E-Space Adviesdocument - Werkversie

Onderzoek naar standaarden en standaardisatieactiviteiten voor Cloud

E-Space Adviesdocument
Werkversie 05 februari 2024

Deze versie:

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

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

Dit document is geenszins af en rijp voor publicatie!!!! Het is onder bewerking en kan nog geheel en gedeeltelijk wijzigen. Aan de inhoud kan op geen enkele manier enig recht worden ontleend

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

Samenvatting

Status van dit document

1. Inleiding

1.1 De aanleiding van het onderzoek

1.2 De onderzoeksvragen

1.3 Uitvoering van het onderzoek

1.4 Leeswijzer

2. Conclusies van het onderzoek

3. Adviezen aan de overheid

3.1 Pak meer regie en zet in op open standaarden

3.2 Bouw kennis en capaciteit op overheidsniveau

3.3 Maak bindende keuzen in normenkaders voor informatieveiligheid en privacy, en sluit daarbij aan op Europese en internationale ontwikkelingen

3.4 Verplicht de standaard Haven

3.5 Verplicht aanbevolen standaarden die dataportabiliteit ondersteunen en zet druk op leveranciers om ze te implementeren

3.6 Laat op de lijst van het Forum Standaardisatie standaarden toe voor leveranciersonafhankelijkheid en digitale soevereiniteit, ook als ze niet toepasbaar zijn op gegevensuitwisseling tussen organisaties

3.7 Identificeer open standaarden voor dataportabiliteit die verplicht moeten worden en meld deze aan bij het Forum Standaardisatie

3.8 Verplicht standaarden die cloud interoperabiliteit ondersteunen en zet druk op leveranciers om ze te implementeren

3.9 Leg best practices vast

4. Standaarden voor de cloud

4.1 Soorten cloudstandaarden

4.2 Beveiligings- en privacystandaarden

4.2.1 Standaarden op de lijst van Open standaarden

4.2.2 Normen en (auditing) frameworks niet op de lijst van Open standaarden

4.2.3 Witte vlekken

4.3 Portabiliteitstandaarden

4.3.1 Standaarden voor systeem- en applicatieportabiliteit niet op de lijst van Open standaarden

4.3.2 Witte vlekken

4.3.3 Standaarden voor dataportabiliteit niet op de lijst van open standaarden

4.3.4 Witte vlekken

4.4 Interoperabiliteitsstandaarden
4.4.1 Standaarden op de lijst van Open standaarden
4.4.2 Standaarden niet op de lijst van Open standaarden
4.4.3 Witte vlekken
4.5 Overige standaarden
4.5.1 Witte vlekken

5. Bijlage 1: Gebruikte bronnen bij het onderzoek

6. Bijlage 2: De betrokken experts

7. Bijlage 3: Aanpak en planning onderzoek

8. Bijlage 4: Wat is cloud?
8.1 Clouddiensten
8.2 Varianten van clouddiensten
8.3 Implementatievarianten van clouddiensten
8.4 Waarom Cloud?
8.5 Cloudleveranciers

9. Bijlage 5: Scope en uitgangspunten
9.1 Hoofdpunten Rijksbreed Cloudbeleid 2022
9.2 Doelstellingen en uitgangspunten van het Forum voor het onderzoek

10. Bijlage 6: Cloudontwikkelingen en trends
10.1 Mondiale trends
10.2 Europese ontwikkelingen
10.3 Cloudontwikkelingen binnen de Nederlandse Overheid

11. Bijlage 7: Risico’s van de toepassing van cloud en clouddiensten

12. Conformiteit

A. Index
A.1 Begrippen gedefinieerd door deze specificatie
A.2 Begrippen gedefinieerd door verwijzing

1. Inleiding

1.1 De aanleiding van het onderzoek

Het Forum Standaardisatie adviseert de overheid over de al dan niet verplichte toepassing van de Open ICT standaarden in de publieke sector. Om de overheid te kunnen adviseren over standaardisatie in relatie tot de cloud, wil het Forum Standaardisatie een beeld krijgen van de standaarden die van belang zijn voor het beleid van de overheid voor het gebruik van cloudiensten. Hiervoor heeft Bureau Forum Standaardisatie een onderzoek laten doen door het onafhankelijk adviesbureau E-Space.

Een belangrijk uitgangspunt voor het onderzoek is de brief van de Staatssecretaris van Huffelen van 29 augustus 2022, waarin zij een wijziging aankondigt in het beleid van de Rijksoverheid voor het gebruik van clouddiensten. Het nieuwe beleid stelt kaders voor het gebruik van commerciële public clouddiensten door de Rijksoverheid en actualiseert het voormalige beleid uit 2011, dat zich vooral richtte op het in eigen beheer houden van clouddiensten.

Het overheidsbeleid voor clouddiensten brengt vragen met zich mee over digitale soevereiniteit, leveranciersonafhankelijkheid en informatiebeveiliging. Open standaarden voor dataportabiliteit, cloud interoperabiliteit en informatiebeveiliging kunnen deze waarden helpen ondersteunen. Het onderzoek had daarom als hoofddoel om een overzicht te geven van Europese, internationale en nationale standaarden en standaardisatieactiviteiten die relevant zijn voor cloud platformen, systemen en diensten. Ook werden trends en risico’s in beeld gebracht.

1.2 De onderzoeksvragen

Forum Standaardisatie formuleerde de volgende onderzoeksvragen voor dit onderzoek:

1. Welke Europese, internationale en nationale standaarden bestaan er in relatie tot cloud, in het bijzonder voor cloudinteroperabiliteit, dataportabiliteit, informatiebeveiliging en orchestratie?
2. Welke Europese, internationale en nationale cloudstandaarden zijn nog in ontwikkeling, of gepland?
3. Zijn er witte vlekken? Dat wil zeggen, cloudtechnologieën of - toepassingen waar open standaarden nodig zijn, maar nog niet bestaan en nog niet ontwikkeling zijn?

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

§ 1.3 Uitvoering van het onderzoek

Het onderzoek werd tussen september en december 2023 uitgevoerd. Voor het onderzoek zijn bronnen geanalyseerd (zie bijlage 1) en interviews gehouden met 27 experts van onder andere NEN, TNO, VNG, ICTU, ACM, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Ministerie van Justitie en Veiligheid, NCSC, Cloud Security Alliance, Microsoft en IBM (zie bijlage 2 voor de volledige lijst met geïnterviewde experts).

Ook zijn bijeenkomsten bijgewoond over het onderwerp cloud en standaarden. Dit betrof bijeenkomsten tijdens het iBestuur congres van 13 september 2023, de Haven community dag van 31 oktober 2023 en het ECP Jaarfestival van 16 november 2023.

§ 1.4 Leeswijzer

Dit rapport is zo piramidaal mogelijk opgesteld, waarbij we beginnen met de conclusies (hoofdstuk 2) en adviezen aan de overheid (hoofdstuk 3), gevolgd door de onderbouwing (hoofdstuk 4).

