E-Space Adviesdocument - Werkversie

Onderzoek naar standaarden en standaardisatieactiviteiten voor Cloud

E-Space Adviesdocument
Werkversie 14 augustus 2023

Deze versie:
https://brienen.github.io/onderzoek-cloudstandaarden/

Laatst gepubliceerde versie:
https://brienen.github.io/publish/dk/onderzoek cloudstandaarden

Laatste werkversie:
https://brienen.github.io/onderzoek-cloudstandaarden/

Vorige versie:
https://brienen.github.io/publish/dk/wv-ad-onderzoek cloudstandaarden-20230813

Redacteur:
Auteurs:
Arjen Brienen (E-Space)
Jeroen de Ruig (E-Space)

Doe mee:
GitHub brienen/onderzoek-cloudstandaarden
Dien een melding in
Revisiehistorie
Pull requests

Dit document is ook beschikbaar in dit niet-normatieve formaat: pdf

Samenvatting

Tekst

Status van dit document

Dit is een werkversie die op elk moment kan worden gewijzigd, verwijderd of vervangen door andere documenten. Het is geen door het TO goedgekeurde consultatieversie.

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

In uw offerteaanvraag schetst u de context van de beoogde opdracht via de kamerbrief Rijksbreed cloudbeleid 2022 en de belangrijke rol van standaardisatie en in het bijzonder standaarden voor portabiliteit van gegevens, cloud-interoperabiliteit en informatieveiligheid.

Bureau Forum Standaardisatie zet namens Forum Standaardisatie de beoogde opdracht uit met de volgende opdrachtomschrijving:

> Om de digitale overheid gevraagd en ongevraagd te kunnen adviseren over standaardisatie voor de Cloud, wil het Forum Standaardisatie graag een beeld krijgen van de standaarden die van strategisch belang zijn voor het Cloudbeleid. In het bijzonder wil Forum Standaardisatie weten welke cruciale standaarden al bestaan, welke nog moeten worden gespecificeerd, en op welke (Europese en internationale) standaardisatie- activiteiten de overheid nog invloed op kan en zou moeten uitoefenen.

1.2 Hoofdvraag

Wij vragen de opdrachtnemer om een onderzoek uit te voeren dat een beeld geeft van de Europese, internationale en nationale standaarden en standaardisatieactiviteiten die relevant zijn voor Cloud platformen, systemen en diensten. Tevens vragen wij aan de opdrachtnemer om ‘witte vlekken’ te identificeren, dat wil zeggen domeinen waar open standaarden voor de Cloud nodig zijn maar nog niet bestaan.

1.3 Deelvragen

Hierbij vraagt u ons de volgende onderzoeksvragen te beantwoorden:

1. Welke Europese, internationale en nationale standaarden bestaan er voor Cloud, in het bijzonder voor Cloud-interoperabiliteit, dataportabiliteit, informatieveiligheid en processen?

2. Welke Europese, internationale en nationale Cloud-standaarden zijn nog in ontwikkeling, of gepland?

3. Zijn er witte vlekken? Dat wil zeggen, Cloud-technologieën of - toepassingen waar open standaarden nodig zijn, maar nog niet bestaan en nog niet ontwikkeling zijn?

4. Op welke (Europese en internationale) standaardisatieactiviteiten voor Cloud zou de overheid of de private sector in Nederland invloed op moeten uitoefenen? Bijvoorbeeld omdat zij zich bewegen in een richting die niet overeenstemt met Nederlandse waarden zoals openheid, inclusie, veiligheid, privacy, digitale soevereiniteit, en een evenwichtige markt? En is dat nog mogelijk?

§ 1.4 Aanpak en betrokkenen

Voor dit onderzoek zijn allereerst bestaande onderzoeken en bronnen geanalyseerd. (zie bijlage 1). Vervolgens hebben er individuele interviews plaatsgevonden met experts op het gebied van standaarden, normeringen, digitale identiteit, Europese en Nederlandse digitale ontwikkelingen en ontwerp en architectuur. De gesprekken hebben plaatsgevonden van medio oktober tot medio november. Hiermee is een beeld ontstaan van de huidige stand van zaken met betrekking tot standaarden voor Regie op Gegevens en meningen die op dat moment leefde. De opgehaalde inzichten uit de gesprekken zijn geanalyseerd en vergeleken met de bestaande informatie en onderzoeken. Op basis hiervan zijn vervolgens de conclusies en aanbevelingen uit deze verkenning opgesteld. Daarna is op 1 december een expert bijeenkomst geweest waarin de resultaten van de verkenning zijn gepresenteerd en verschillende vraagstukken zijn besproken. De resultaten en individuele opmerkingen van de experts tijdens en na de expertbijeenkomst zijn zoveel mogelijk verwerkt in dit eindrapport.

