

# Antwoord op uw vragen over cloud. Easy.

TKP Pensioen  
Versie 1.2, maart 2019

## Algemeen

### Waarom kiest TKP voor cloudtechnologie?

Onze pensioenuitvoering is in hoge mate geautomatiseerd. De inrichting van ons ICT-landschap bestaat uit vele onderdelen, zoals software en infrastructuur. Onderdelen die we zelf ontwikkelen en bestaande producten die we met elkaar integreren tot een samenhangend geheel.

Een deel van deze bestaande producten (zoals infrastructuur) is inmiddels zo standaard geworden dat deze ook als hoogwaardige dienst kan worden afgenomen bij verschillende cloudproviders zoals Amazon Web Services (AWS), Microsoft en Google. Cloudinfrastructuur zorgt voor een hogere beschikbaarheid en is beter bestand tegen piekbelasting of eventuele aanvallen.

Cloud biedt ook nieuwe mogelijkheden die in het bestaande landschap minder makkelijk te realiseren zijn. Voorbeelden hiervan zijn nieuwe toepassingen binnen onze kanalen zoals chat, integratie met *third-party* oplossingen zoals een SaaS DC-administratie en uitgebreide mogelijkheden voor data science en analytics.

Door gebruik te maken van cloudtechnologie kunnen we ons meer focussen op het beheren, uitbouwen en innoveren van de kern van onze dienstverlening. Hiermee worden we slagvaardiger en kunnen we de gewenste en noodzakelijke aanpassingen in onze dienstenportfolio eenvoudiger en sneller doorvoeren.

### Hoe gaat de financiële sector om met cloud?

Toepassing van cloudtechnologie is sinds enkele jaren binnen de financiële sector volledig geaccepteerd. Onze cloudinrichting is mede gebaseerd op *best practices* uit deze sector. Ander pensioenuitvoeringsorganisaties bereiden zich op dit moment ook voor op wijzigingen in het pensioenstelsel en daarmee vernieuwing van hun ICT-landschap. Deze vernieuwing wordt ook mede gefaciliteerd door cloudtechnologie. We onderzoeken de samenwerkingsmogelijkheden met andere pensioenuitvoeringsorganisaties op het gebied van kennisdeling en hebben afstemming met onder andere DNB.

## Impact cloudtechnologie op onze dienstverlening

### Wat gebeurt er met de huidige SLA's?

We doen geen afbreuk aan de overeengekomen SLA's. We verwachten de servicelevels te verbeteren door gebruik te maken van cloudtechnologie.

## Selectieproces cloudleveranciers

### Hoe selecteert en contracteert TKP cloudleveranciers?

We selecteren en contracteren cloudleveranciers op basis van standaardprocessen binnen Contract- en leveranciersmanagement.

### Waarom is Amazon Web Services (AWS) geselecteerd?

In het selectieproces is een afweging gemaakt tussen Amazon Web Services (AWS), Google Cloud Platform en Microsoft Azure Cloud. Uiteindelijk is gekozen voor AWS op basis van de Gartner-rapportage (Magic Quadrant - indicatie marktleiderschap), de mate van innovatie en de breedte van het dienstenportfolio.

Verder hebben veel financiële partijen in Nederland, waaronder onze moeder Aegon, gekozen voor AWS en staat DNB positief tegenover deze cloudprovider. Google Cloud Platform viel af door de locatie van de opgeslagen gegevens (GDPR), omdat een groot deel van de diensten 'global' zijn. Microsoft Azure Cloud viel af, omdat deze cloudprovider een minder breed portfolio heeft dan AWS en diensten mist die voor ons van belang zijn.

### Hoe kijkt TKP aan tegen AWS in combinatie met Environmental Sustainable Governance (ESG)?

We hebben AWS met name geselecteerd op basis van de uitgangspunten die direct zijn terug te voeren op onze dienstverlening. In de media was Amazon onderwerp van voor wat betreft duurzaamheid en werknemersbeleid. We begrijpen dat ESG een belangrijk aspect is in de pensioensector. De betreffende media-aandacht heeft met name betrekking op het retailbedrijf van Amazon en in mindere mate op AWS. AWS is in de technologiesector een aantrekkelijke werkgever waar veel ruimte is voor ontwikkeling en arbeidsomstandigheden.

Daarnaast heeft Amazon de afgelopen periode verbeteringen doorgevoerd in het retailbedrijf. Zo is in 2018 het minimumloon voor medewerkers in distributiecentra in de VS [omhoog gebracht naar \\$15 per uur](#) (dat is bijna het dubbele van het wettelijk minimumloon in de VS). Europese fulfilment-medewerkers hebben een vergelijkbare verhoging gekregen. Ook zijn de [opleidingsmogelijkheden verbeterd](#).

