze beschikbaar zijn), met een maximum van twee (2) back-ups per dag, zulks tot ten hoogste de in zijn overeenkomst opgenomen opslagcapaciteit.

De Klant kan bepalen hoeveel eerdere back-ups ('snapshots' genoemd) hij in zijn opslagruimte wenst te bewaren (zulks tot ten hoogste de in zijn overeenkomst opgenomen opslagcapaciteit).

- Instellen van een wekelijkse of incrementele back-up

Bij het sluiten van de serviceovereenkomst wordt de server van de Klant door OVH geconfigureerd om backups mogelijk te maken, waarna de Klant van het goede verloop van de configuratie in kennis wordt gesteld. De Klant mag deze configuratie in geen geval veranderen.

Vervolgens moet de Klant in de beheersinterface (manager) de back-upparameters specificeren (keus van de directory, data van de back-ups, e-mailadres, enz.).

De back-ups worden in gang gezet door de back-upservers van OVH. Na iedere back-up verstuurt OVH een e-mail om te melden dat de back-up goed, of (eventueel) minder goed is verlopen. De Klant dient de ontvangst van deze e-mail te controleren en na te gaan of de back-up goed is uitgevoerd (de back-uphistorie kan worden bekeken via de beheersinterface). Uitsluitend de Klant kan controleren of de service is geactiveerd.

Wanneer de back-up niet lukt (opslagruimte is vol, geen toegang tot de server van de Klant, e.d.), kan de back-upservice tijdelijk worden gedeactiveerd. De Klant dient deze dan via de beheersinterface opnieuw te activeren.

- Ophalen van gegevens uit een wekelijkse of incrementele back-up

De Klant kan al zijn gegevens of een deel hiervan terughalen via het protocol voor gegevensoverdracht RSYNC, uitsluitend vanaf de server waarvoor hij de serviceovereenkomst heeft gesloten. De ID's en de naam van de back-upserver zijn bij het aangaan van de overeenkomst aan de Klant doorgegeven.

Ingeval van een wekelijkse back-up kan de Klant via de beheersinterface (manager) vragen om al zijn gegevens vanaf zijn laatste back-up op zijn server te kopiëren (bij deze procedure worden de eventueel op de dedicated server aanwezige gegevens vervangen).

- FTP back-up

De FTP back-upservice is een opslagruimte die toegankelijk is via het protocol voor bestandsoverdracht FTP. Deze opslagruimte wordt beschermd door een ID en een wachtwoord, is uitsluitend toegankelijk vanuit de dedicated server van de Klant en dient uitsluitend voor de back-ups van zijn server.

De Klant dient zelf de back-up- of overdrachttools op zijn opslagruimten te installeren.

VERPLICHTINGEN VAN OVH

- Verbintenissen

De opgeslagen gegevens zijn OVH niet bekend. De Klant dient zich derhalve ervan te vergewissen dat hij voldoende rechten op deze gegevens heeft en dat de inhoud geen inbreuk vormt op het Nederlandse en internationale recht en de goede zeden.

OVH verplicht zich haar uiterste best te doen om een service van hoge kwaliteit te leveren, in overeenstemming met de gebruiken in de branche en de State of the Art.

OVH behoudt zich het recht voor de server te onderbreken voor technische ingrepen ter verbetering.

OVH dient de Klant hierover binnen een redelijke termijn, en voor zover mogelijk vooraf, onder vermelding van de aard en de duur van de ingreep te informeren, teneinde de hem in staat te stellen de nodige maatregelen te nemen. De Klant dient er dan op toe te zien dat de volgende back-up plaatsvindt.

Ingeval van een defect aan een back-upserver en/of wanneer de gegevens op de server beschadigd of niet toegankelijk zijn voert OVH zo spoedig mogelijk een nieuwe back-up uit van de gegevens van de Klant (in geval van een wekelijkse of incrementele back-up) of verzoekt zij de Klant een nieuwe back-up uit te voeren (ingeval van een FTP back-up).