Tabel 1

Aanpak verkenning

Wat	Activiteit	Resultaat	Wanneer
Voorbereiding	Gesprekken met opdrachtgever en adviseurs van deze voor afkadering Desk research Benaderen experts	Duidelijke focus en afkadering onderzoek	Oktober 2022
Onderzoek	Individuele (online) gesprekken met 10 experts	Kennis, meningen en ideeën experts ophalen	Oktober-November

Analyse en opmaak conceptrapport	Analyseren en verwerken resultaten interviews en deskresearch	Beeld van de huidige stand van zaken	November 2022
Toetsing en validatie	Delen conceptrapport met experts voor feedback Organiseren expert bijeenkomst voor discussie inzichten, aanbevelingen en vragen	Verdieping op de resultaten, aanvullende inzichten en validatie door experts	November-December 2022
Definitief eindrapport	Verwerken feedback experts en inzichten expert bijeenkomst	Gevalideerde verkenning naar benodigde standaarden	December 2022-Maart 2023

Betrokken experts

Onderstaande experts zijn geraadpleegd voor deze verkenning. In de selectiecriteria is rekening gehouden met een representatie van experts vanuit diverse (overheids)organisaties en aanverwante organisaties die betrokken zijn bij het thema Regie op Gegevens. Het betreft de volgende experts:

-

§ 1.5 Leeswijzer

§ 1.6 Wat is Cloud?

Hiermee geven de afbakening van het onderzoek en een algemene beschrijving van Cloud-technologie en -ontwikkelingen. De uitwerking bevat: wat verstaan we onder Cloud en wat niet? Welke globale ontwikkelingen zijn er en welke problemen worden hiermee opgelost? Deze afbakening en beschrijving dient als kader voor het verdere onderzoek.

Het moderne bestuurlijke landschap van Nederland heeft, net als de rest van de wereld, een technologische transformatie ondergaan, en cloud computing heeft hierbij een cruciale rol gespeeld. Als centrum van beleidsvorming, regelgeving en dienstverlening aan burgers, heeft de

Nederlandse overheid baat gehad bij de vele voordelen van de cloud. Laten we deze ontwikkeling nader bekijken.

Cloud computing stelt gebruikers in staat om gegevens op te slaan, op te vragen en applicaties uit te voeren via het internet in plaats van op lokale servers of computers. Voor de overheid betekent dit een verhoogde capaciteit en flexibiliteit bij het leveren van diensten, zonder de noodzaak van enorme fysieke IT-infrastructuren.

§ 1.6.1 Cloudvarianten: IaaS, PaaS en SaaS

Wanneer we het hebben over cloudoplossingen, zijn er drie vooraanstaande servicemodellen die de ruggengraat vormen van wat de cloud te bieden heeft, met name voor organisaties zoals de Nederlandse overheid. Dit zijn Infrastructure as a Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS).

1. **Infrastructure as a Service (IaaS)**: IaaS biedt gebruikers toegang tot essentiële infrastructuur zoals fysieke machines, virtual machines, netwerk, opslag en andere fundamenten zonder dat ze de daadwerkelijke hardware hoeven te bezitten of te onderhouden. Voor de Nederlandse overheid kan dit betekenen dat er minder behoefte is aan grote datacenters of serverfarms, omdat deze resources op aanvraag vanuit de cloud kunnen worden verkregen.

2. **Platform as a Service (PaaS)**: PaaS gaat een stap verder door naast de basisinfrastructuur ook een platform te bieden waarop applicaties kunnen worden ontwikkeld, uitgevoerd en beheerd. Denk hierbij aan besturingssystemen, databases, webservers en ontwikkeltools. Voor overheidsinstellingen die unieke applicaties willen bouwen voor hun diensten, kan PaaS een waardevol hulpmiddel zijn door het ontwikkelproces te stroomlijnen zonder zich zorgen te maken over het onderliggende systeembeheer.

3. **Software as a Service (SaaS)**: Dit is wellicht het bekendste model, waarbij gebruikers toegang hebben tot softwaretoepassingen via het web. Denk bijvoorbeeld aan e-maildiensten, CRM-systemen of samenwerkingstools. Voor de Nederlandse overheid betekent dit dat verschillende departementen en agentschappen toegang kunnen hebben tot de nieuwste software zonder zich zorgen te hoeven maken over installaties, updates of compatibiliteitsproblemen.

Voor de overheid kunnen deze modellen helpen om diensten efficiënter te leveren, te reageren op veranderende technologische behoeften en tegelijkertijd de overheadkosten te verlagen. Door de juiste mix van IaaS, PaaS en SaaS te kiezen, kan de Nederlandse overheid een technologische infrastructuur creëren die zowel flexibel als robuust is.