Meer informatie vindt u op de website van Amazon:

- <https://www.aboutamazon.com/sustainability>
- <https://www.aboutamazon.com/our-communities>
- <https://www.aboutamazon.com/job-creation-and-investment>

## DNB: proces en risicoanalyse

### Hoe ondersteunt TKP pensioenfondsen op het gebied van de toezichtseisen (cloud computing risicoanalyse)?

Als onder toezicht staande onderneming moet u DNB informeren over een uitbesteding. DNB vermeldt daarover in haar circulaire cloud computing: ‘Alvorens een onder toezicht staande onderneming overgaat tot het gebruik van cloud computing verwacht DNB dat zij geïnformeerd wordt voordat de uitbesteding zal plaatsvinden. Als onderdeel van het risicogebaseerde toezicht zal DNB bij de onder toezicht staande onderneming de risicoanalyse ten aanzien van cloud computing opvragen en beoordelen.’

Op dit moment bereiden we de risicoanalyse zoveel mogelijk voor en maken we een blauwdruk. De verwachting is dat u daarna deze blauwdruk kunt aanvullen en overleggen aan DNB. We hebben een gespecialiseerde partij ingeschakeld (Oblivion Cloud Control, een AWS Premium Partner) die ons adviseert over de verschillende producten en ons begeleidt tijdens het proces.

We overleggen met DNB om dit proces voor fondsen nog verder te vereenvoudigen en te faciliteren. Zodra we weten hoe dit gaat, informeren wij u hierover. Meer informatie over het toetsingskader vindt u op [de website van DNB](#).

## Beheersing & Continuïteit

### Hoe beheerst TKP de risico's van cloud?

We staan voor een beheerste overgang naar cloud. Cloud is een vorm van uitbesteding, die wordt beheerst volgens ons inkoop- en uitbestedingsbeleid. Dat betekent dat we maatregelen hebben genomen om risico's te beheersen. Denk hierbij aan (niet uitputtend):

- Risk Self Assessment;
- Contract & SLA;
- SLA-rapportage & -bespreking;
- Normenkader uitbesteding;
- Assurance van leverancier;
- Periodieke contractreview;
- Verantwoording via ISAE 3402;
- Dashboardrapportage.

### Hoe zorgt TKP ervoor dat het voldoet aan de vereisten die worden gesteld aan de systemen door bijvoorbeeld de accountant?

We nemen de huidige eisen van ISAE 3402 en compliance mee in de nieuwe inrichting van het ICT-landschap. Deze worden op de bestaande wijze geaudit.

## Wat zijn de kosten van cloud?

De beweging naar cloud is voornamelijk gebaseerd op een kwalitatieve business case. We willen de interne dienstverlening op het gebied van het platform en de infrastructuur verbeteren en innovatie versnellen. Cloud heeft als voordeel dat we minder tijd en inspanning kwijt zijn aan de 'commodity' onderdelen van het platform. Uiteraard zijn kosten een belangrijk aandachtspunt. De verwachting is dat dit ongeveer break-even zal zijn en past binnen de huidige budgettering. De business case is daarom meer kwaliteit bij gelijke kosten.

## Is er een exitstrategie?

Ja, de exit strategie behelst, naast de door DNB voorgeschreven contractuele clausules, ook een architectuur- en technologie-strategie. Uitgangspunt is dat we ons platform zo portabel mogelijk bouwen. Dat wil zeggen cloudprovider-onafhankelijk. Afwijkingen van deze strategie beheersen we en stemmen we af binnen de TKP Technology Board, waar onze CIO verantwoordelijk voor is.

## Kent cloud onomkeerbare beslissingen?

Nee, we bouwen het cloudplatform met producten die gebaseerd zijn op open standaarden. Het platform is op deze manier cloudprovider-onafhankelijk en ICT-oplossingen zijn portabel naar alternatieve cloudplatformen en/of een eigen datacenter.

Het kost echter wel tijd om terug te gaan naar een eigen datacenter of naar een alternatief cloudplatform, mochten we daartoe besluiten.

## Kan TKP blijven werken zonder internet?

Onze systemen blijven gewoon werken zonder internet. Koppelingen met ketenpartners worden wel tijdelijk onderbroken. Wij hebben meerdere fysiek gescheiden toegangspaden in onze systemen bij AWS, die het risico op verstoring tot een minimum beperken.