De aanpak, scope en uitgangspunten en de resultaten van de deskresearch zijn in bijlagen opgenomen. In bijlage 3 is een overzicht opgenomen van de uitgevoerde stappen in het onderzoek met de bestede tijdsperiode per stap. Bijlage 4 bevat een uitleg van de cloud en clouddiensten, implementatievarianten van clouddiensten en een opsomming van belangrijke cloudleveranciers wereldwijd, in Europa en in Nederland. In bijlage 5 zijn de uitgebreide scope en uitgangspunten van het onderzoek beschreven, onder andere een samenvatting van het vernieuwde Rijkscloudbeleid van augustus 2022. Bijlage 6 bestaat uit een overzicht van de mondiale trends, Europese ontwikkelingen en initiatieven vanuit de Nederlandse overheid met betrekking tot het cloudbeleid. Tot slot is in bijlage 7 een opsomming opgenomen van mogelijke risico’s van cloud en clouddiensten.

§ 2. Conclusies van het onderzoek

In het onderzoek kwamen de onderzoekers tot de volgende conclusies:

1. Er bestaan nog onvoldoende open dataportabiliteit- en interoperabiliteitstandaarden die algemeen geaccepteerd zijn en breed ondersteund worden. Mede hierdoor wordt de overheid steeds afhankelijker van leveranciers van clouddiensten.

2. Met name voor de portabiliteit van *complexe data* zoals databases bestaan nog geen Europese standaarden. Leveranciers ontwikkelen vooralsnog hun eigen data transfer technologieën. Voor de portabiliteit van minder complexe data op bestandsniveau kunnen wel beproefde open standaarden worden gebruikt zoals IMAP, WebDAV, JSON, XML en CSV. De overheid zou de ondersteuning hiervan voor bestanduitwisseling tussen clouddiensten moeten verplichten.

3. Voor cloud security bestaan er juist veel overlappende standaarden, vooral voor de management-, proces- en certificeringsaspecten. Hierin moet de overheid een duidelijke lijn kiezen en daarbij aansluiten op de Europese en internationale actualiteit.

4. De verweving van commerciële clouddiensten met (proprietary) AI maakt het moeilijker om dataportabiliteit en interoperabiliteit met open standaarden te realiseren. Leveranciers gebruiken AI om afnemers afhankelijker te maken van hun diensten.

5. Leveranciers van clouddiensten willen deels meebewegen als de overheid regie neemt en duidelijkheid geeft over welke open standaarden ondersteund moeten worden. Dit is onder andere te zien bij de Haven standaard die is ontwikkeld vanuit de Vereniging Nederlandse Gemeenten (VNG). Door beleid op Europees niveau af te stemmen zullen de grote hyperscalers meer bereid zijn mee te bewegen.

6. Door de discussie rond digitale soevereiniteit en opkomende regelgeving als de Data Act gaan er nieuwe normen en standaarden ontstaan. Daarom is het belangrijk om standaarden voor clouddiensten actief te blijven monitoren.

Deze conclusies worden nader onderbouwd bij de verdere uitwerking van de servicemodellen in bijlage 4.

> *“I see no gaps in standards for cloud security. There are in fact too many overlapping standards in this domain’.*
>
> *Linda Strick, director Cloud Security Alliance*

§ 3. Adviezen aan de overheid

Het onderzoek heeft een goed beeld gegeven van de uitdagingen met betrekking tot het verder toenemende gebruik van cloudvoorzieningen en clouddiensten. Uit de conclusies van het onderzoek komt een aantal adviezen aan de overheid voort, die hier worden weergegeven.

§ 3.1 Pak meer regie en zet in op open standaarden

Grote leveranciers van clouddiensten zijn deels bereid om mee te werken aan standaarden die interoperabiliteit en dataportabiliteit mogelijk maken. Tegelijkertijd blijft de afhankelijkheid van deze leveranciers groeien. In het marktonderzoek van de ACM van 2022 is deze tendens al duidelijk zichtbaar.

Voor clouddiensten is een '*winner takes all*' aan het ontstaan die ertoe leidt dat het marktaandeel van de grootste hyperscalers alleen maar groeit ten koste van kleinere marktpartijen. De verweving van clouddiensten met proprietary AI versterkt deze ontwikkeling. Kleinere beschikken niet over de kennis en rekenkracht voor grootschalige AI, wat de positie van de grote hyperscalers verder versterkt. De Data Act is een stap in de goede richting om de markt meer in evenwicht te brengen, maar deze moet wel worden geïmplementeerd, onder andere door de ontwikkeling en verplichting van open standaarden. Daarvoor is initiatief en regie nodig.

Advies aan de overheid: pak meer regie op de markt voor clouddiensten, zowel op nationaal als Europees niveau. Leveranciers van clouddiensten willen best meebewegen, maar hebben duidelijkheid nodig over de te implementeren standaarden. Open standaarden op Europees niveau zijn nodig om afhankelijkheid van hyperscalers en andere aanbieders te verkleinen. Deze zijn er nog niet, hier moet de overheid in Europees verband op inzetten. De overheid en de Europese Commissie kunnen daarnaast druk uitoefenen op cloudleveranciers om hun proprietary standaarden openbaar te maken, zodat deze ook door derden te gebruiken zijn.

> *"Cloud is een netwerkmarkt, die zich niet houdt aan de regels van de traditionele markten. Open standaarden zijn nodig om deze markt gezond te houden."*
>
> *Rudi Bekkers, Professor of Standardisation and Intellectual Property at Eindhoven University of Technology, tijdens ECP congres 16 november 2023*

§ 3.2 Bouw kennis en capaciteit op overheidsniveau

Kennis en kunde op het gebied van public clouddiensten is schaars en versnipperd bij de overheid. Dit in tegenstelling tot *on-premise* cloud-omgevingen waar veel meer kennis en ervaring over beschikbaar is. Meerdere ondervraagden geven aan dat er binnen de overheid weinig coördinatie is op alle maatregelen en acties die moeten worden ondernomen om de snelle ontwikkeling op het gebied van clouddiensten bij te houden en in goede banen te leiden. Zonder eigen, gebundelde expertise wordt de overheid ook qua kennis steeds afhankelijker van marktpartijen, en in het bijzonder de grote buitenlandse clouddienstverleners.

Advies aan de overheid: zet in op training, kennisopbouw en kennisbehoud, en op samenwerking tussen overheidsorganisaties. Sluit hiervoor aan bij internationale organisaties als NEN en de Cloud Security Aliance. Overweeg om een overheidsorganisatie hier verantwoordelijk voor te maken, zodat de coördinatie centraal wordt geregeld. Dit zou wellicht de Rijksacademie voor Digitalisering en Informatisering Overheid (RADIO) kunnen zijn. En trek meer experts aan binnen de overheid.