Cloud computing heeft het potentieel om de manier waarop de Nederlandse overheid opereert en interageert met haar burgers te transformeren. Door de kansen te benutten en tegelijkertijd de

uitdagingen te herkennen en aan te pakken, kan de overheid een duurzamere, efficiëntere en meer responsieve toekomst voor Nederland creëren

‘Cloud’ is een containerbegrip en dat vraagt om een nadere precisering. Hieronder een aanzet.

IAAS, PAAS, SAAS

Deze veelgebruikte indeling brengt verschillende soorten afwegingen met zich mee, zoals:

- Infra as a service: Er wordt alleen gebruik gemaakt van servers, netwerken, opslagcapaciteit en andere infrastructuur van de cloudprovider, waarop ‘eigen’ basisvoorzieningen (platformen) en applicaties draaien.
- Platform as a service: De PaaS-laag biedt de cloudprovider een aantal diensten boven op de infrastructuur die het mogelijk maken hun toepassingen op een gestructureerde en geïntegreerde wijze aan te bieden. Voorbeelden van diensten in deze laag zijn toegangsbeheer, identiteitenbeheer, portaalfunctionaliteiten en integratiefaciliteiten. De afnemers van PAAS kunnen hierop hun eigen applicaties draaien.
- Software as a service: De cloudprovider biedt eindapplicaties aan. Deze applicaties kunnen van allerlei soort zijn, bijvoorbeeld kantoorapplicaties (bijv. Microsoft365), cliëntenbeheer (CRM, bijv. Salesforce), softwareontwikkeling (bijv. GITHub), enz., enz.

§ 1.6.2 Cloudleveranciers

de Nederlandse markt voor cloud computing is in veel opzichten een weerspiegeling van de bredere Europese en mondiale trends, maar heeft ook zijn eigen unieke kenmerken. Hier is een overzicht van de cloudleveranciers in Nederland:

Belangrijkste wereldwijde cloudleveranciers actief in Nederland:

1. **Amazon Web Services (AWS)**: AWS heeft een actieve aanwezigheid in Nederland en biedt diensten aan vanuit datacenters in de regio Europa (Frankfurt, Ierland, Londen, Parijs, Stockholm, en sinds 2020 ook een aangekondigde regio in Spanje). Veel Nederlandse bedrijven en startups gebruiken AWS vanwege de brede reeks diensten en schaalbaarheid.
2. **Microsoft Azure**: Gezien de diepgewortelde relatie van veel Nederlandse bedrijven met Microsoft-producten, is Azure een populaire keuze. Microsoft heeft ook een datacenterregio in Nederland, wat helpt bij compliance- en datalocatievereisten.
3. **Google Cloud Platform (GCP)**: Google heeft in 2020 zijn datacenteruitbreiding in Eemshaven voltooid, waarmee het zijn capaciteit in Nederland versterkte. Dit heeft het voor lokale bedrijven aantrekkelijker gemaakt om GCP te gebruiken.

4. **IBM Cloud**: Met een sterke aanwezigheid in de zakelijke markt biedt IBM Cloud diensten aan die populair zijn bij grotere Nederlandse organisaties, vooral die welke al in een IBM-ecosysteem zitten.

5. **Oracle Cloud**: Oracle heeft relaties met veel grote Nederlandse bedrijven, vooral op het gebied van database- en bedrijfssoftware. Hun cloudaanbod wordt vaak overwogen door bedrijven die al gebruik maken van Oracle-producten.

Lokale en regionale spelers:

1. **KPN Cloud**: Als een van de grootste telecomproviders in Nederland biedt KPN ook cloudservices aan, vooral gericht op de lokale markt.

2. **TransIP**: Een Nederlandse webhosting- en cloudserviceprovider, populair bij kleinere bedrijven en individuele gebruikers.

3. **LeaseWeb**: Met hoofdkantoor in Amsterdam, biedt LeaseWeb een scala aan cloudhostingdiensten en heeft het een aanzienlijke aanwezigheid in Nederland.

4. **Interxion**: Een grote Europese aanbieder van colocatie datacenterdiensten, met meerdere datacenters in Nederland.

§ 1.6.3 Nederlandse Overheid

De Nederlandse overheid heeft de afgelopen jaren flink geïnvesteerd in het moderniseren van haar IT-infrastructuur. Cloud-oplossingen zijn hierbij naar voren gekomen als een strategisch middel om efficiëntie te verhogen, kosten te besparen en diensten te verbeteren. Verschillende overheidsinstanties hebben projecten en initiatieven geïmplementeerd om de overgang naar de cloud te faciliteren.

§ *1.6.3.1 Waarom Cloud?*

1. **Efficiëntie en Flexibiliteit**: Met de veranderende eisen van de moderne samenleving kan de overheid haar dienstverlening snel aanpassen door de flexibele capaciteit van de cloud.

2. **Kostenbesparing**: De cloud vermindert de noodzaak voor de overheid om te investeren in fysieke infrastructuur, wat resulteert in aanzienlijke besparingen.