- Back-up van de gegevens

In het kader van een wekelijkse of incrementele back-up wijst OVH iedere aansprakelijkheid voor de goede uitvoering van de back-up van de hand. Bij iedere back-up zendt OVH bericht aan de Klant op het e-mailadres van de beheerder of het adres dat bij de configuratie van

de back-upservice is aangegeven en stuurt zij hiermee steeds de back-up logs mee. De Klant dient de uitvoering van de back-up te controleren, in geval van een storing na te gaan wat hiervan de oorzaak was en de technische helpdesk van OVH van een en ander in kennis te stellen zodat een nieuwe back-up van de directory's kan worden gemaakt. Indien een storing wordt vastgesteld kan OVH de service stopzetten na de Klant hiervan in kennis te hebben gesteld.

- Vertrouwelijkheid van de gegevens van de Klant

De gegevens in de back-up directory's zijn vertrouwelijk. Ze worden beschermd door een wachtwoord en zijn uitsluitend toegankelijk via het IP-nummer van de server waarvoor een back-upservice is aangegaan. OVH verplicht zich deze gegevens niet te verspreiden. Indien de rechter hierom verzoekt dient OVH echter de justitiële autoriteiten de gewenste informatie te verschaffen. Ook wanneer wordt vermoed dat is ingebroken tijdens de verwerking van gegevens op de installaties van OVH, behoudt OVH zich het recht voor om zich toegang te verschaffen tot de gegevens van de Klant en eventueel diens account onmiddellijk stop te zetten.

- Aansprakelijkheid

OVH is op geen enkele wijze aansprakelijk voor de inhoud van informatie, geluid, tekst, beelden, vormelementen en gegevens die toegankelijk zijn in de opgeslagen directory's van de Klant.

VERPLICHTINGEN EN AANSPRAKELIJKHEID VAN DE KLANT

De Klant dient na te gaan of de back-up van zijn directory's met succes is uitgevoerd. Indien zich problemen voordoen neemt de Klant alle noodzakelijke maatregelen om de back-up van de directory's opnieuw uit te voeren. Wanneer de dedicated server opnieuw moet worden geïnstalleerd (herinstallatie van het systeem of vervanging van de harde schijf), dient de Klant ervoor te zorgen dat de wekelijkse of incrementele back-up opnieuw wordt geconfigureerd (hij kan dit doen via zijn beheersinterface).

De Klant handelt als zelfstandige entiteit en draagt derhalve als enige het risico voor zijn activiteiten. De Klant is als enige verantwoordelijk voor de in zijn directory's aanwezige bestanden en gegevens. Hij is verantwoordelijk voor de inhoud van de verzonden, verspreide of verzamelde informatie, de exploitatie en update daarvan, en voor alle bestanden, met name adresbestanden.

DUUR VAN DE SERVICE EN OPZEGGING

De serviceovereenkomst wordt gesloten voor de looptijd die op het moment van de aanmaak van het bestelformulier door de Klant wordt gekozen of tot de afloop van de overeenkomst voor de dedicated server, en gaat in op de datum waarop de service ter beschikking wordt gesteld.

Na afloop van de overeenkomst kan de service door de Klant worden verlengd voor de door hem gekozen looptijd en volgens de tarieven, bepalingen en voorwaarden van OVH die gelden op de datum van de verlenging, tenzij een der partijen de overeenkomst opzegt volgens de hierna genoemde voorwaarden en termijnen.

- Wissen van de gegevens van een wekelijkse of incrementele back-up Tenzij uiterlijk op de 30e dag na afloop van de serviceovereenkomst (of van de overeenkomst voor de dedicated server als deze eerder afloopt) verlenging plaatsvindt worden alle gegevens door OVH gewist.
- Wissen van de gegevens van de FTP back-up

De gegevens van de FTP back-up worden op hetzelfde moment gewist als die van de dedicated server.