§ 3.3 Maak bindende keuzen in normenkaders voor informatieveiligheid en privacy, en sluit daarbij aan op Europese en internationale ontwikkelingen

Met betrekking tot standaarden en normenkaders voor informatiebeveiliging en privacy is er al veel gaande. Sommige ontwikkelingen overlappen elkaar, en dit kan tot onduidelijkheid leiden. In het onderzoek kwam aan het licht dat de overheid werkt aan *security controls* zonder aan te sluiten bij internationale standaarden of organisaties. Dit terwijl internationale samenwerking juist de positie van de overheid kan versterken.

Advies aan de overheid: doe verdiepend onderzoek naar de samenhang en de overlap tussen nationale, Europese en internationale normenkaders. Kies vervolgens een duidelijke lijn, maak keuzes en sluit daarbij aan bij Europese en internationale organisaties en ontwikkelingen. Zorg dat deze tot verplichte norm verheven worden zodat partijen zich hieraan moeten houden.

§ 3.4 Verplicht de standaard Haven

Met betrekking tot standaarden voor systeem- en applicatieportabiliteit in de cloud heeft Haven (initiatief van de VNG) een goede basis gelegd voor uniform gebruik van Kubernetes. Haven wordt ondersteund door de commerciële hyperscalers en kent al diverse implementaties bij gemeenten. Deze ontwikkeling draagt sterk bij aan interoperabiliteitsverbetering.

Advies aan de overheid: meld de standaard Haven aan voor opname op de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie. Help de ontwikkeling van Haven te versterken door te zorgen voor een bredere toepassing en solide financiering. Versterk Haven door een breder pallet aan functies te laten ondersteunen, die de standaard doorontwikkelen tot een vervanging van proprietary diensten.

§ 3.5 Verplicht aanbevolen standaarden die dataportabiliteit ondersteunen en zet druk op leveranciers om ze te implementeren

Op de lijst aanbevolen standaarden van het Forum Standaardisatie staan standaarden die dataportabiliteit op bestandsniveau ondersteunen en verplicht zouden moeten worden gesteld aan

cloudleveranciers. Het gaat bijvoorbeeld om open standaarden zoals IMAP, waarmee e-mailberichten van een cloudleverancier naar een andere kunnen worden overgezet. En WebDAV, waarmee bestanden met een standaard interface kunnen worden beheerd. Door deze standaarden op de ‘pas toe of leg uit’ lijst te zetten, moeten overheden ze uitvragen in hun aanbesteding van clouddiensten en moeten leveranciers ze dus ook aanbieden.

Advies aan de overheid: meld aanbevolen standaarden die relevant zijn voor dataportabiliteit aan voor opname op de ‘pas toe of leg uit’ lijst van het Forum Standaardisatie. Oefen via het strategisch leveranciers management (SLM) van de overheid druk uit op de cloudleveranciers om open standaarden te implementeren. Nog beter is het om deze druk met gelijkgestemde lidstaten op Europees niveau uit te oefenen.

§ 3.6 Laat op de lijst van het Forum Standaardisatie standaarden toe voor leveranciersonafhankelijkheid en digitale soevereiniteit, ook als ze niet toepasbaar zijn op gegevensuitwisseling tussen organisaties

Forum Standaardisatie richt zich vooralsnog alleen op standaarden voor gegevensuitwisseling *tussen* organisaties. Dat maakt het moeilijk om standaarden te verplichten zoals IMAP, die cruciaal zijn voor dataportabiliteit en leveranciersonafhankelijkheid, maar die doorgaans niet worden gebruikt voor gegevensuitwisselingsstandaarden tussen organisaties.

Advies aan het Forum Standaardisatie: onderzoek of de scope van de ‘pas toe of leg uit’-lijst binnen het bestaande mandaat kan worden verbreed met standaarden die leveranciersonafhankelijkheid en digitale soevereiniteit bevorderen, ook als deze standaarden niet overwegend worden toegepast op gegevensuitwisseling *tussen* organisaties.

§ 3.7 Identificeer open standaarden voor dataportabiliteit die verplicht moeten worden en meld deze aan bij het Forum Standaardisatie

Er zijn nog weinig open standaarden die dataportabiliteit ondersteunen. ISO 8000 biedt richtlijnen voor het effectief en efficiënt uitwisselen van data tussen verschillende systemen, organisaties en technologieën. Dit omvat standaardisatie van formats en terminologie om misverstanden en fouten te voorkomen. Er is echter geen vastgestelde standaard voor uitwisseling van gegevens opgenomen in databases.

Advies aan de overheid: richt een werkgroep op die open standaarden voor dataportabiliteit identificeert en aanmeldt voor verplichting op de ‘pas toe of leg uit’ lijst van het Forum Standaardisatie. Het kan ook gaan om standaarden die nog ontwikkeld worden of moeten worden. In het laatste geval kan de werkgroep aangeven wie deze standaarden zou moeten ontwikkelen,

liefst in Europees verband. Maak praktische keuzen voor de periode waarin deze standaarden nog niet bestaan. Kies bijvoorbeeld voor Amazon Simple Storage Service (S3) API-specificatie voor bestandsuitwisseling tot hier een open standaard voor is ontwikkeld. Stel een lijst op van te ondersteunen opensource databaseformaten die cloudaanbieders tenminste moeten implementeren, en die door overheidspartijen gebruikt worden zoals Postgres, Mysql en Mongo.

§ 3.8 Verplicht standaarden die cloud interoperabiliteit ondersteunen en zet druk op leveranciers om ze te implementeren

Ter bevordering van de interoperabiliteit tussen clouddiensten van verschillende leveranciers zijn in dit onderzoek diverse standaarden geïdentificeerd die nog niet op de lijst van Open standaarden van het Forum Standaardisatie staan, maar mogelijk wel in aanmerking komen voor verplichting.

Advies aan de overheid: doe nader onderzoek welke van deze standaarden in aanmerking komen voor opname op de ‘pas toe of leg uit’ lijst van het Forum Standaardisatie. Sluit hierbij aan op standaarden die via de Data Act worden verplicht. Dit onderzoek kan worden gedaan door dezelfde werkgroep die in advies 3.6 genoemd werd.

§ 3.9 Leg best practices vast

Standaarden en normenkaders zijn cruciaal, maar ook belangrijk is het delen van kennis en ervaring over de toepassing ervan.

Advies aan de overheid: leg ook *best practices* vast over de implementatie van clouddiensten met normenkaders en standaarden. Net zoals ISO 27002 een soort *best practice* uitwerking is van ISO 27001. Dit geeft meer praktische handvatten aan overheden die de standaarden moeten uitvragen en normenkaders moeten toepassen.

§ 4. Standaarden voor de cloud

§ 4.1 Soorten cloudstandaarden

Voor het onderzoek is gebruik gemaakt van de drie servicemodellen van clouddiensten zoals gedefinieerd door NIST SP 800-145: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS). Bijlage 4 geeft een nadere toelichting van deze drie

servicemodellen. Al deze servicemodellen worden door overheidsorganisaties bij leveranciers afgenomen.