3. **Toegankelijkheid en Transparantie**: Door gegevens in de cloud op te slaan, kan de overheid zorgen voor een bredere en gemakkelijkere toegang voor haar burgers, wat bijdraagt aan transparantie en openheid.

4. **Beveiliging en Compliance**: Gerenommeerde cloud-aanbieders bieden geavanceerde beveiligingsfuncties en kunnen helpen om te voldoen aan strenge regelgevingsnormen.

Publiek, gemeenschappelijk, privaat

Voor de toegankelijkheid van cloud bestaan drie varianten:

- Publiek: De software en data staan dan volledig op de servers van de cloudprovider en er wordt een generieke (voor alle afnemers gelijke) functionaliteit geleverd.
- Gemeenschappelijk: De cloudvoorziening is toegankelijk voor een beperkte groep afnemers, die elkaar onderling voldoende vertrouwen.
- Privaat: Er wordt gewerkt op een (virtueel) private ICT-infrastructuur. In deze cloud heeft de gebruiker volledige controle over data, beveiliging en kwaliteit van de dienst. De applicaties die via de Private Cloud beschikbaar worden gemaakt, maken gebruik van gedeelde infrastructuurcomponenten die slechts voor één organisatie worden ingezet.

Intern, extern

Cloud is ook te beschouwen als een technologie, welke zowel in een eigen rekencentrum kan worden gehuisvest (on premise) of bij een externe serviceprovider (cloudprovider). Een aantal overheidsorganisaties beschikt over interne cloudtechnologie.

Gemeenten willen de veranderkracht van digitalisering benutten en tegelijkertijd een antwoord vinden op de risico’s en uitdagingen die dit met zich meebrengt. Met als doel: op weg naar een veilige, mensgerichte, transparante, effectieve digitale toekomst.

De gemeente kan daarbij de volgende doelstellingen hanteren:

Bij het formuleren van het cloudbeleid zijn er een aantal keuzes te maken die bepalend zijn voor de uitgangspunten van het beleid. Hieronder volgt een voorbeeld van deze keuzes, iedere gemeente maakt uiteraard zelf haar keuzes in haar cloudbeleid:

- We kiezen bewust voor een Cloud First strategie. Cloud heeft zichzelf bewezen, bedrijfsvoering en dienstverlening profiteren ervan.
- Voorkeursmodel:
    - Public Cloud is het voorkeursmodel bij alle vernieuwingsvraagstukken, al dan niet bewust bij één cloudleverancier.
    - OF het voorkeursmodel is een combinatie van een on-premises omgeving en een private en public cloud. Oftewel een combinatie van verschillende leveranciers.
- Gebruik volwassen technologie waar het kan, vernieuwende technologie waar het moet

- Commodity functionaliteit wordt als SaaS-dienst afgenomen, PaaS en IaaS worden gebruikt voor maatwerk oplossingen
- Clouddiensten worden centraal ingekocht en beheerd door het i-domein en kunnen naar decentrale behoeften worden aangepast

§ *1.6.3.2 Uitdagingen en Overwegingen*

Hoewel de voordelen evident zijn, brengt de migratie naar de cloud ook uitdagingen met zich mee. Vragen over dataprivacy, beveiliging en de integratie met bestaande systemen zijn zaken die zorgvuldig moeten worden aangepakt. De Nederlandse overheid moet ook zorgen voor de naleving van zowel nationale als Europese regelgeving met betrekking tot gegevensbescherming.

§ *1.6.3.3 Privacy en beveiliging*

De volgende zaken spelen er op het gebied van privacy en beveiliging:

1. **Data Locatie**: Waar worden de gegevens fysiek opgeslagen? In welk land bevinden de datacenters zich? De locatie kan invloed hebben op de regelgeving die van toepassing is op de gegevens. Bijvoorbeeld, gegevens opgeslagen binnen de EU zijn onderhevig aan de GDPR, wat strenge eisen stelt aan gegevensbescherming.
2. **Data Overdracht**: Hoe worden gegevens tussen locaties en tussen de cloud en eindgebruikers overgedragen? Tijdens deze overdracht kunnen gegevens kwetsbaar zijn voor onderschepping, vooral als de overdracht niet adequaat wordt gecodeerd.
3. **Toegangscontrole**: Wie heeft er toegang tot de gegevens? Zowel vanuit de kant van de cloud service provider als vanuit de kant van de gebruiker moet duidelijk zijn wie welke gegevens mag inzien, wijzigen of verwijderen.
4. **Multi-Tenancy Risico's**: Cloud providers gebruiken vaak multi-tenancy modellen waarbij de gegevens van meerdere klanten op dezelfde servers kunnen worden opgeslagen. Dit kan leiden tot zorgen over datalekken tussen 'tenants'.
5. **Wettelijke en Regelgevende Uitdagingen**: Verschillende landen en regio's hebben verschillende wetten met betrekking tot gegevensbescherming en privacy. Cloud providers moeten deze wetten navigeren, wat ingewikkeld kan zijn als ze in meerdere rechtsgebieden opereren.

