Ministerie van Justitie en Veiligheid

Bestuurlijke Cloudstrategie
Ministerie van Justitie en Veiligheid

"Op gecontroleerde, veilige en zorgvuldige wijze de publieke cloud in"

Versie 1.2

Datum	27 juni 2024
Status	V1.2 Definitief (vastgesteld in CIO-raad 27 juni 2024)
	V1.1 Definitief (vastgesteld in BBR 18 december 2020)

Voorwoord

Binnen het ministerie van Justitie en Veiligheid (JenV) wordt de laatste 3, 4 jaar steeds vaker gebruik gemaakt van publieke clouddiensten. In 2020 als gevolg van Corona hebben diensten als Webex en Microsoft Teams hun intrede gedaan. Veel applicaties en software worden enkel en alleen nog maar aangeboden via de publieke clouddiensten (cloud-only). De reden is dat aanbieders van applicaties via een Cloud Service Provider (CSP) zoals Microsoft Azure, Amazon Web Services, Google of andere CSP's over een dusdanig groot afnemersbereik kunnen beschikken dat ontwikkeling van on-premise producten voor hun geen aantrekkelijke optie is. Dit geldt tevens voor de producten van de CSP's zelf, Microsoft365 is daar een goed voorbeeld van, deze applicatie is voor de online producten enkel nog als cloud toepassing beschikbaar. De publieke clouddiensten levert tevens toepassingen die binnen de eigen besloten omgeving van een afnemer eenvoudigweg niet meer mogelijk zijn, dan wel een dusdanige hoge investering vragen dat de validiteit van zo'n grote investering ontbreekt. Naast deze ontwikkelingen zijn er ook kansen die met het gebruik van cloud toepassingen kunnen worden gecreëerd. Zo kan het invulling geven aan de behoefte in het veilig en flexibel opslaan van grote hoeveelheden data en het efficiënt inzetten van rekenkracht en functionaliteit. De opkomst in afgelopen jaar van Generatieve AI applicaties, zoals ChatGPT, Mistral AI, Bing AI, Bard, PaLM, etc. creëren een exponentiële versnelling op de afname van clouddiensten.

Op 18 december 2020 is de Cloud Strategie van JenV door de Brede Bestuursraad vastgesteld. Gelet op de Rijksbrede ontwikkelingen, zoals het Rijksbreed Cloudbeleid (aug. 2022) en het Implementatiekader risicoafweging cloudgebruik (jan. 2023) is aanscherping van de JenV Cloudstrategie gewenst. De noodzaak voor JenV om middels clouddiensten de mogelijkheid én flexibiliteit om functionele vraagstukken middels de inzet daarvan de ICT beter en sneller aan te laten sluiten op de wensen vanuit de organisatie is daarbij onveranderd. Als ook het strategisch belang dat JenV mee kan bewegen in de steeds snellere ontwikkelingen op ICT-gebied en niet overvallen wordt door disruptieve technologie, maar daarop is voorbereid.

De JenV cloudstrategie geeft zowel invulling van de strategie hoe JenV op een gecontroleerde, veilige en zorgvuldige wijze clouddiensten kan gebruiken, maar ook invulling aan het JenV cloudbeleid welke geldt voor het verwerven en toepassen van clouddienstverlening door de onderdelen van JenV.

Management Samenvatting

In december 2020 is in de Brede Bestuursraad de JenV-brede bestuurlijke cloudstrategie vastgesteld. De overheid is tot die tijd altijd terughoudend geweest in het gebruik van de publieke cloud[1]. Op dat moment een logische terughoudendheid, want op het gebied als bescherming van persoonsgegevens, gegevensopslag, digitale soevereiniteit[2], beveiliging en beschikbaarheid bij het gebruik van clouddiensten is weinig ervaring binnen JenV. Het belang van clouddiensten voor JenV is de afgelopen 3 jaar steeds verder toegenomen. Als aanjager van nieuwe technologieën en innovatie. Als ook het voordeel om de organisatie wendbaarder en flexibeler te maken. Met het vergroten van die snelheid en wendbaarheid van de IV-voorziening vergroot eveneens de slagkracht en uitvoeringssnelheid van JenV. Gezien het 'Rijksbrede cloudbeleid' en andere kaders en richtlijnen zoals het 'Implementatiekader risicoafweging cloudgebruik' is een aanscherping van de JenV Cloudstrategie uit 2020 gewenst.

De cloudstrategie van JenV staat niet op zichzelf, maar heeft relaties met de cloudstrategie van de Europese Commissie waar Nederland zich aan heeft gecommitteerd[3], het Rijkscloud beleid [4], het ketenperspectief en de organisatie specifieke cloudstrategieën. De verantwoordelijke voor de Cloudstrategie JenV is de CIO van het Ministerie van Justitie en Veiligheid. De opdrachtgever voor beheer en doorontwikkeling van de strategie in deze is de directeur van de Directie Informatievoorziening en Inkoop (DI&I). DI&I/CIO-office JenV zorgt tevens voor ondersteuning bij het gebruik van de cloudstrategie. De Cloudstrategie JenV ondersteunt alle organisaties van het Ministerie van Justitie en Veiligheid bij het nemen van beslissingen over het gebruik van cloud dienstverlening. De Cloudstrategie JenV inclusief onderliggende documenten is van toepassing voor alle JenV onderdelen en ZBO's vallende onder JenV. Voor de onderdelen onder ministeriële verantwoordelijkheid heeft het strategiedocument daarin een "*comply*" or "*explain*" status en is het onderliggende afwegingskader kaderstellend. Voor de Sui Generis organisaties kan de JenV Cloudstrategie dienen als referentiedocument. Deze onderdelen zijn zelfstandig verantwoordelijk voor hun eigen IV/IT-beleid en -strategie en dus ook hun eigen cloudstrategie. Gezien het ketenbelang en ketenafhankelijkheid van de JenV onderdelen en de Sui Generis organisaties is het van belang dat er onderlinge afstemming is over deze strategieën. De gemaakte keuzes en afwegingen kennen een doorwerking in de keten welke zonder deze afstemming leidt tot knelpunten in de keten. Het cloud afwegingskader is hierin richtinggevend.

De hoofdredenen voor het gebruik van *public cloud* diensten zijn de volgende:
- Vergroten van de snelheid en wendbaarheid van de Informatie Voorziening (IV);
- Het adequaat kunnen inzetten en benutten van technische cloud gebaseerde innovaties;
- Het creëren van een cloud-ready organisatie, ten behoeve van de realisatie van een toekomstbestendig landschap en het voorkomen van achterstand risico's.

De cloud visie en strategie zijn:

Cloud Visie:

JenV maakt gebruik van, en zal steeds meer, op een verantwoorde manier gebruik maken van de publieke cloud en de daarin aangeboden diensten, voor haar bedrijfsvoerings, beleidsmatige en operationele taken. Hierbij zullen diensten geïntegreerd zijn met de traditionele on-premise omgevingen van JenV waardoor sprake is van een hybride omgeving. Gebruik van publieke cloud maakt JenV meer wendbaar, innovatief en klaar voor huidige en toekomstige ICT-ontwikkelingen en noodzakelijk om de risico's van legacy ICT te voorkomen.