De drie servicemodellen van cloudcomputing hebben een scala aan standaarden nodig om interoperabiliteit, informatiebeveiliging, privacy en portabiliteit te bevorderen:

1. **Beveiligings- en privacystandaarden:** De implementatie van de beveiligingsstandaarden draagt bij aan het beperken van het risico van toegang door onbevoegden van informatie die impact kan hebben op de "informatieveiligheid" van de eigenaren en gebruikers van die informatie. De standaarden hebben betrekking op aspecten zoals data-encryptie, authenticatie, autorisatie en auditlogboekregistratie.
   Privacystandaarden richten zich op het betrouwbaar verwerken en vertrouwelijk houden van persoonsgegevens die in de cloud worden opgeslagen en/of daar worden verwerkt. Hierbij kan ook gedacht worden aan standaarden die betrekking hebben op gegevensmaskering, anonimisering en pseudonimisering.

2. **Portabiliteitstandaarden:** Deze standaarden maken het gemakkelijker om applicaties en gegevens van de ene cloudomgeving naar de andere te verplaatsen. Denk hierbij aan standaarden voor containerization en orchestratie. Ze kunnen helpen bij het vermijden van vendor lockin en het ondersteunen van multi-cloudstrategieën.

3. **Interoperabiliteitsstandaarden:** Deze standaarden zorgen ervoor dat verschillende cloudservices en -componenten met elkaar op een gestandaardiseerde wijze kunnen communiceren en gegevens kunnen uitwisselen. Deze kunnen ook helpen bij het vermijden van vendor lockin en het ondersteunen van multi-cloudstrategieën.

4. **Overige standaarden:** Standaarden die niet passen in bovenstaande classificatie maar wel relevant zijn voor cloud en clouddiensten en daarom niet ongenoemd mogen blijven.

Per soort standaard worden in onderliggen rapport de volgende beschouwingsaspecten behandeld:

- Normen.
- Bestaande standaarden opgenomen op de lijst van Open standaarden van het Forum Standaardisatie.
- Bestaande standaarden en standaard technologieën die nog niet zijn opgenomen op de lijst van Open standaarden.
- Standaarden die in ontwikkeling zijn.
- Ontbrekende standaarden, zogenaamde witte vlekken.

Bij het onderscheid tussen *standaarden* en *normen* zijn in het onderzoek de volgende definities gehanteerd: een *standaard* is een algemeen aanvaarde specificatie of richtlijn voor de beste

praktijk, terwijl een *norm* een officieel vastgestelde eis is waaraan producten, diensten of processen moeten voldoen.

Dit document gebruikt het woord ‘standaard’ in brede zin. Hieronder vallen zowel open standaarden en leveranciersafhankelijke (‘proprietary’) standaarden, als technologieën die als de facto standaard opgevat kunnen worden.

§ 4.2 Beveiligings- en privacystandaarden

Privacy en veiligheid is een belangrijk aandachtsgebied voor gebruikers van clouddiensten. De cloudvoorziening moet voldoen aan alle privacy en veiligheidseisen, net zoals deze nu gelden voor on-premise voorzieningen.

Beveiligings- en privacystandaarden zijn te bezien op meerdere lagen (strategisch, tactisch en operationeel). Uit de interviews met de experts komt het beeld naar voren van meerdere en elkaar deels overlappende certificatieschema’s op tactisch niveau, elkaar deels overlappende auditingframeworks op operationeel niveau, en daarnaast ook meerdere frameworks en richtlijnen voor cloudbeveiliging.

In het kader van de cloud is het ook belangrijk dat de persoonsgegevens veilig worden opgeslagen en verwerkt. Hiervoor zijn er binnen de kaders van Europese wetgeving drie varianten. Persoonsgegevens worden:

- in de EU opgeslagen en verwerkt,
- worden in een land waarvoor een adequaatheidsbesluit geldt verwerkt en opgeslagen, of
- worden in een land verwerkt en opgeslagen waarbij er ten aanzien van die verwerkingen waarborgen zijn vastgesteld waaruit blijkt dat de bescherming van persoonsgegevens dezelfde bescherming heeft als ware de verwerking in de EU.

Voor een gebruiker is het momenteel is nog niet altijd duidelijk waar de cloudvoorziening fysiek staat en wie toegang heeft tot deze voorziening. Ook is het tot nu toe is het vrij gebruikelijk dat het beheer van een cloudvoorziening in landen wordt uitgevoerd die niet dezelfde regels hebben ten aanzien van de bescherming van persoonsgegevens. Cloudleveranciers werken hard aan de realisatie van cloudvoorzieningen die voldoen aan een van de drie eerdergenoemde varianten.

§ **4.2.1 Standaarden op de lijst van Open standaarden**

De beveiligings- en privacystandaarden bouwen voor een groot deel voort op de beveiligings- en privacystandaarden die al op de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie zijn

opgenomen. Het gaat hier om:

1. TLS: TLS zorgt voor beveiligde internetverbindingen, met als doel de veilige uitwisseling van gegevens tussen een internetsystemen (zoals websites of mailservers);

2. DNSSEC: Met DNSSEC kan de ontvanger de echtheid van de domeinnaaminformatie (waaronder IP-adressen) controleren. Dit voorkomt bijvoorbeeld dat een aanvaller het IP-adres ongemerkt manipuleert (DNS-spoofing) en daarmee verstuurde e-mails omleidt naar een eigen mailserver of gebruikers misleidt naar een frauduleuze website.

3. STARTTLS en DANE: Mailverkeer tussen mailservers verloopt via SMTP. STARTTLS in combinatie met DANE gaan, in aanvulling op SMTP, afluisteren of manipuleren van dit mailverkeer door internetcriminelen tegen.

4. HTTPS en HSTS: HTTPS en HSTS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowser). Dit maakt het voor cybercriminelen moeilijker om verkeer om te leiden naar valse websites en om de inhoud van webverkeer te onderscheppen;

5. NEN-ISO/IEC 27001: De norm ISO 27001 beschrijft eisen waar een 'Information Security Management System' (ISMS) aan moet voldoen;

6. SAML: Security Assertion Markup Language (SAML) is een standaard voor het veilig uitwisselen van authenticatie- en autorisatiegegevens van gebruikers tussen verschillende organisaties. SAML maakt het mogelijk om op een veilige manier via het internet toegang te krijgen tot diensten van verschillende organisaties, zonder dat je per dienst eigen inloggegevens nodig hebt, of bij elke dienst apart moet inloggen. SAML wordt gebruik bij onder andere DigiD machtigen en eHerkenning.

De beveiligings- en privacystandaarden bouwen voor een groot deel voort op de beveiligings- en privacystandaarden die al op de lijst aanbevolen standaarden staan opgenomen. Het gaat hier om:

1. Oauth2.0 : Met OAuth 2.0 kunnen gebruikers of organisaties een programma of website toegang geven tot specifieke (privé)gegevens, die opgeslagen zijn op een ander systeem, zonder hun gebruikersnaam en wachtwoord uit handen te geven.