6. **Afhankelijkheid van de Service Provider**: Als een cloud provider failliet gaat of zijn diensten wijzigt, wat gebeurt er dan met de gegevens van de klant? Hoe kunnen organisaties hun gegevens terughalen of overzetten naar een andere provider?

7. **Eindpuntbeveiliging**: Aangezien cloud diensten vaak toegankelijk zijn vanaf diverse apparaten en locaties, wordt het beveiligen van elk eindpunt waarvan toegang wordt verkregen tot de cloud cruciaal.

8. **Incidentrespons en Melding**: In het geval van een beveiligingsincident, hoe snel en effectief zal de cloud provider reageren? Hoe en wanneer worden klanten op de hoogte gesteld?

9. **Back-ups en Gegevensverlies**: Hoewel de cloud vaak wordt gezien als een veiligere opslagplaats, kunnen er nog steeds zorgen zijn over hoe gegevens worden geback-upt en wat er gebeurt in het geval van gegevensverlies of corruptie.

10. **Compliance en Audits**: Hoe kunnen organisaties verifiëren dat hun cloud provider voldoet aan de benodigde normen en regelgeving, vooral als deze normen veranderen of evolueren?

Deze vraagstukken vereisen een zorgvuldige overweging bij de overgang naar of uitbreiding van het gebruik van cloud-diensten. Organisaties, waaronder overheidsentiteiten, moeten samenwerken met cloud providers en juridische en beveiligingsexperts om te zorgen voor een veilige en conforme cloud-omgeving

§ 1.7 Onderzoek

§ **1.7.1 Cloudontwikkelingen**

§ *1.7.1.1 Mondiale Trends*

Cloud computing heeft de manier waarop bedrijven, overheden en individuen technologie gebruiken en benaderen getransformeerd. Dit dynamische veld blijft evolueren met nieuwe innovaties, gebruikspatronen en businessmodellen. Hier is een overzicht van de belangrijkste mondiale trends in cloud computing:

1. **Hybride en Multi-Cloud Strategieën**: Bedrijven en organisaties gaan steeds meer voor een hybride cloudbenadering, waarbij ze zowel private als public cloud resources combineren. Bovendien adopteren ze multi-cloud strategieën, waarbij ze gebruikmaken van diensten van meerdere cloudproviders, om flexibiliteit te vergroten en risico's te verminderen.

2. **Serverloze Architecturen**: Serverloos computing, vaak aangeduid als 'Function as a Service' (FaaS), stelt ontwikkelaars in staat om applicaties te bouwen en uit te voeren zonder zich zorgen te maken over de onderliggende infrastructuur. Dit leidt tot snellere ontwikkeling en kan kosten verminderen.

3. **Edge Computing**: Met de opkomst van IoT (Internet of Things) devices is er een groeiende behoefte om gegevensverwerking dichter bij de bron van gegevensgeneratie te brengen. Edge computing stelt organisaties in staat om gegevens te verwerken aan de "rand" van het netwerk, vaak op het apparaat zelf of in lokale servers, in plaats van in een gecentraliseerd datacenter.

4. **AI en Machine Learning Integratie**: Cloudproviders breiden hun diensten uit met tools en platforms die AI en machine learning integreren. Dit stelt organisaties in staat om krachtige data-analyses uit te voeren en intelligentie toe te voegen aan hun applicaties zonder grote voorafgaande investeringen.

5. **Verbeterde Beveiligingsmaatregelen**: Met de toenemende zorgen over cyberbeveiliging investeren cloudproviders in geavanceerde beveiligingstechnologieën, zoals AI-gedreven beveiligingsanalyses, encryptie en zero-trust beveiligingsmodellen.

6. **Containers en Orkestratie**: Containers, zoals Docker, en orkestratietools, zoals Kubernetes, zijn in populariteit gestegen, omdat ze ontwikkelaars helpen om applicaties te bouwen die gemakkelijk kunnen worden geschaald en over verschillende cloudomgevingen kunnen worden verplaatst.

7. **Duurzaamheid**: Met de groeiende zorgen over klimaatverandering kijken bedrijven en consumenten steeds meer naar de milieueffecten van technologie. Cloudproviders reageren hierop door duurzamere datacenters te bouwen en groene energie te gebruiken.

8. **Verticale Cloudoplossingen**: Cloudproviders bieden steeds vaker branchespecifieke cloudoplossingen aan, die zijn afgestemd op de unieke behoeften van sectoren zoals gezondheidszorg, financiën en productie.

9. **Data-soevereiniteit en Lokale Regulaties**: Met strengere gegevensbeschermingswetten in verschillende landen en regio's zijn cloudproviders begonnen met het bouwen van regionale datacenters en het aanbieden van specifieke oplossingen om aan lokale regelgeving te voldoen.