Cloudstrategie

"De cloudstrategie draagt op JenV–breed niveau bij aan de efficiënte en flexibele levering van kwalitatief hoogwaardige en innovatieve ICT-dienstverlening, waarbij JenV optimaal op de toekomst is voorbereid. Dit doen we door de inzet en het gebruik van clouddiensten op een voor het onderdeel juiste snelheden en op gecontroleerde, veilige en zorgvuldige wijze verder te ontwikkelen en te implementeren."

1 De Publieke Cloud: dit zijn generieke cloud-diensten die in principe door elke organisatie of persoon gratis of via betaling kunnen worden afgenomen.

2 De mogelijkheid van een overheidspartij (JenV) om haar rol en wettelijke taken in de digitale wereld onafhankelijk, zelfbepaald en veilig te kunnen uitoefenen.

3 https://ec.europa.eu/info/publications/european-commission-cloud-strategy_en

4 https://www.rijksoverheid.nl/documenten/kamerstukken/2022/08/29/kamerbrief-rijksbreed-cloudbeleid-2022

De JenV cloudstrategie gaat uit van samenwerking tussen de JenV onderdelen om de vaak schaarse kennis op het gebied van cloudtechnologie, -gebruik en -ontwikkelingen (zowel technisch, juridisch, privacy als security vlak) te bundelen, gezamenlijk ervaring op te doen en op basis van deze lessen en ervaringen de cloud adoptie verder te vergroten.

De implementatie-strategie gaat daarbij vanuit dat in het gebruik van clouddiensten bij organisaties met weinig ervaring en kennis gestart wordt met toepassingen met een relatief laag risico. Hierbij kan gedacht worden aan test- ontwikkelomgevingen of toepassingen waarvan de vertrouwelijkheid van data geen rol speelt. Vanuit daar zal op basis van een lerende organisatie en kennisopbouw deze doorgroeien naar het inzetten en faciliteren van productieomgevingen en diensten met een hogere vertrouwelijkheid. Op deze manier wordt de hoognodige cloud ervaring opgedaan die noodzakelijk is om JenV te laten profiteren van de mogelijkheden van de publieke cloud. Organisaties met uitgebreide ervaring of kennis op het gebied van cloud kunnen hierin voortvarender ter werk gaan. In de afgelopen 4 jaar is deze kennis sterk toegenomen en bij meerdere JenV organisaties in hogere mate van volwassenheid aanwezig.

Met de inzet van public clouddiensten ontstaan relaties met publieke IT-dienstenleveranciers van buiten het (Rijks)overheidsdomein. Dergelijke afhankelijkheden moeten worden beoordeeld met betrekking tot aandachtspunten om bedreigingen van de digitale soevereiniteit van JenV uit te sluiten of op zijn minst te beperken. Digitale soevereiniteit en data-autonomie dienen ook in de publieke cloud te worden gewaarborgd. Om invulling en borging te geven aan de digitale soevereiniteit hebben we de volgende richtinggevende principes gedefinieerd. Deze vormen een afwegingskader voor het nemen van besluiten ten aanzien van clouddiensten door het Ministerie van Justitie en Veiligheid.

Het JenV Cloudbeleid onderdeel van de Cloudstrategie hanteert de volgende richtinggevende principes[5]:

- We hanteren een Multi-vendor strategie
- We zorgen voor een veilige ontsluiting via JuBIT
  JuBIT staat voor Justitie Beveiligde Internet Toegang.
- We houden IAM in eigen beheer
  IAM staat voor een gemeenschappelijke Identity management en Access managementvoorziening.
- We monitoren vanuit het JenV SOC[6]
  Het Security Operations Center (SOC) JenV staat geheel in het teken staat van de informatiebeveiliging van het ministerie.
- We passen privacy by design en security by design toe.

De eisen en bepaling van de security eisen voor een Publieke Cloud toepassing zijn in wezen niet anders dan voor een ‘on premise’ toepassing van een leverancier of een product of dienst in eigen beheer. Door de aard van Publieke Clouddiensten liggen de risico’s echter anders dan bij de traditionele oplossingen. De mate van directe invloed op de genomen beveiligingsmaatregelen bij de cloud leverancier zijn beperkter en het zicht en invloed op de implementatie van de genomen beveiligingsmaatregelen is bij cloud oplossingen lastiger.

Om die reden heeft JenV een gemeenschappelijke **JenV ‘Trusted’ cloud (Sovereign Cloud)** in het gebruik van grote Cloud Service Providers (CSP’s) ontwikkeld. In dit concept worden eigen[7] stuurmiddelen op het gebied van beveiliging ingezet op de af te nemen publieke cloud(dienst). Dit betreft zowel netwerkbeveiliging, identiteitscontrole als monitoring en data-encryptie.
Naast de maatregelen om tot een dergelijke trusted cloud(dienst) te komen, dienen de JenV-onderdelen eigen maatregelen conform de kaders van de BIO in te richten (de informatiebeveiligingseisen voor functionaliteit in de cloud zijn niet anders dan voor een

5 Deze staan verder uitgewerkt in het document “Min JenV - Cloud uitgangspunten - 20190927”. Sui generis organisaties zijn zelfstandig verantwoordelijk voor hun eigen invulling hiervan.

6 Sui generis organisaties zijn zelfstandig verantwoordelijk voor hun eigen invulling hiervan en maken veelal gebruik van een eigen SOC.

7 Gezamenlijke maatregelen eventueel aangevuld met organisatie eigen maatregelen

applicatie *on-premise*). Hiervoor is een Cloud Security en Privacy Control Framework opgesteld welke de JenV onderdelen ondersteunt in de verplichte maatregelen die nodig zijn op het gebied van security en privacy.

Bij een implementatie met inachtneming van alle toepasselijke wet- en regelgeving, inclusief op het gebied van informatiebeveiliging en privacy, is het voor JenV (voor de uitvoering van bepaalde taken) goed mogelijk om gebruik te maken van de publieke cloud. **Gecontroleerd, veilig** en **zorgvuldig** zijn hierbij de belangrijke randvoorwaarden.

Inhoud

1 Achtergrond en aanleiding

1.1 Aanleiding opstellen Bestuurlijke Cloudstrategie JenV

In december 2020 is in de Brede Bestuursraad de JenV-brede bestuurlijke cloudstrategie vastgesteld. Deze is nu in de versie van 2024 aangescherpt op basis van de huidige ontwikkelingen en status.