## Cloudtransitie en roadmap

### Wat is de planning van de cloudtransitie?

De globale planning voor de cloud is als volgt:

- |  |             |
|--|-------------|
| • Stap 1 Ontwikkelen administratieve kern: Borg          | 2018 - 2019 |
| • Stap 2 Fondswebsite, Mijn Omgeving en werkgeversportal | medio 2019  |
| • Stap 3 Werkplektools (concept)                         | 2019        |
| • Stap 4 Kernadministratie en kerninfrastructuur         | na 2020     |

We houden u op de hoogte over de voortgang en de meer gedetailleerde planningen als deze bekend zijn. Voor de duidelijkheid: pas nadat AWS als subverwerker is aangesloten (via de reguliere processen) migreren we onze klantdata naar AWS.

## Hoe lang duurt het voordat TKP overgaat naar cloud?

De overgang naar cloud is een business- c.q. architectuurvraagstuk en gebeurt in verschillende stappen. Na uw melding bij DNB worden de verschillende onderdelen van het bestaande landschap en nieuwe pensioenkernel verplaatst naar de cloud. We passen de roadmap regelmatig aan. We rekenen op een transitie van 3 tot 4 jaar.

## Security en dataveiligheid

### In hoeverre is data van pensioenfondsen afgeschermd en veilig?

We baseren onze beveiligingsmaatregelen op best practices en geldende normenkaders, aangevuld met specifieke maatregelen indien de uitkomsten van risicoanalyses hiertoe aanleiding geven. De gegevens die in de cloud worden bewaard zijn versleuteld op ieder niveau (*in transit* en *at rest*). Verder treffen we minimaal dezelfde beveiligingsmaatregelen als in de huidige omgevingen en op elementen passen we additionele maatregelen toe. De toepassing van extra maatregelen is een van de voordelen van cloudtechnologie doordat deze laagdrempelig worden gefaciliteerd.

## Toepassing van Amazon Web Services (AWS)

### Waar wordt data in de cloud van AWS opgeslagen?

Data wordt binnen de Europese grenzen opgeslagen. De primaire AWS-regio is Dublin, Ierland. Binnen de dienstverlening van AWS in Europa is deze regio de meest vooruitstrevende en heeft de langste historie.

Nieuwe diensten worden doorgaans binnen de Europese grenzen als eerste ingezet in Ierland. De regio Ierland is tenslotte ook kostentechnisch de meest aantrekkelijke Europese regio. Naast regio Ierland wordt gebruikgemaakt van Frankfurt, Duitsland als secundaire regio voor het opslaan van back-ups.

### Op basis waarvan zijn de AWS-producten gekozen?

Welke producten en diensten worden afgenomen binnen de dienstverlening van AWS wordt door de reguliere innovatie- en uitbestedingsprocessen beheerst en onder architectuur uitgewerkt. Onder meer de TKP Technology Board en Contract- en leveranciersmanagement spelen hierbij een prominente rol. Documentatie van de gebruikte producten en diensten vindt plaats in het uitbestedingsdossier.

### Blijft TKP in de toekomst diensten aanbieden vanuit zowel de cloud als haar eigen datacenter?

We richten ons met TKP Connect op het vernieuwen en verbeteren van onze dienstverlening op basis van een cloudplatform. Hierbij worden stapsgewijs de diensten naar de cloud gemigreerd, om uiteindelijk tot 'cloud only'-dienstverlening te

komen. Op termijn bieden we geen diensten meer aan vanuit ons eigen datacenter.

### Is AWS een nieuwe subverwerker?

AWS wordt een nieuwe subverwerker voor uw fonds. Wij sturen u binnenkort een brief met meer informatie. Dit proces verloopt volgens het proces 'Aanstellen nieuwe subverwerker'.

### Hoe is de back-up straks geregeld?

Ons cloudplatform wordt zodanig ingericht dat de productieservices een hoge beschikbaarheid kennen. Dat doen we door deze binnen AWS te verdelen over een aantal fysiek gescheiden datacenters die naadloos op elkaar aansluiten (een zogenaamde Availability Zone). Daarnaast wordt een back-up van data gemaakt naar een andere regio. Mocht de productieregio niet beschikbaar zijn, dan kan worden uitgeweken naar de back-upregio.

### Als klanten massaal weggaan bij AWS of AWS zelf stopt, kan TKP daar dan weg?

Dit scenario is onderdeel van onze exitstrategie. We zijn hier op voorbereid.

### Kunnen buitenlandse overheden data opvragen bij AWS?

Dit kan niet worden uitgesloten. Er zijn situaties denkbaar waarin een buitenlandse overheid via juridische procedures toegang eist tot data. In dit geval zal AWS zich maximaal verzetten en verwijzen naar haar klanten, in dit geval TKP. Wij verwijzen op dat moment naar onze klanten. De data is echter wel versleuteld en een derde partij kan in principe niets met deze data. Ook is de semantiek – het interpreteren van data – alleen bekend bij ons.