10. **Uitbreiding van Cloud naar Traditionele Sectoren**: Sectoren die traditioneel terughoudend waren in het adopteren van de cloud, zoals overheid, financiële dienstverlening en gezondheidszorg, zijn nu actief op zoek naar cloudoplossingen vanwege de bewezen voordelen op het gebied van schaalbaarheid, flexibiliteit en kosten.

De mondiale trends in cloud computing zijn een reflectie van de snel veranderende technologische landschap en de behoeften van organisaties en individuen. Terwijl cloud computing blijft evolueren, zullen de fundamentele principes van flexibiliteit, schaalbaarheid en on-demand toegang

de drijvende krachten achter deze transformatie blijven. Het is cruciaal voor organisaties om deze trends te begrijpen en te benutten om concurrentievoordeel te behalen en te voldoen aan de veranderende verwachtingen van klanten en stakeholders.

§ *1.7.1.2 Europese Cloudontwikkelingen*

In een tijdperk waarin gegevens de nieuwe olie zijn en technologie centraal staat in beleidsvorming, regelgeving en dienstverlening, is het cruciaal voor de Nederlandse overheid om op de hoogte te blijven van belangrijke Europese cloudontwikkelingen. Deze ontwikkelingen zijn van invloed op de manier waarop gegevens worden opgeslagen, verwerkt en gedeeld op Europees niveau. Hier zijn enkele van de belangrijkste ontwikkelingen en hun implicaties:

1. **Europese Datastrategie**: In 2020 heeft de Europese Commissie een datastrategie gelanceerd die beoogt een gemeenschappelijke Europese data-ruimte te creëren. Deze strategie heeft directe implicaties voor cloud computing, aangezien het beoogt sectorspecifieke, gedeelde Europese datasystemen te ontwikkelen. Voor Nederland betekent dit dat overheidssystemen compatibel en in lijn moeten zijn met deze Europese initiatieven.

2. **GAIA-X**: Dit initiatief, voornamelijk aangestuurd door Duitsland en Frankrijk, streeft naar de oprichting van een concurrerend, veilig en betrouwbaar cloudaanbod voor Europa. GAIA-X heeft als doel Europese waarden en regelgeving rondom data te waarborgen. De Nederlandse overheid moet de ontwikkelingen rondom GAIA-X nauwlettend volgen, gezien de potentiële implicaties voor interoperabiliteit en data-soevereiniteit.

3. **Digitale Soevereiniteit**: De EU heeft de ambitie uitgesproken om de digitale soevereiniteit van haar lidstaten te vergroten. Dit heeft betrekking op de capaciteit van Europa om onafhankelijke digitale oplossingen te ontwikkelen, waaronder cloud infrastructuren. Dit kan gevolgen hebben voor waar en hoe overheidsgegevens worden opgeslagen.

4. **Versterking van de GDPR**: De Algemene Verordening Gegevensbescherming (AVG of GDPR in het Engels) blijft zich ontwikkelen met aanvullende richtlijnen en interpretaties. Het is cruciaal voor de Nederlandse overheid om zich aan te passen aan deze evoluerende normen, vooral in de context van cloud-diensten.

5. **EU Cloud Code of Conduct**: Deze gedragscode, goedgekeurd door de Europese Autoriteit voor gegevensbescherming, biedt richtlijnen voor cloud service providers over hoe zij de GDPR in hun diensten kunnen integreren. Het zorgt voor een uniforme interpretatie van de GDPR binnen de cloud-sector, wat relevant is voor de Nederlandse overheid bij het selecteren van cloud partners.

6. **Europese Cybersecurity Act**: Ingesteld in 2019, deze wet introduceert een EU-breed kader voor cybersecurity-certificering. Als de Nederlandse overheid gebruik maakt van cloud-

diensten, is het belangrijk te waarborgen dat deze diensten voldoen aan de Europese cybersecurity-normen.

In de dynamische wereld van cloud computing is het essentieel voor de Nederlandse overheid om op de hoogte te blijven van de ontwikkelingen op Europees niveau. Deze veranderingen bieden zowel uitdagingen als kansen. Door proactief te zijn en een weloverwogen benadering van cloud-adoptie te handhaven, kan Nederland zorgen voor een veilige, efficiënte en conform de regelgeving cloud-omgeving voor zijn burgers en instellingen

§ *1.7.1.3 Cloudontwikkelingen Nederlandse Overheid*

De cloudtransitie heeft zich wereldwijd volop ingezet en de Nederlandse overheid is daarop geen uitzondering. Als reactie op de wereldwijde technologische ontwikkelingen en in lijn met haar eigen ambitie om moderner, efficiënter en dienstbaarder te zijn voor haar burgers, heeft de Nederlandse overheid verschillende cloudinitiatieven ontplooid. Hier volgt een blik op de belangrijkste cloudontwikkelingen binnen de Nederlandse overheid:

1. **Digitale Overheid en Cloud Eerst-Beleid**: Onder het streven naar een meer digitale overheid is er een 'cloud eerst'-beleid ontstaan. Dit betekent dat bij de overweging van nieuwe IT-projecten de voorkeur uitgaat naar cloudoplossingen, tenzij er overtuigende redenen zijn om dit niet te doen.