Tijdens het onderzoek werd aangegeven dat de attributen die in het kader van Oauth2.0 worden uitgewisseld uitbreiding behoeven als ze in het kader van Trusted Cloud van het Ministerie van Justitie en veiligheid worden ingezet;

2. IP Sec: De standaard maakt het mogelijk om IP-verbindingen te encrypten. Hierdoor is het netwerk beveiligd waardoor gevoelige data kan worden uitgewisseld. Vooral relevant voor VPN's. In andere gevallen is beveiliging op transport niveau meer toepasselijk.

3. OIDC: OpenID Connect (OIDC) is een open en gedistribueerde manier om één authenticatiedienst naar keuze te kunnen hergebruiken bij meerdere (semi-)overheidsdienstverleners, bij gebruik vanuit onder andere webapplicaties en mobiele apps. Belangrijkste redenen om op OIDC in te zetten is de actieve ontwikkelingen en de mobile-first strategie ondersteuning van digitale overheidsdiensten.

§ 4.2.2 Normen en (auditing) frameworks niet op de lijst van Open standaarden

1. **Certification Scheme on Cloud Services (EUCS):** Het Certification Scheme on Cloud Services (EUCS) wordt in opdracht van de Europese Commissie ontwikkeld door ENISA en omgevormd tot twee Europese standaarden door CEN/CENELEC. De verwachting is dat dit schema in 2024 beschikbaar komt. Dit schema stelt normen vast voor de beveiliging van gegevens die worden opgeslagen en verwerkt in de cloud. Het doel is om het vertrouwen in cloudserviceproviders te vergroten en tegelijkertijd de naleving van de EU-regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG), te verzekeren. Clouddienstverleners kunnen zich dan laten certificeren op 3 verschillende Assurance levels (Basic, Substantial en High). De certificaten worden dan Europees erkend en spelen ook een rol bij de ontwikkeling van Europese regelgeving waar de mogelijkheid bestaat "verwacht conform" te zijn als de clouddienstenleverancier is gecertificeerd voor EUCS. Door middel van EUCS kunnen cloudserviceproviders aantonen dat ze voldoen aan hoge beveiligingsnormen, wat essentieel is voor bedrijven en organisaties die gevoelige gegevens in de cloud willen opslaan en verwerken. Opmerkelijk feit: er is nog geen link gelegd vanuit de GDPR/AVG naar deze certificering.

2. **CCM-framework**: De Cloud Control Matrix (CCM) is een besturingsframework dat specifiek is ontworpen voor cloudcomputing-omgevingen. Het biedt een gedetailleerde structuur van beveiligingsbeleid, procedures en technische maatregelen die kunnen worden toegepast op verschillende cloudservicemodellen, waaronder Infrastructure as a Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS). Naast de kerncontroledoelstellingen omvat CCM:
   - Implementatierichtlijnen
   - Model voor gedeelde veiligheidsverantwoordelijkheid
   - Auditrichtlijnen
   - In kaart brengen van andere relevante beveiligingsnormen en -kaders en wettelijke en regelgevende vereisten
   - Continue zekerheidsstatistieken
   - Beoordelingsvragenlijst (Consensus Initiative-vragenlijst - CAIQ)

   De CCM is ook een open standaard die gratis beschikbaar is. De CCM vormt de ruggengraat van het Security, Trust, Assurance, and Risk (STAR)-programma van de Cloud Security Aliance (CSA), een breed toegepast cloud-borgingsprogramma dat een ecosysteem vormt van de best practices, standaarden, technologie en auditpartners. STAR ondersteunt organisaties bij

het effectief en efficiënt aanpakken van het definiëren van vertrouwen in de cloud, het bevorderen van verantwoordelijkheid, het evalueren van risico's, het meten van zekerheid en het vereenvoudigen van compliance en inkoop.
Als onderdeel van het STAR-programma kunnen organisaties de naleving van de CCM-vereisten aantonen via een reeks beoordelingsmechanismen, zoals:
 STAR Self Assessment: een zelfevaluatie op basis van een gestandaardiseerde vragenlijst (CAIQ)
 STAR-certificering: een onafhankelijk certificeringsproces van derden op basis van ISO27001-vereisten, aangevuld met CCM-controles en aanvullende transparantievereisten.
 STAR Attestation: een onafhankelijk attesteringsproces van derden op basis van SOC 2-vereisten, aangevuld met CCM-controles en aanvullende transparantievereisten.
Het STAR-programma vereist dat organisaties details over hun beveiligings- en nalevingspositie, inclusief de naleving van regelgeving, standaarden en raamwerken, publiceren in een openbaar beschikbaar register, genaamd STAR Registry. Deze informatie is waardevol voor huidige en potentiële klanten die zekerheid zoeken over de beveiligingspraktijken van cloudserviceproviders (CSP's). Samenvattend bieden het STAR-programma en CCM een gestructureerde aanpak voor organisaties, zowel aanbieders van clouddiensten als gebruikers, om hun cloudbeveiligingspraktijken te verbeteren en onder de aandacht te brengen, waardoor risicobeheer, naleving van de regelgeving en transparantie in de cloudcomputingruimte worden vergemakkelijkt.

3. QERMS (Qualified Registered Electronic Mail Service): QERMS, of Qualified Registered Electronic Mail Service, is een geavanceerde vorm van elektronische communicatie die bedoeld is om de traditionele aangetekende post te vervangen. Het biedt een juridisch erkende manier om elektronische berichten met een hoge mate van zekerheid te verzenden en te ontvangen, waarbij de identiteit van de afzender en de ontvanger wordt geverifieerd en de integriteit en de onweerlegbaarheid van de verzonden inhoud wordt gewaarborgd. Dit houdt in dat zowel de verzend- als ontvangsttijden van berichten nauwkeurig worden vastgelegd, wat QERMS ideaal maakt voor juridische en officiële correspondentie waarbij bewijs van verzending en ontvangst essentieel is. QERMS wordt vaak gebruikt in zakelijke en overheidsomgevingen voor het betrouwbaar uitwisselen van gevoelige of juridisch bindende documenten. QERMS is opgesteld conform EU Regulation eIDAS (EU) No. 910/2014 en is gebaseerd op ETSI 319 401, ETSI EN 319 521 en ETSI EN 319 531.

4. NTA7516: NTA 7516 is een Nederlandse technische afspraak (NTA) die richtlijnen biedt voor het veilig uitwisselen van gezondheidsinformatie via e-mail. Deze norm is specifiek ontwikkeld om de privacy en de beveiliging van patiëntgegevens te waarborgen bij het versturen van medische informatie tussen zorgverleners en patiënten of tussen verschillende zorginstellingen. NTA 7516 stelt eisen aan aspecten zoals de identificatie en authenticatie van de verzender en ontvanger, de versleuteling van de data, en de integriteit en vertrouwelijkheid van de verstuurde informatie. Het doel van deze norm is om te zorgen dat elektronische communicatie in de zorgsector voldoet aan de strikte privacy vereisten, zoals vastgelegd in de

Algemene Verordening Gegevensbescherming (AVG), en om een veilige en betrouwbare uitwisseling van medische gegevens te faciliteren.