De cloudstrategie geeft invullingen aan:

- De wens en noodzaak om samenhang te hebben tussen de verschillende onderliggende cloudstrategieën van de onderdelen;
- De behoefte om duidelijkheid te creëren over het cloud gebruik binnen JenV;
- De ketenafhankelijkheden te adresseren;
- De risico's op het gebied van internationaal privaatrecht en botsende rechtsregimes te adresseren;
- De wens om kennis binnen JenV te delen;
- Groeiend belang van ketensamenwerking waarbij ook de informatie-uitwisseling in digitale vorm een cruciale rol speelt;
- Duidelijkheid over de reikwijdte van de cloudstrategie van JenV;

1.2 Politiek bestuurlijke context en achtergrond

Inmiddels is de Verkenning van het Cloudbeleid uit 2019 omgezet in Rijksbreed Cloudbeleid vastgesteld in de Misterraad van 29-8-2022.
Hierin is opgenomen dat op basis daarvan alle departementen hun eigen cloudbeleid en cloudstrategie formuleren.

1.3 Het belang van publieke clouddiensten voor JenV

Steeds vaker wordt de cloud gezien als een aanjager van nieuwe technologieën. Deze kunnen liggen op het vlak van data-analyse, de inzet van Artificiële Intelligentie (AI)[8], maar ook op het vlak van verbinding van IoT-devices (Internet of Things)[9] of nieuwe toepassingen die enkel in de cloud worden aangeboden. De cloud maakt het mogelijk om snel innovatieve ideeën te testen. Ze stimuleert een data-gedreven cultuur op basis van gezamenlijke besluitvorming en biedt een platform voor het ontwikkelen van nieuwe technologieën. Niet alleen innovatieve technologieën verplaatsen steeds vaker naar de cloud. Ook bestaande applicaties worden steeds vaker enkel nog maar aangeboden via de cloud. Dit werd tijdens de coronacrisis pijnlijk duidelijk. Het thuiswerken betekende bijvoorbeeld dat wij een andere manier van vergaderen hebben moeten omarmen. De tools om dit te doen zijn veelal clouddiensten, ingezet door zowel JenV als de rest van de overheid, zoals Webex en Teams, beide clouddiensten. Andere bekende gebruikte cloudiensten, binnen JenV zijn onder andere: WhatsApp, diensten op de JenV IPhone/iPad (volledig geïntegreerd met iCloud), Microsft365, Facebook, YouTube, LinkedIn, Twitter, Instagram, etc..

Een ander belangrijk voordeel van cloudcomputing is dat het mee kan helpen om de organisatie wendbaarder en flexibeler te maken. Het vergroten van de snelheid en wendbaarheid van de IV-voorziening vergroot de slagkracht en uitvoeringssnelheid van JenV. De traditionele aanpak van aanschaf van hardware, installeren en onderhouden van software en applicaties verdwijnt. De snelheid waarmee nieuwe functionaliteit in gebruik kan worden genomen neemt daardoor enorm toe.

1.4 Wat is cloud computing?

De standaard definitie van cloud computing, die ook in dit document wordt gebruikt, is de definitie van het National Institute of Standards and Technology (NIST) (Mell & Grance, September 2011)[10], een USA overheidsinstituut; vertaald naar het Nederlands:

8 Artificiële intelligentie (AI) is de wetenschap die zich bezighoudt met het creëren van een artefact dat een vorm van intelligentie vertoont.

9 Niet alleen mensen zijn online, ook dingen. Denk aan machines, sieraden, auto's, de thermostaat en de koelkast. Ze vormen samen een groot 'internet of things', oftewel het internet der dingen.

10 https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp

"Cloud computing is een model om op afroep op een gemakkelijke manier via een netwerk onbeperkt toegang te krijgen tot een gedeelde verzameling van configureerbare computermiddelen (bijvoorbeeld netwerken, servers, opslag, toepassingen/applicaties en diensten) die snel kunnen worden geleverd en vrijgegeven met een minimale beheersinspanning of tussenkomst van de leveranciers".

In de loop der jaren zijn er binnen Cloud computing diverse **servicemodellen** ontstaan. NIST heeft de volgende hoofdindeling:

Software as a Service:
De leverancier biedt de klant de mogelijkheid om gebruik te maken van applicaties van de leverancier, welke draaien op een cloudinfrastructuur. De klant heeft geen controle over de onderliggende cloudinfrastructuur, of de toepassingsmogelijkheden; met uitzondering van een beperkte set aan gebruiker specifieke configuratie instellingen.

Platform as a Service:
De leverancier biedt de klant de mogelijkheid door de klant zelf gemaakte of verworven applicaties te implementeren. De klant heeft geen controle over de onderliggende cloudinfrastructuur, maar heeft controle over de geïmplementeerde applicaties; en mogelijk over diverse configuratie-instellingen voor de applicatie-hostingomgeving.

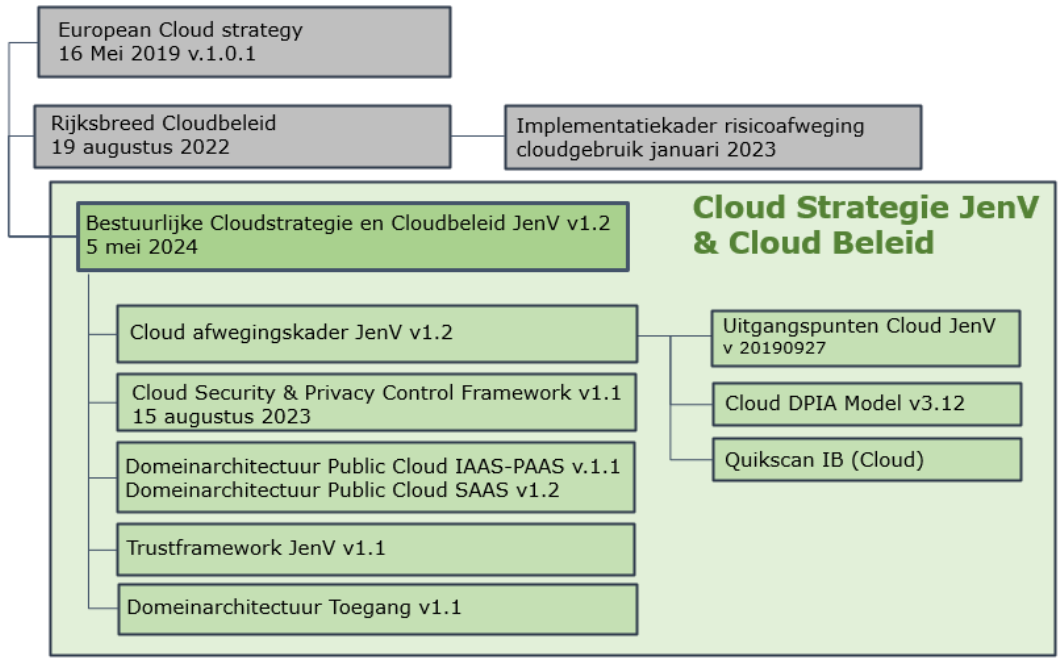
Infrastructure as a Service:
De leverancier biedt de klant verwerking, opslag, netwerken en andere fundamentele computermiddelen, waarmee de consument in staat is om willekeurige software te implementeren en uit te voeren. De klant heeft geen controle over de onderliggende cloudinfrastructuur, maar wel over de geïmplementeerde besturingssystemen, geïnstalleerde applicaties en gegevens; en mogelijk beperkte controle over geselecteerde netwerkcomponenten.