2. **DigiD in de Cloud**: Als een centrale dienst voor identiteitsverificatie heeft DigiD onderzocht hoe cloudtechnologieën de service betrouwbaarder en schaalbaarder kunnen maken, met name gezien het groeiend aantal gebruikers en diensten die DigiD vereisen.

3. **Focus op Open Standaarden**: Er is een groeiende nadruk gelegd op het gebruik van open standaarden bij cloud-implementaties. Dit zorgt voor interoperabiliteit tussen verschillende overheidsdiensten en vermindert het risico van 'vendor lock-in', waarbij de overheid te afhankelijk wordt van één leverancier.

4. **Cloudbeveiligingsbeleid**: In lijn met de wereldwijde zorgen over cyberbeveiliging heeft de Nederlandse overheid specifieke richtlijnen en best practices ontwikkeld voor het beveiligen van cloudservices. Dit omvat zaken zoals encryptie, toegangscontroles en regelmatige beveiligingsaudits.

5. **Dataopslag binnen Nederland**: Gezien de gevoeligheid van overheidsgegevens en de wettelijke beperkingen rondom gegevensopslag, geven sommige overheidsinstanties de voorkeur aan cloudoplossingen waarbij de gegevensopslag binnen Nederlandse grenzen blijft.

6. **Integratie van AI en Cloud**: Met de opkomst van kunstmatige intelligentie (AI) heeft de overheid onderzoek gedaan naar hoe cloud-infrastructuren kunnen worden geoptimaliseerd

voor AI-toepassingen, zoals voorspellende analyses en automatisering.

7. **Scholing en Training**: Erkenning van het feit dat cloudtechnologieën andere vaardigheden vereisen, heeft geleid tot initiatieven om overheidsmedewerkers op te leiden en te trainen in cloudcompetenties.

8. **Samenwerking met de Private Sector**: De overheid werkt steeds nauwer samen met de private sector, zowel om expertise te verkrijgen als om gezamenlijke cloud-oplossingen te ontwikkelen die kunnen worden gebruikt door zowel publieke als private entiteiten.

De cloudontwikkelingen binnen de Nederlandse overheid zijn een weerspiegeling van zowel de mondiale technologische trends als de unieke behoeften en uitdagingen van Nederland als natie. Door voorop te lopen in deze transitie en tegelijkertijd rekening te houden met beveiliging, privacy en interoperabiliteit, streeft de Nederlandse overheid ernaar een modern en effectief technologisch landschap te creëren voor haar burgers en instellingen

§ 1.7.2 Cloudtechnologie

Hier zijn de belangrijkste cloudtechnologieën waar de Nederlandse overheid rekening mee moet houden:

1. **Hybride Cloud Infrastructuren**: Deze stellen de overheid in staat om gegevens en applicaties te verdelen over private en public clouds, waardoor er flexibiliteit ontstaat in gegevensbeheer en -toegang, terwijl de veiligheid en compliance worden gewaarborgd.

2. **Serverloze Computing**: Hiermee kan de overheid applicaties uitvoeren zonder zich bezig te houden met de onderliggende infrastructuur. Dit kan leiden tot kostenbesparingen en een snellere time-to-market voor overheidsapplicaties.

3. **Containers en Orkestratiesystemen**: Met technologieën zoals Docker en Kubernetes kan de overheid applicaties bouwen die zowel schaalbaar als draagbaar zijn, waardoor ze gemakkelijk kunnen worden overgebracht tussen verschillende cloudomgevingen.

4. **Edge Computing**: Vooral relevant voor smart city-initiatieven en IoT-projecten van de overheid. Het verwerken van data dichtbij de bron zorgt voor snellere reactietijden en vermindert de belasting op centrale systemen.

5. **AI en Machine Learning Services**: Cloud-gebaseerde AI-diensten kunnen de overheid helpen bij het analyseren van grote datasets, het voorspellen van trends en het bieden van gepersonaliseerde diensten aan burgers.

6. **Cloud-gebaseerde Analysetools**: Deze kunnen de overheid helpen bij het beter begrijpen van grote hoeveelheden data, van verkeerspatronen tot sociale dienstverlening, wat leidt tot beter geïnformeerde besluitvorming.