5. MTA-STS (Mail Transfer Agent Strict Transport Security) is een beveiligingsstandaard die de veiligheid van e-mailtransport tussen servers verhoogt door het afdwingen van TLS (Transport Layer Security) encryptie en het specificeren van de vereiste TLS-beleidsniveaus. Deze standaard is ontworpen om veelvoorkomende beveiligingsproblemen aan te pakken, zoals man-in-the-middle-aanvallen, waarbij e-mails tijdens het transport onderschept kunnen worden. Door het publiceren van een MTA-STS-beleid op hun domein, kunnen domeineigenaren aangeven dat hun servers TLS ondersteunen en definiëren welke versie van TLS moet worden gebruikt, wat zorgt voor een veiligere e-mailuitwisseling. Dit helpt bij het waarborgen van de vertrouwelijkheid en integriteit van e-mails tijdens de overdracht en is een belangrijke stap in de richting van een veiligere e-mailinfrastructuur. MTA-STS verbetert dus de beveiliging van e-mailcommunicatie door te zorgen voor gecodeerde verbindingen en het verminderen van de kans op onderschepping of afluisteren.
   Opmerking: in het expertadvies over STARTTLS en DANE van augustus 2018 wordt het Forum Standaardisatie opgeroepen om over een jaar na de expertbijeenkomst van STARTTLS en DANE de stand van zaken rond de alternatieve technologie MTA-STS te evalueren.

6. mTLS: Mutual TLS (mTLS) is een beveiligingsprotocol waarbij zowel de client als de server elkaar verifiëren via TLS (Transport Layer Security) certificaten, een proces dat een extra beveiligingslaag biedt bovenop de standaard TLS/SSL-handshake. In tegenstelling tot standaard TLS, waarbij alleen de server identiteit aantoont aan de client, vereist mTLS dat beide partijen hun identiteit aantonen door middel van digitale certificaten. Dit versterkt de beveiliging doordat het beide partijen zekerheid geeft over de identiteit van de ander, waardoor het risico op onderschepping of vervalsing van gegevens vermindert. mTLS wordt vaak gebruikt in omgevingen waar strenge beveiligingseisen gelden, zoals in financiële diensten, gezondheidszorg en bij interne netwerkcommunicatie van bedrijven. Het zorgt voor een betrouwbaardere en veiligere communicatie doordat ongeautoriseerde toegang tot netwerken en data wordt voorkomen.

Er zijn vele **ISO**-standaarden op het vlak informatiebeveiliging, cyberveiligheid en privacybescherming, waaronder de ISO 27100-serie. Het gaat hier om generieke standaarden. De volgende ISO-standaarden richten zich op cloud:

1. **ISO/IEC 27017**: ISO/IEC 27017 is een internationale norm die richtlijnen en best practices biedt voor informatiebeveiliging in cloudomgevingen. Deze norm is een uitbreiding op ISO/IEC 27002, specifiek gericht op cloudbeveiliging, en biedt aanvullende beveiligingscontroles en implementatiebegeleiding voor zowel cloudserviceproviders als cloudgebruikers. ISO/IEC 27017 richt zich op aspecten zoals de beveiliging van cloudinfrastructuur, beheer van virtuele machines, gegevensencryptie, en operationele beveiligingsprocedures in de cloud. Het helpt organisaties bij het identificeren en beheren van de beveiligingsrisico's die gepaard gaan met het gebruik van cloudservices en ondersteunt hen

bij het naleven van regelgeving en industrienormen. Door het volgen van deze norm kunnen organisaties de integriteit, vertrouwelijkheid en beschikbaarheid van hun gegevens in de cloud beter waarborgen, wat van cruciaal belang is in het huidige digitale tijdperk.

2. **ISO/IEC 27018**: ISO/IEC 27018 is een internationale standaard die richtlijnen biedt voor de bescherming van persoonlijke gegevens in de cloud. Deze norm is een code voor de praktijk voor cloudserviceproviders die persoonlijke data verwerken, en vormt een aanvulling op bestaande ISO/IEC 27001- en 27002-normen voor informatiebeveiligingsbeheer. ISO/IEC 27018 richt zich specifiek op privacyaspecten, waaronder het beheer van persoonlijke identificeerbare informatie (PII), transparantie over het gebruik van gegevens, en sterke beveiligingsmaatregelen om de privacy van de gebruikers te beschermen. Deze standaard is van bijzonder belang voor organisaties die cloudgebaseerde diensten aanbieden of gebruiken, en helpt hen te voldoen aan wettelijke privacyvereisten en het vertrouwen van klanten en stakeholders te behouden door aan te tonen dat ze serieuze maatregelen nemen om persoonlijke gegevens te beschermen.

§ 4.2.3 Witte vlekken

Voor de privacy en beveiligingstandaarden zijn geen witte vlekken gedefinieerd. Het beeld is dat er voldoende normen, standaarden en frameworks zijn, die zelfs overlappend zijn aan elkaar. Voor privacy en beveiliging moet juist worden gewerkt aan het verminderen van de overlap.

§ 4.3 Portabiliteitstandaarden

Portabiliteitstandaarden zijn richtlijnen en specificaties die ontworpen zijn om de overdraagbaarheid van gegevens, software, systemen tussen verschillende platforms, systemen en apparaten te vergemakkelijken. In de context van cloudstandaarden zijn portabiliteitstandaarden essentieel om applicaties, systemen en gegevens te kunnen verplaatsen van de ene cloudomgeving naar de andere.

We maken onderscheid tussen twee typen portabiliteitstandaarden:

1. **Standaarden voor systeem- en applicatieportabiliteit:** Dit betreft de mogelijkheid van software om te functioneren op verschillende hardware of besturingssystemen zonder significante wijzigingen. Deze standaarden helpen bij het verminderen van afhankelijkheden van specifieke platformen.

2. **Standaarden voor dataportabiliteit:** Dit verwijst naar het vermogen om gegevens gemakkelijk van het ene systeem of platform naar het andere te verplaatsen. Dataportabiliteit is cruciaal in het digitale tijdperk, waar gegevens vaak moeten worden overgedragen tussen verschillende applicaties, databases of opslagsystemen. Standaarden voor dataportabiliteit

zorgen ervoor dat deze gegevensoverdracht soepel verloopt, met behoud van de integriteit en bruikbaarheid van de gegevens.