Public Cloud:
Hierbij richt de provider van de clouddienst op het leveren van een SAAS-, PAAS- of IAAS-dienst die is ingericht voor open gebruik door het grote publiek.
Veel van deze diensten worden geleverd door Cloud Service Providers vanuit hun eigen Datacenters. Of stellen de CSP's hun Cloudinfrastructuur beschikbaar aan derden om met inzet van deze infrastructuur eigen diensten aan te bieden (dit zou je kunnen vergelijken met het aanbieden van Apps door derden op bijv. Apple en Android telefoontoestellen).

Deze strategie gaat over het gebruik van de public cloud en focust zich zowel op de IaaS, PaaS en SaaS servicemodellen.

1.5 De componenten van de JenV Cloudstrategie en JenV Cloudbeleid

De JenV Cloudstrategie en het JenV Cloudbeleid bestaat uit een aantal samenhangende documenten die JenV in staat stelt afgewogen besluiten te nemen ten aanzien van clouddienstverlening. Zie figuur 1. Dit document is het hoofddocument waarin de JenV cloudstrategie en het JenV Cloudbeleid beschreven wordt.



Figuur 1: De Cloudstrategie JenV v1.2 (dit document) met onderliggende documenten irt omgeving.

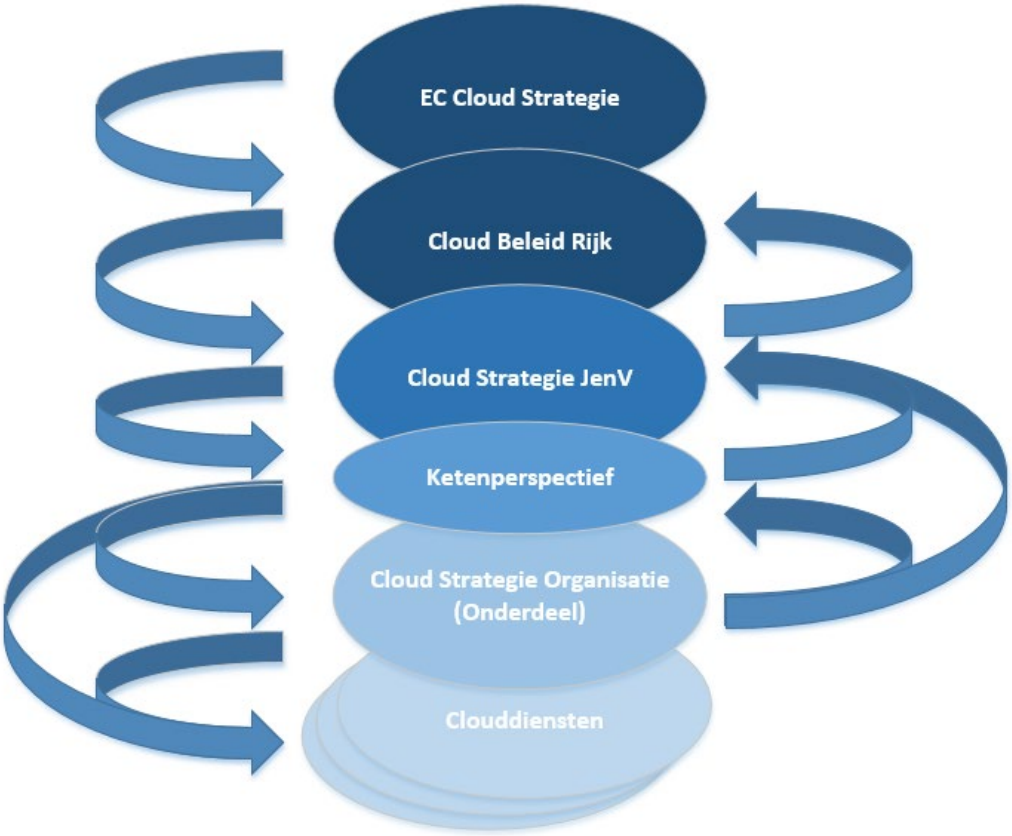
Als losse bijlagen bij dit document zijn gevoegd:

- Het cloud afwegingskader JenV (inclusief het cloud DPIA model)
- Cloud uitgangspunten JenV
- Cloud Security & Privacy Control Framework
- De Cloud architectuur JenV (IAAS-PAAS en SAAS)
- Trustframework JenV
- Domein Architectuur Toegang

2 Positionering en besturing

2.1 Positionering van de bestuurlijke Cloudstrategie JenV

De cloudstrategie van JenV staat niet op zichzelf. In onderstaande figuur is aangegeven hoe de cloudstrategie JenV zich verhoudt tot de EC cloudstrategie, het cloud beleid Rijk, het ketenperspectief en de organisatie specifieke cloudstrategieën.



De ***EC Cloudstrategie***[11] van de Europese Commissie heeft als visie een ***Cloud First*** aanpak met de inzet van beveiligde hybride multi-cloud diensten.
Het ***Cloud Beleid Rijk*** [12] bevat voor het hele Rijk de kaders (beleid) ten aanzien van de inzet van clouddiensten.
De ***Cloudstrategie JenV*** sluit aan op het cloudbeleid van het Rijk. JenV volgt daarin 1 op 1 het Rijksbrede Cloudbeleid en beschrijft/detailleert op JenV niveau onder meer hoe op ***een beheerste en veilige*** manier en met de implementatie van de noodzakelijke waarborgen gebruik kan worden gemaakt van publieke clouddiensten.
Het ***ketenperspectief***[13] beschrijft de randvoorwaarden voor clouddienstverlening voor onderdelen en diensten die deel uit maken van een keten en is randvoorwaardelijk voor onderliggende diensten. Per keten is het van belang een ketenperspectief op te zetten.
In de ***cloudstrategie per organisatie*** *(onderdeel)* wordt nader uitgewerkt hoe ***cloud dienstverlening*** per onderdeel kan worden ingezet met inachtneming van de kaders die door JenV en de keten worden opgegeven. Tevens beschrijft dit document eventuele afwijkingen t.o.v. de Cloudstrategie JenV.