### Kan de Amerikaanse overheid data opvragen bij AWS via de CLOUD Act?

Ja, op basis van de CLOUD Act zijn er situaties mogelijk dat de Amerikaanse overheid toegang eist tot data. Dat wil echter niet zeggen dat die informatie ook daadwerkelijk verstrekt moet worden of dat de data bruikbaar is voor de Amerikaanse overheid.

Op basis van de CLOUD Act kan de Amerikaanse overheid alleen data opvragen indien dat relevant is voor de publieke veiligheid of ter opsporing van strafbare feiten (waaronder terrorisme). Daarnaast moet sprake zijn van een verzoek goedgekeurd door een Amerikaanse rechter in overeenstemming met procedures in de VS. Dat betekent dat er een gericht verzoek naar een bepaald persoon of bepaalde groep personen moet zijn en er geen sprake kan zijn van zogenaamde 'fishing expeditions'.

We laten in de overeenkomst met AWS opnemen dat AWS zich maximaal verzet tegen een dergelijk verzoek. Indien wettelijk toegestaan zal AWS ons (en onze klanten) op de hoogte stellen indien een dergelijk verzoek wordt ingediend. AWS staat er bekend om zich ook daadwerkelijk te verzetten tegen dergelijke verzoeken en rapporteert hierover.

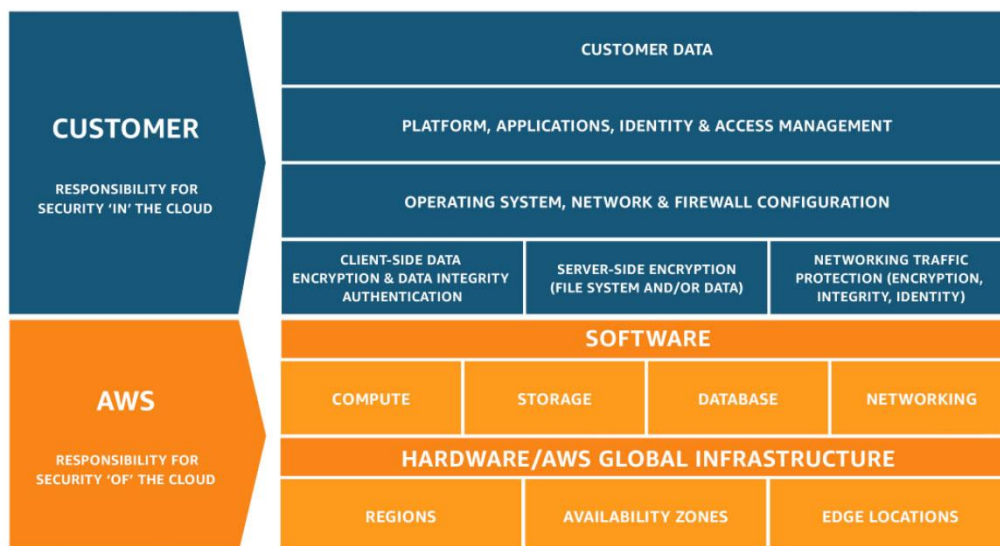
Daarnaast geldt dat we data versleutelen en het niet zeker is dat AWS onder de CLOUD Act gedwongen kan worden om de encryptiesleutel te verstrekken.

Tot slot is het de vraag of de data die verstrekt wordt door AWS aan de Amerikaanse overheid, begrijpelijk is. Doordat AWS en de Amerikaanse overheid geen toegang hebben tot de pensioenapplicatie is het voor hen lastig de data te interpreteren. Meer informatie over de CLOUD Act en hoe AWS hiermee omgaat vindt u hier:

- [d1.awsstatic.com/analyst-reports/Don't Get Spooked\\_CloudAct\\_JM181119.pdf](https://d1.awsstatic.com/analyst-reports/Don't_Get_Spooked_CloudAct_JM181119.pdf)
- <https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF>

### Kan TKP het AWS shared responsibility model delen?

Het shared responsibility model is een model dat AWS gebruikt om de verschillende verantwoordelijkheden rondom het gebruik van haar cloud toe te lichten.



Dit document is openbaar en beschikbaar op <https://aws.amazon.com/compliance/shared-responsibility-model>.

## Overig

### Wat is de verhouding tussen PPS en cloud?

PPS en cloud staan los van elkaar. De huidige administratie op basis van PPS staat in ons eigen datacenter. PPS wordt op termijn vervangen door BORG dat maximaal gebruik maakt van cloudtechnologie. Naast BORG wordt ook de vernieuwing van onze dienstverlening gebaseerd op de cloud.



## Kan blockchain worden toegepast?

Ja, AWS faciliteert dit. We zijn regelmatig in gesprek met APG en PGGM over blockchain. De transitie naar cloud staat echter los van de mogelijke toepassing van blockchain.