§ 4.3.1 Standaarden voor systeem- en applicatieportabiliteit niet op de lijst van Open standaarden

De basis bij systeem- en applicatieportabiliteit ligt bij containerization en virtualisatie. Containerization is een technologie die applicaties en hun afhankelijkheden inpakt in containers, waardoor een consistente, geïsoleerde en lichtgewicht omgeving voor applicaties ontstaat. Het resultaat is makkelijk verplaatsbare containers tussen verschillende cloudleveranciers. Deze aanpak bevordert portabiliteit, schaalbaarheid en efficiëntie, en is cruciaal voor moderne ontwikkelmethoden.

Naast containerization speelt virtualisatie nog een belangrijke rol. Virtualisatie is een zwaardere vorm van abstractie van de fysieke machine, aangezien virtuele machine een volledig OS bevat.

In de praktijk worden deze technologieën vaak complementair gebruikt. Veel bedrijven gebruiken VM's voor het creëren van robuuste, geïsoleerde omgevingen voor hun infrastructuur, terwijl ze containers gebruiken binnen die VM's om hun applicaties efficiënt en consistent te beheren.

Tijdens het onderzoek zijn de volgende standaarden op het gebied van systeem- en applicatieportabiliteit genoemd die niet op de lijst van Open standaarden van het Forum Standaardisatie voorkomen:

1. **Kubernetes**: Kubernetes, vaak afgekort als K8s, is een krachtig opensource systeem voor het beheren van containerized applicaties in een cluster. Het werd oorspronkelijk ontwikkeld door Google en is gebaseerd op hun interne systeem genaamd Borg. Kubernetes werd in 2014 vrijgegeven als open-source software. Kubernetes is op dit moment dé de facto standaard voor containerorchestratie wereldwijd.

Kubernetes is een open-source platform ontworpen voor het automatiseren van het deployen, schalen en beheren van containerized applicaties, waardoor het eenvoudiger wordt om complexe applicaties betrouwbaar en op schaal uit te rollen en te beheren.

Kubernetes wordt breed ondersteund door nagenoeg alle cloudproviders. De drie hyperscalers bieden ieder een standaard setup gebaseerd op Kubernetes. Kubernetes is strikt genomen geen standaard maar een opensource technologie en daarom een standaard technologie ter bevordering van de portabiliteit.

2. **OCI (Docker)**: De Open Container Initiative (OCI), opgericht in 2015 door Docker en andere leiders in de containerindustrie, is een project onder de Linux Foundation. Het doel van OCI is het creëren van open industriestandaarden rond containerformaten en -runtimes.

Een belangrijk onderdeel van de OCI is de specificatie van de container runtime en image formaat. Docker, als een toonaangevend platform in containerization, speelt een cruciale rol in deze standaardisatie-inspanningen. Docker containers zijn gebaseerd op OCI-specificaties, wat betekent dat ze compatibel zijn met andere OCI-conforme tools en systemen. Dit zorgt voor consistentie in de manier waarop containers worden gebouwd, gedeeld en uitgevoerd, ongeacht de onderliggende omgeving. Docker heeft ook bijgedragen aan de ontwikkeling van belangrijke standaarden en tools in het OCI-ecosysteem, wat de algemene acceptatie en het succes van containerization in de software-industrie verder heeft gestimuleerd. De OCI-specificaties zijn te vinden op GitHub.

3. **Haven:** Haven kan gezien worden als het Nederlandse implementatieprofiel voor Kubernetes. Het schrijft een specifieke configuratie van Kubernetes voor die dient te worden geïmplementeerd op bestaande technische infrastructuur, bijvoorbeeld een cloud of on-premise platform. Hiermee voorziet het in een standaard inrichting gericht voor de Nederlandse overheid. De voorgeschreven configuratie zorgt ervoor dat iedere Haven omgeving functioneel gelijk is ongeacht de onderliggende technische infrastructuur. Zie het als een abstractielaag die resulteert in een gezamenlijk vertrekpunt. Dit brengt diverse voordelen met zich mee: uniformiteit in technische infrastructuur, uitwisselbaarheid van toepassingen, leveranciersonafhankelijkheid, platformonafhankelijkheid en kostenreductie.

4. **Terraform**: Terraform, ontwikkeld door HashiCorp, is een invloedrijke opensource infrastructuur als code (IaC) tool die het mogelijk maakt om infrastructuur te definiëren en te beheren met behulp van een hoog-niveau configuratietaal. Het stelt gebruikers in staat om zowel cloud als on-premise middelen op een consistente en voorspelbare manier te implementeren en te beheren. Terraform gebruikt declaratieve configuratiebestanden die de gewenste staat van de infrastructuur specificeren, variërend van fysieke apparaten zoals servers en netwerkapparatuur tot hoog-niveau componenten zoals DNS-entries, SaaS-kenmerken en meer. Dit maakt het mogelijk voor ontwikkelaars en operators om infrastructuur op een efficiënte, herhaalbare manier uit te rollen en te beheren.

Eén van de sleutelkenmerken van Terraform is de ondersteuning van een breed scala aan infrastructuurproviders, zoals AWS, Microsoft Azure, Google Cloud, VMWare, OpenStack, en vele anderen. Het brede bereik van compatibiliteit stelt gebruikers in staat om multi-cloud strategieën te implementeren en te beheren zonder te hoeven leren omgaan met de implementatiedetails van elke provider.

Terraform, hoewel geen implementatie van een formele externe standaard, is gebouwd rond een aantal kernprincipes en -ontwerpen. Terraform is een standaard in de wereld van infrastructuur als code (IaC). De belangrijkste standaard die Terraform introduceert en volgt, is zijn eigen configuratietaal genaamd HashiCorp Configuration Language (HCL). Aangezien Terraform wereldwijd als de de facto standaard wordt gezien is deze opgenomen in dit rapport.

Terraform was een volledig opensource product, maar is dat sinds enige tijd niet meer. Alhoewel het nog breed wordt toegepast zijn er ook opensource forks, waarvan OpenTofu de bekendste is.

5. **Open Virtualization Format (OVF)**: Open Virtualization Format (OVF) is een open standaard voor het verpakken en distribueren van softwareoplossingen voor virtuele machines, ontwikkeld door de Distributed Management Task Force (DMTF). OVF is ontworpen om portabiliteit en eenvoudige installatie van virtuele applicaties over verschillende virtualisatieplatforms heen te vergemakkelijken. Dit formaat beschrijft een virtuele machine, inclusief de structuur van de VM, de benodigde hardwarebronnen en de vereiste software-afbeeldingen. Het omvat ook metadata zoals productinformatie, licenties en configuratieopties.

OVF biedt een standaardmanier om virtuele machines en bijbehorende configuraties te verpakken in één distributie-eenheid. Deze aanpak vereenvoudigt het beheer van multi-tier applicaties, vermindert de complexiteit van het inzetten en verplaatsen van VM's tussen verschillende omgevingen en zorgt voor grotere interoperabiliteit tussen verschillende virtualisatieplatforms. Door het gebruik van OVF kunnen organisaties en individuele gebruikers eenvoudig complexe multi-platform, multi-VM-workloads distribueren en beheren. OVF wordt ondersteund door alle belangrijke virtualisatie leveranciers waaronder: Virtual Box, Red Hat, VMWare, Microsoft, IBM, Google en AWS.