11 https://ec.europa.eu/info/publications/european-commission-cloud-strategy_en
12 "Verkenning cloudbeleid voor de rijksdienst"
13 Door de verschillende ketens bij JenV zelf op te stellen

2.2 Besturing

De cloudstrategie van JenV staat niet op zichzelf, maar heeft relaties met de cloudstrategie van de Europese Commissie waar Nederland zich aan heeft gecommitteerd, het Rijksbrede cloudbeleid, het ketenperspectief en de organisatie specifieke cloudstrategieën. De verantwoordelijke voor de Cloudstrategie JenV is CIO van het Ministerie van Justitie en Veiligheid. De opdrachtgever voor beheer en doorontwikkeling van de strategie is de directeur van de directie Informatievoorziening en Inkoop (DI&I). DI&I/CIO-office JenV zorgt tevens voor ondersteuning bij het gebruik van de cloudstrategie. De Cloudstrategie JenV ondersteunt alle organisaties van het Ministerie van Justitie en Veiligheid bij het nemen van beslissingen over het gebruik van cloud dienstverlening.

2.3 Reikwijdte van de Cloudstrategie JenV

De Cloudstrategie JenV ondersteunt alle organisaties van het Ministerie van Justitie en Veiligheid bij het nemen van beslissingen over het gebruik van cloud dienstverlening. De cloudstrategie is een gezamenlijke strategie en beschrijft middels het JenV brede Cloudbeleid de randvoorwaarden, afwegingen en kaders waaraan een onderdeel van JenV moeten voldoen bij de sourcing van publieke clouddiensten.

De Cloudstrategie JenV inclusief onderliggende documenten is van toepassing voor alle JenV onderdelen en ZBO's vallende onder JenV. Voor de onderdelen onder ministeriële verantwoordelijkheid heeft het strategiedocument daarin een "comply" or "explain" status en is het onderliggende afwegingskader kaderstellend. Voor de Sui Generis organisaties kan de JenV Cloudstrategie dienen als referentiedocument. Deze onderdelen zijn zelfstandig verantwoordelijk voor hun eigen IV/IT-beleid en -strategie en dus ook hun eigen cloudstrategie. Gezien het ketenbelang en ketenafhankelijkheid van de JenV onderdelen en de Sui Generis organisaties is het van belang dat er onderlinge afstemming is over deze strategieën. De gemaakte keuzes en afwegingen kennen een doorwerking in de keten welke zonder deze afstemming leidt tot knelpunten in de keten. Het cloud afwegingskader is hierin richtinggevend.

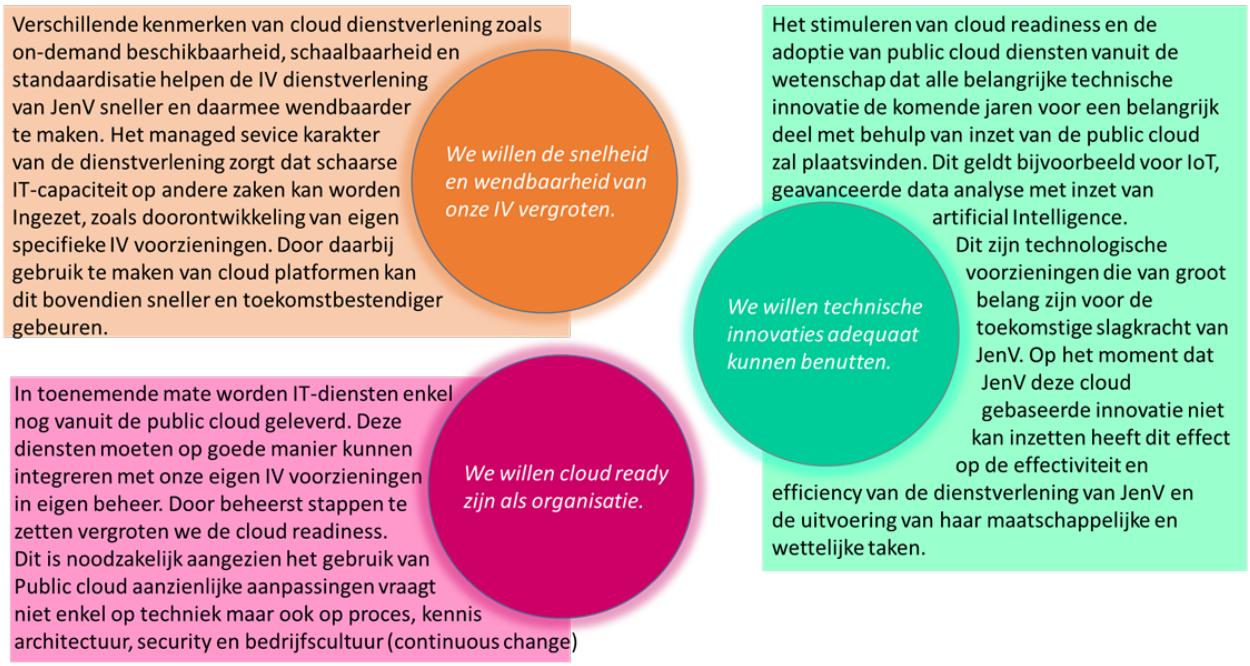
2.4 Clouddiensten: Een sourcingsvraagstuk

Clouddienstverlening is in de meeste opzichten niet anders dan andere soorten van IV-dienstverlening. Veel van de kaders en regels die derhalve voor deze "normale" dienstverlening gelden, gelden ook voor cloud vraagstukken. De vraag vanuit een organisatie om gebruik te gaan maken van cloud technologie is dus ook een sourcingsvraag en daarmee ook onderdeel van de sourcingstrategie JenV.

3 Het Cloud vraagstuk: strategie en doel

De informatievoorziening van JenV is omvangrijk, veelzijdig en complex gezien de ketens en netwerkorganisatie waarin JenV en haar partners opereren. Binnen JenV worden (digitale) diensten aan burgers en bedrijven ontwikkeld. Van belang is dat deze diensten niet alleen gebruiksvriendelijk zijn maar tevens dat deze flexibel ingericht zijn. JenV moet toegankelijk, veilig en vraaggericht opereren met de diensten die zij aan burgers en bedrijfsleven digitaal aanbiedt. De inzet van Publieke Clouddiensten levert daarin kansen en mogelijkheden, maar is tevens noodzaak in het veranderend ICT-landschap. Gelet op de genoemde complexiteit van de informatievoorziening van JenV, de integratie en afname van publieke clouddiensten en de effecten die niet enkel technisch van aard zijn voorziet de JenV strategie in de mogelijkheid om de flexibiliteit en innovatie van publieke clouddiensten te kunnen benutten.

De hoofdredenen voor het gebruik van publieke clouddiensten zijn de volgende:
- Vergroten van de snelheid en wendbaarheid van de Informatie Voorziening (IV);
- Het adequaat kunnen inzetten en benutten van technische cloud gebaseerde innovaties;
- Het creëren van een cloud-ready organisatie, ten behoeve van de realisatie van een toekomstbestendig landschap en het voorkomen van achterstand risico's.