7. **Blockchain in de Cloud**: Voor bepaalde toepassingen, zoals transparante overheidsuitgaven of beveiligde digitale identiteiten, kan blockchain-technologie in de cloud van belang zijn.
8. **Data Lakes en Opslagoplossingen**: Gezien de enorme hoeveelheid data die door overheidsdiensten wordt gegenereerd, zijn schaalbare en flexibele opslagoplossingen essentieel.
9. **Unified Communications**: Cloud-gebaseerde communicatiesystemen kunnen de samenwerking tussen overheidsafdelingen verbeteren en een efficiënte externe communicatie mogelijk maken.
10. **Cloud Security en Identity Access Management (IAM) Systemen**: Naarmate meer diensten naar de cloud verhuizen, wordt de beveiliging ervan van cruciaal belang. IAM-systemen zorgen ervoor dat alleen geautoriseerde gebruikers toegang hebben tot bepaalde bronnen.

Het is van essentieel belang voor de Nederlandse overheid om proactief te zijn in het begrijpen en integreren van deze cloudtechnologieën. De juiste implementatie kan leiden tot verbeterde dienstverlening, operationele efficiëntie en kostenbesparingen. Tegelijkertijd moeten potentiële risico's, zoals beveiligingszorgen en gegevensbescherming, zorgvuldig worden aangepakt om het vertrouwen van het publiek te behouden

§ 1.7.3 Cloudstandaarden en -normen

bestaande standaarden, standaarden in ontwikkeling en ontbrekende standaarden, in relatie tot cloud-interoperabiliteit, dataportabiliteit, informatieveiligheid en processen.

laten we eerst het verschil tussen "standaarden" en "normen" definiëren:

- **Standaarden**: Deze zijn technische specificaties of andere nauwkeurige criteria die worden gebruikt als regels of richtlijnen om consistentie en interoperabiliteit te waarborgen. Ze kunnen worden opgesteld door officiële normeringsorganisaties, door brancheorganisaties, of kunnen zelfs de facto standaarden worden door wijdverbreid gebruik.
- **Normen**: In de context van technologie en IT, zijn normen vaak officiële documenten die best practices, methodologieën, processen of specificaties bevatten die algemeen worden geaccepteerd. Normen worden meestal uitgegeven door officiële normeringsorganisaties.

§ *1.7.3.1 Cloudstandaarden*

1. **Open Virtualization Format (OVF)**: Een open standaard voor het verpakken en distribueren van gevirtualiseerde applicaties.
2. **OAuth**: Een open standaard voor toegangsdelegatie, die veel wordt gebruikt voor token-gebaseerde authenticatie en autorisatie op het internet.
3. **OpenID Connect**: Een simpele identiteitslaag bovenop het OAuth 2.0-protocol, die gebruikersauthenticatie mogelijk maakt.
4. **Cloud Data Management Interface (CDMI)**: Een set van protocollen die zijn gedefinieerd voor het beheer van cloud storage.

§ *1.7.3.2 Cloudnormen*

1. **ISO/IEC 27001**: Een wereldwijd erkende norm voor het beheren van risico's op het gebied van informatiebeveiliging.
2. **ISO/IEC 27017**: Een cloud-specifieke norm die extra beveiligingscontroles bevat bovenop ISO/IEC 27001 specifiek voor cloudservices.
3. **ISO/IEC 27018**: Een code voor de bescherming van persoonlijke gegevens in de cloud, op basis van ISO/IEC 27001.
4. **NIST SP 500-292**: Het NIST Cloud Computing Reference Architecture is een generiek high-level conceptueel model dat dient als een gebruikersgericht referentiepunt.
5. **ENISA Cloud Computing Risk Assessment**: Een norm van het European Network and Information Security Agency (ENISA) dat zich richt op risicobeoordeling in de cloudomgeving.
6. **Cloud Security Alliance (CSA) Best Practices**: Hoewel niet een "norm" in de traditionele zin, biedt CSA richtlijnen en best practices voor cloudbeveiliging die algemeen worden geaccepteerd in de industrie.
7. **GAIA-X**: Een initiatief in Europa, gericht op het creëren van een uniform framework voor cloud services, dat bepaalde principes en beleidsregels vaststelt die functioneren als normen.

Hoewel standaarden en normen vaak door elkaar worden gebruikt, is het onderscheid tussen de twee vooral dat standaarden doorgaans technischer van aard zijn, terwijl normen eerder de algemeen geaccepteerde practices en procedures beschrijven. In de cloudomgeving is het cruciaal voor organisaties om zowel de relevante standaarden als normen te kennen om te zorgen voor interoperabiliteit, beveiliging en compliance.

1.7.4 Witte vlekken

1.8 Conclusies en aanbevelingen

2. Conformiteit

Naast onderdelen die als niet normatief gemarkeerd zijn, zijn ook alle diagrammen, voorbeelden, en noten in dit document niet normatief. Verder is alles in dit document normatief.

A. Index

A.1 Begrippen gedefinieerd door deze specificatie

A.2 Begrippen gedefinieerd door verwijzing

↥