Bron: cloudervaringsdocument NCSC[14]

3.1 Visie, Strategie en doelen

Uitgangspunt bij het gebruik van publieke clouddiensten is dat dit bijdraagt aan het realiseren van zowel de bedrijfs- als de (IV) doelstellingen van het Ministerie van Justitie en Veiligheid. De belangrijkste ambities waaraan deze cloudstrategie bijdraagt zijn o.a.:

- Een meer flexibele en wendbare organisatie
- Meer mogelijkheden tot inzet van innovatie
- Meer mogelijkheden in de Digitale transformatie

14 https://www.ncsc.nl/documenten/rapporten/juni/ervaringsdocument/20/cloudervaringsdocument

Cloud Visie:

JenV maakt gebruik van, en zal steeds meer, op een verantwoorde manier gebruik maken van de publieke cloud en de daarin aangeboden diensten, voor haar bedrijfsvoerings, beleidsmatige en operationele taken. Hierbij zullen diensten geïntegreerd zijn met de traditionele on-premise omgevingen van JenV waardoor sprake is van een hybride omgeving. Gebruik van publieke cloud maakt JenV meer wendbaar, innovatief en klaar voor huidige en toekomstige ICT-ontwikkelingen en noodzakelijk om de risico's van legacy ICT te voorkomen.

Cloudstrategie:

"De cloudstrategie draagt op JenV–breed niveau bij aan de efficiënte en flexibele levering van kwalitatief hoogwaardige en innovatieve ICT-dienstverlening, waarbij JenV optimaal op de toekomst is voorbereid. Dit doen we door de inzet en het gebruik van clouddiensten op een voor het onderdeel juiste snelheden en op gecontroleerde, veilige en zorgvuldige wijze verder te ontwikkelen en te implementeren."

Deze strategie focust zich daarbij verder op het creëren van een JenV ***'Trusted Cloud'*** (Sovereign Cloud) die de wendbaarheid, innovatie en nieuwe ontwikkelingen ondersteunt. Belangrijke randvoorwaarden daarbij zijn; behoud van onafhankelijkheid, digitale soevereiniteit en data-autonomie, informatiebeveiliging en gegevensbescherming.

Het doel van de JenV cloudstrategie is om met de inzet ***van publieke clouddiensten*** op een gecontroleerde, veilige en zorgvuldige manier de JenV-processen en -organisatie verder te optimaliseren, te innoveren en wendbaarder te maken. In te kunnen spelen op toekomstige ontwikkelingen en disruptieve ontwikkelingen die het gebruik van cloud met zich mee brengt.

Hiermee willen we het volgende bereiken:

Vergroten van de snelheid en wendbaarheid van de Informatie Voorziening (IV)
Het vergroten van de snelheid en wendbaarheid van de IV-voorziening vergroot de slagkracht en uitvoeringssnelheid van JenV. De traditionele aanpak van aanschaf van hardware, installeren van software en applicaties verdwijnt. De snelheid waarmee nieuwe platformen en applicaties in gebruik kunnen worden genomen neemt daardoor enorm toe. Als ook het feit dat de cloud voornamelijk gebaseerd is op hardware- en OS-agnostische toepassingen levert een grote versnelling in het ontwikkelproces.

Het adequaat kunnen inzetten en benutten van technische innovaties
In toenemende mate worden IT-diensten enkel nog vanuit de public cloud geleverd. Office365 en nieuwe technologieën als in de inzet van real-time data-analyse middels Artificial Intelligence zijn daar voorbeelden van. De tooling daarvoor wordt als cloudnative product aangeboden. Deze diensten moeten daarbij op goede manier kunnen integreren met onze eigen on-premise voorzieningen.

Het creëren van een cloud-ready organisatie, ten behoeve van de realisatie van een toekomstbestendig landschap en het voorkomen van achterstand risico's
Het stimuleren van cloud readiness en de adoptie van public cloud diensten vanuit de wetenschap dat alle belangrijke technische innovatie de komende jaren voor een belangrijk deel met behulp van inzet van de public cloud zal plaatsvinden. De inzet van nieuwe technologische voorzieningen zijn van groot belang zijn voor de toekomstige slagkracht van JenV. Op het moment dat JenV deze cloud gebaseerde innovatie niet kan inzetten heeft dit effect op de effectiviteit en efficiency van de dienstverlening van JenV en de uitvoering van haar maatschappelijke en wettelijke taken.

Het stimuleren van cloud readiness en de adoptie van public cloud diensten vanuit de wetenschap dat alle belangrijke technische innovatie de komende jaren voor een belangrijk deel met behulp van inzet van public clouddiensten zal plaatsvinden. De inzet van nieuwe technologische voorzieningen zijn van groot belang zijn voor de toekomstige slagkracht van JenV. Op het moment dat JenV deze cloud gebaseerde innovatie niet kan inzetten heeft dit effect op de effectiviteit en efficiency van de dienstverlening van JenV en de uitvoering van haar maatschappelijke en wettelijke taken.

Maar ook:

- Het verhogen van de kwaliteit van de ICT-dienstverlening: bij het verhogen van de kwaliteit van de ICT-dienstverlening zijn stabiele en flexibele dienstverlening en de juiste functionaliteit de kernbegrippen. Met bijzondere aandacht voor het borgen/verhogen van de kwaliteit van de dienstverlening m.b.t. het primair proces en ketens;
- Het verhogen van de efficiency: bereiken van schaalvoordelen. Daarbij zijn acceptabele, marktconforme en beheersbare kosten voor informatievoorziening leidend;
- Het ontwikkelen en borgen van (interne) kennis: betere toegang tot schaarse of juist beperkt benodigde deskundigheid en daarmee ook het verhogen van het aanpassingsvermogen m.b.t. adoptie van (proven) technologieën. Daarnaast het opbouwen en behouden van kennis binnen de eigen organisatie.

3.2 Digitale soevereiniteit

Met de inzet van publieke clouddiensten ontstaan relaties met publieke IT-dienstenleveranciers van buiten het (Rijks)overheidsdomein. Dergelijke afhankelijkheden moeten worden beoordeeld met betrekking tot aandachtspunten om bedreigingen van de digitale soevereiniteit van JenV uit te sluiten of op zijn minst te beperken. Digitale soevereiniteit en data-autonomie dienen ook in de publieke cloud te worden gewaarborgd. De hier gedefinieerde cloudstrategie onderkent de noodzaak om de onafhankelijkheid van cloud leveranciers te behouden en te versterken.
De toenemende concentratie van ICT-leveranciers op de markt zal dergelijke afhankelijkheden echter nog verder vergroten. Digitale soevereiniteit voor JenV wordt gedefinieerd als:

> ***De mogelijkheid van JenV om haar rol en wettelijke taken in de digitale wereld onafhankelijk, zelfbepaald en veilig te kunnen uitoefenen. (GAIAX definitie van digitale soevereiniteit)***

Een dergelijke onafhankelijke uitoefening is zeer belangrijk voor JenV om zo haar soevereine taken uit te voeren via digitale processen. Als de digitale soevereiniteit onvoldoende wordt gewaarborgd, kan het handelingsvermogen ernstig worden beperkt. Mede om deze reden wordt ingezet op het ***'Trusted Cloud'*** (Sovereign Cloud) concept, waarbij eigen maatregelen in de publieke cloud deze soevereiniteit zoveel mogelijk moeten beschermen en garanderen. Een 100% onafhankelijkheid kan niet worden gerealiseerd, maar dat geldt eveneens voor het huidige bestaande ICT-landschap. Deze afhankelijkheid mag er echter niet toe leiden dat JenV haar wettelijke taken niet langer zelfbepaald en veilig zou kunnen uitvoeren. Daarbij geldt dat er zoveel mogelijk zeggenschap moet zijn over de locatie waar de contentdata wordt opgeslagen (binnen de EU). Voor de data waar locatiegarantie niet mogelijk is, dienen contractuele afspraken te worden gemaakt (opslagtermijnen, verwerkingsinstructies, nevenverwerkingen niet toegestaan). De verwerking van persoonsgegevens wordt aan strikte instructies onderworpen en kunnen er controles plaatsvinden m.b.v. audits etc.

Het opgestelde JenV cloud afwegingskader ondersteunt bij het nemen van beslissingen over de inzet en gebruik van clouddiensten. Het gebruik van publiek clouddiensten vraagt tevens om de afweging tussen cloud toepassingen en inzet van eigen on-premise toepassingen. In dit kader kan gesproken worden over een hybride-cloudstrategie als ook een multi-cloudstrategie om de afhankelijkheid van één Cloud Service Leverancier daarmee te beperken.

3.3 Richtinggevende principes

Om invulling en borging te geven aan de digitale soevereiniteit hebben we de volgende richtinggevende principes gedefinieerd. Deze vormen een afwegingskader voor het nemen van besluiten ten aanzien van gebruik van publieke clouddiensten door het Ministerie van Justitie en Veiligheid.

De richtinggevende principes[15] zijn:

- We hanteren een Multi-vendor strategie
- We zorgen voor een veilige ontsluiting via JuBIT
  JuBIT staat voor Justitie Beveiligde Internet Toegang. De JuBIT dienstverlening vormt het beveiligd koppelvlak tussen het interne vertrouwde landelijke datacommunicatienetwerk (Justitienet) en externe netwerken zoals Internet, Partnernetwerken (Publieke partijen en semi-overheidspartijen) en Overheidsnetwerken (Haagse Ring, Gemnet, Rinis, etc.). Naast de beveiligingsinfrastructuur omvat de dienstverlening aanvullende diensten en een groot aandeel (complexe) webhosting.
- We houden IAM in eigen beheer
  Identity en Access Management (IAM) is een overkoepelende voorziening voor processen die zich richten op het administreren en beheren van gebruikers en resources in het netwerk inclusief de toegangscontrole van de gebruikers op applicaties en systemen.
  Deze gemeenschappelijke voorziening(en) ondersteunt JenV-taakorganisaties bij:
    - Identity Management (IdM): het registreren, verifiëren en beheren van de identiteitsgegevens en de werkrelatie van medewerkers;
    - Access Management (AM): het beheren van de bevoegdheden (autorisaties) op voorzieningen van de geregistreerde personen.
- We monitoren vanuit het JenV SOC[16]
  Het Security Operations Center (SOC) JenV staat geheel in het teken staat van de informatiebeveiliging van het ministerie. Dit departementale SOC waakt over de digitale veiligheid van de gemeenschappelijke ICT-infrastructuur, systemen en applicaties die het ministerie van Justitie en Veiligheid gebruikt. Het SOC is een 'eigen' intern georganiseerde dienst binnen het ministerie van Justitie en Veiligheid.
- We passen privacy by design en security by design toe bij de opzet van elke cloudomgeving.

15 Deze staan verder uitgewerkt in het document "Cloud uitgangspunten JenV". Sui generis organisaties zijn zelfstandig verantwoordelijk voor hun eigen invulling hiervan.

16 Sui generis organisaties zijn zelfstandig verantwoordelijk voor hun eigen invulling hiervan en maken veelal gebruik van een eigen SOC.

4 JenV Cloudbeleid

4.1 JenV Cloudbeleid

Het JenV Cloudbeleid bestaat uit:

- Het JenV cloud afwegingskader, voor IaaS, PaaS en SaaS-diensten.
- De geïmplementeerde JenV '**Trusted Cloud'** als gemeenschappelijke dienst;
- Onderdeel van die 'trusted cloud' zijn tevens centrale beveiligingsdiensten t.a.v. data protectie, toegang, monitoring, kaders;
- Een Cloud domeinarchitectuur IAAS-PAAS en SAAS om richting te kunnen geven aan de Cloudarchitecturen.
- Monitoring en logging middels inzet van JenV SOC (security operations center) in een federatief model met de JenV onderdelen op verschillende niveaus.
- De integratie van public clouddiensten met eigen on-premise voorzieningen (hybride cloud)[17];
- Het hanteren van een '**multi cloud'** strategie als gemeenschappelijke dienst;

4.2 Samenwerking tussen de onderdelen

De JenV cloudstrategie gaat uit van samenwerking tussen de JenV onderdelen om de vaak schaarse kennis op het gebied van cloudtechnologie, -gebruik en -ontwikkelingen cloud (zowel technisch, juridisch, privacy als security vlak) te bundelen, gezamenlijk ervaring op te doen en op basis van deze lessen en ervaringen de cloud adoptie verder te vergroten.
De implementatie-strategie gaat daarbij vanuit dat in het gebruik van clouddiensten bij organisaties met weinig ervaring en kennis gestart wordt met toepassingen met een relatief laag risico. Hierbij kan gedacht worden aan test- ontwikkelomgevingen of toepassingen waarvan de vertrouwelijkheid van data geen rol speelt. Vanuit daar zal op basis van een lerende organisatie en kennisopbouw deze doorgroeien naar het inzetten en faciliteren van productieomgevingen en diensten met een hogere vertrouwelijkheid. Op deze manier wordt de hoognodige cloud ervaring opgedaan die noodzakelijk is om JenV te laten profiteren van de mogelijkheden van de publieke cloud. Organisaties met uitgebreide ervaring of kennis op het gebied van cloud kunnen hierin voortvarender ter werk gaan.

De samenwerking van de JenV onderdelen richt zich op het zorgvuldig gebruik van clouddiensten en het adequaat beveiligen van data en voorzieningen.
Primair doel is stimuleren en leren, om enerzijds te komen tot een cloud-ready organisatie en anderzijds een integratiesystematiek die veilig en schaalbaar is en waarmee we eenvoudig cloud voorzieningen kunnen op- en afschalen. Onderdeel van dit doel is het kunnen delen van code, informatiebeveiligingsinformatie en processen.
Cloud adoptie heeft eveneens gevolgen voor de security architectuur. Dit heeft onder meer te maken met het feit dat het gaat om managed services waarbij een ander (in dit geval de cloud serviceleverancier) grotendeels verantwoordelijk is voor de inzet van benodigde maatregelen maar de gebruiker verantwoordelijk blijft voor de juiste beveiliging van zijn data en voorzieningen.

Om het gebruik van de Publieke Cloud bij JenV onderdelen zoveel mogelijk samen te ontwikkelen, wordt vanuit het oogpunt van samenwerking, maar tevens ontzorging en kostenbesparing de volgende aspecten centraal binnen JenV geregeld:

- De verbinding met twee of drie van de grootste Cloud Service Providers (CSP's) wordt centraal gerealiseerd (via de internettoegangsdienst JUBIT), zodat onderdelen van JenV daar eenvoudig op kunnen aansluiten, waarbij partijen die dat nodig hebben over eigen koppelingen kunnen beschikken mits deze deel uitmaken van het JenV-trusted cloud concept;
- Zoveel mogelijke generieke infrastructuur beveiligingsmaatregelen conform BIO BBN2 niveau zullen centraal worden aangebracht conform het JenV trusted cloud

17 On-premise voorzieningen naast public cloud voorzieningen

concept, waar bovenop de JenV-Onderdelen de eigen maatregelen stapelen om te kunnen komen op basis van Risico Analyse op BIO-BBN3 niveau.
- Er is inmiddels met Microsoft een Rijksbrede overkoepelende overeenkomst gesloten waardoor een deel van de Microsoft producten en diensten in overeenstemming met de AVG gebruikt kunnen worden zoals in de kamerbrief[18] van 1 juli 2019 gerapporteerd.
- Met andere Cloudleveranciers worden gelijksoortige overkoepelende overeenkomsten (Framework Agreements) gesloten, zoals met Amazone Web Services (per 1 juni 2023) om zo te borgen dat die aanbieders de gegevens uitsluitend inzetten met de benodigde privacy waarborgen;
- Samenwerkings- en Code sharings platform t.b.v. kennisdeling en versterking;
- Communicatie platform.

Het JenV cloud afwegingskader is geformuleerd uitgaande van deze uitgangspunten en gemeenschappelijke beveiligingsmaatregelen. Deze maatregelen zijn beschreven in de JenV domeinarchitectuur cloud, deze is onder coördinatie van DI&I ingeregeld, als eerste in de Microsoft Azure Cloud. Hiermee is sprake van generieke maatregelen en waarbij ieder JenV onderdeel zelf nog specifieke maatregelen zal moeten aanbrengen op basis van het afwegingskader en zoals gedefinieerd in het Cloud Security en Privacy Control Framework.

4.3 Implementatie van Trusted Cloud JenV

De eisen en bepaling van de security eisen voor een Publieke Cloud omgeving in wezen niet anders dan voor een 'on premise' omgeving van een leverancier of een omgeving in eigen beheer. Door de aard van Publieke Clouddiensten liggen de risico's echter anders dan bij de traditionele oplossingen. De mate van directe invloed op de genomen beveiligingsmaatregelen bij de Cloud leverancier zijn beperkter en het zicht en invloed op de implementatie van de genomen beveiligingsmaatregelen is bij Cloud oplossingen lastiger.
Om die reden kiest JenV bij de inzet van public clouddiensten voor een implementatie conform een **'Trusted' cloud concept**. In dit concept worden eigen[19] stuurmiddelen op het gebied van beveiliging ingezet op de af te nemen publieke cloud(dienst). Dit betreft zowel netwerkbeveiliging, identiteitscontrole als monitoring en data-encryptie.
Naast de maatregelen om tot een dergelijke trusted cloud(dienst) te komen, dienen de JenV-onderdelen zoals gewoonlijk de maatregelen conform de kaders van de BIO in te richten (de informatiebeveiligingseisen voor functionaliteit in de cloud zijn niet anders dan voor een applicatie *on-premise*).
Vertrekpunt is dat de organisatie inschat hoe kritiek de eigen processen zijn en de bijbehorende data die daarin verwerkt wordt. Uiteindelijk gaat het erom welk risico de organisatie bereid is te nemen op de eerdergenoemde betrouwbaarheidseisen. Hiervoor is een standaard Informatie Beveiligings (IB) proces beschikbaar. Ten behoeve van de inzet van publieke clouddiensten is er in het JenV Cloudafwegingskader en Cloud Security en Privacy Control Framework, rekening gehouden met een aantal cloud specifieke IB-risico's.
Om JenV uitvoeringsorganisaties die de stap naar Public Cloud overwegen te ondersteunen is tevens het gebruiksvriendelijke Cloud specifieke DPIA-model ontwikkeld, dat organisaties kunnen hanteren om privacy risico's zorgvuldig af te kunnen wegen. Het Cloud DPIA Model is eveneens onderdeel van het JenV Cloudafwegingskader.

18 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019Z13829&did=2019D28465
19 Gezamenlijke maatregelen eventueel aangevuld met organisatie eigen maatregelen

5 Cloud computing; het juridisch en security kader

5.1 Het juridisch kader

Elke organisatie moet voldoen aan de toepasselijke wet- en regelgeving. Gebruik maken van Clouddiensten kan diep ingrijpen op de informatiehuishouding van de organisatie[20]. Omdat de gegevens zich veelal niet in Nederland bevinden en er vaak wordt gewerkt met buitenlandse bedrijven is niet alleen de nationale wet- en regelgeving van belang bij cloud computing. Internationale regelgeving kan ook van toepassing zijn en daarbij zelfs botsen met nationale wet- en regelgeving. Denk hierbij bijvoorbeeld aan de CLOUD-act en de FIS-act van de VS. De verschillende wet en regelgeving evenals de impact op de nationale wet- en regelgeving staat verder beschreven in het cloud afwegingskader JenV.

5.2 Het security kader

Net als bij alle andere IV-systemen van de overheid moeten ook cloud systemen voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). Deze helpt het lijnmanagement bij het nemen van zijn verantwoordelijkheid ten aanzien van informatiebeveiliging. Specifiek voor cloud computing is het BIO Thema[21]:
"Clouddiensten" uitgewerkt. Dit themadocument over clouddiensten, is in opdracht van BZK door het CIP opgesteld om overheidsorganisaties een beeld te geven van de meest relevante onderwerpen bij het verwerven van veilige clouddiensten. In het cloud afwegingskader JenV wordt verder ingegaan op de security aspecten van cloud computing. In het Cloud Security en Privacy Control Framework worden de diverse Cloud beveiligings en privacy risico benoemt en aanbevelingen gedaan welke maatregelen daarin een verplichtend karakter hebben naast een aantal maatregelen gebaseerd op de eigen Risico Analyse en in geval van persoonsgegevens uitgevoerde DPIA.

20 Whitepaper NCSC Cloudcomputing & Security - Januari 2012.
21 https://cip-overheid.nl/media/1422/26022020-themadocument-clouddiensten-10.pdf

Dit is een uitgave van:

Directie Informatievoorziening en Inkoop
Ministerie van Justitie en Veiligheid
Turfmarkt 147 | 2511 DP Den Haag
Postbus 20301 | 2500 EH Den Haag

www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid

Mei 2024