6. **ISO/IEC 19941:2017**: ISO/IEC 19941:2017 is een internationale norm die richtlijnen en best practices biedt voor cloudcomputing interoperabiliteit en portabiliteit. Deze norm richt zich op het vergemakkelijken van de uitwisseling en het gebruik van data en toepassingen over verschillende cloudservices en platforms heen. Het definieert termen en concepten gerelateerd aan interoperabiliteit (het vermogen van verschillende systemen om effectief samen te werken) en portabiliteit (het vermogen om toepassingen en data gemakkelijk te verplaatsen tussen verschillende cloudomgevingen). ISO/IEC 19941:2017 behandelt essentiële onderwerpen zoals het ontwerp van cloudsystemen, dataformaat en -uitwisseling, en de interactie tussen verschillende cloudservice-modellen. Het streeft ernaar om organisaties te ondersteunen bij het verminderen van vendor lockin risico's en het verbeteren van de flexibiliteit en keuzevrijheid in cloudcomputing oplossingen.

Naast bovengenoemde is een aantal standaarden nog in ontwikkeling die wellicht in de toekomst relevant zullen worden, waaronder Liqo.io. Liqo.io is een opensource project dat dynamische en naadloze Kubernetes federated cluster topologieën mogelijk maakt. Het ondersteunt heterogene infrastructuren, waaronder on-premise, cloud en edge omgevingen. Het is ontwikkeld door de Italiaanse universiteit van Turijn.

§ 4.3.2 Witte vlekken

De hierboven opgesomde standaarden staan niet op de lijst van Open standaarden van het Forum Standaardisatie. Deze lijst van standaarden voorzien voor een groot deel in de behoefte van

systeem en applicatieportabiliteit met betrekking tot clouddiensten. Het is dus van belang om te onderzoeken of deze standaarden opgenomen kunnen worden op de lijst van Open standaarden.

§ 4.3.3 Standaarden voor dataportabiliteit niet op de lijst van open standaarden

Dataportabiliteit gaat over het makkelijk kunnen overdragen van gegevens van het ene systeem naar het andere systeem. De ISO-norm ISO 17788 geeft de volgende definitie van dataportabiliteit:

> *"Het vermogen om gegevens gemakkelijk over te dragen van het ene systeem naar het andere, zonder dat het nodig is om gegevens opnieuw in te voeren. Het gaat hier om het gemak waarmee de gegevens verplaatst kunnen worden. Dit kan bereikt worden doordat het bronsysteem de gegevens levert in precies het formaat dat geaccepteerd wordt door het doelsysteem. Zelfs als de formaten niet overeenkomen, kan de transformatie tussen deze formaten eenvoudig en rechttoe rechtaan zijn met behulp van algemeen beschikbare hulpmiddelen. Aan de andere kant, een proces van het uitprinten van de gegevens en deze opnieuw invoeren in het doelsysteem kan niet beschreven worden als 'gemakkelijk'."*

Bij standaarden voor dataportabiliteit dient onderscheid gemaakt te worden tussen data in de vorm van bestanden (zoals: foto's, video's of officebestanden) en complexe data, zoals databases.

Op lijst open standaarden van het Forum Standaardisatie is een beperkt aantal standaarden opgenomen voor dataportabiliteit op bestandsniveau:

1. CalDAV: CalDAV is een internetstandaard die wordt gebruikt voor het synchroniseren en delen van kalendergegevens op servers. Het is een uitbreiding op WebDAV (Web-based Distributed Authoring and Versioning), een protocol gebaseerd op HTTP, en is ontworpen om gebruikers toegang te geven tot planningsinformatie op een server. CalDAV stelt gebruikers in staat om afspraken en geplande evenementen te creëren, wijzigen en verwijderen op een gedeelde server, waarbij de wijzigingen automatisch worden bijgewerkt en gesynchroniseerd over alle apparaten van de gebruiker.

2. WebDAV: WebDAV (Web-based Distributed Authoring and Versioning) is een uitbreiding van het HTTP-protocol dat gebruikers in staat stelt om op een collaboratieve manier bestanden te creëren, bewerken en beheren op webservers. Deze technologie maakt het mogelijk voor meerdere gebruikers om samen te werken aan documenten en bestanden alsof ze zich op een lokale netwerkschijf bevinden, met functionaliteiten zoals het uploaden en downloaden van bestanden, het creëren van mappen, het kopiëren en verplaatsen van bestanden, en het bijhouden van versies. Veelgebruikt in verschillende toepassingen zoals contentmanagementsystemen, online samenwerkingstools en cloudopslagdiensten, biedt WebDAV een gestandaardiseerde manier voor gebruikers om direct via hun webbrowser of specifieke clientsoftware toegang te krijgen tot en te werken met bestanden op afstand.

Beide standaarden hebben de status ‘aanbevolen’ op de lijst van het Forum Standaardisatie. Verschillende experts pleiten ervoor om CalDAV en WebDAV de status ‘pas toe of leg uit’ te geven, en zo te verplichten bij de aanschaf van clouddiensten. Naast genoemde standaarden bestaan er ook gangbare tools zoals *rsync* en *dd* om bestanden tussen systemen uit te wisselen.

Er is geen breed geaccepteerde open standaard voor Cloud-opslag. Amazon Simple Storage Service (S3) kan beschouwd worden als een de facto standaard in cloudopslag, vanwege zijn uitgebreide acceptatie en gebruik in de industrie. Veel andere cloudopslagdiensten en -tools bieden compatibiliteit bieden met de S3 API (Application Programming Interface Naast Amazon zijn er diverse leveranciers die objectstorage producten en diensten aanbieden volgens de S3-standaard, zoals Minio. Vergelijkbare functionaliteit wordt geboden door Microsoft Azure Blob Storage.

Naast bovengenoemde standaarden is het DTP het vermelden waard. Het Data Transfer Project (DTP) is een open-source initiatief dat zich richt op het mogelijk maken van dataportabiliteit tussen meerdere online platforms. Het project werd op 20 juli 2018 gelanceerd door Google en heeft partnerschappen met grote technologiebedrijven zoals Facebook, Microsoft, Twitter en Apple. DTP faciliteert door de klant gecontroleerde bulkgegevensoverdrachten tussen twee online-diensten, waardoor gebruikers hun gegevens gemakkelijker tussen verschillende platforms kunnen verplaatsen.

Door de samenwerking tussen verschillende technologiegiganten streeft het project ernaar om een naadloze en efficiënte ervaring te creëren voor gebruikers die hun gegevens willen overzetten, bijvoorbeeld bij het wisselen van e-maildiensten, sociale mediaplatforms, of dataopslagdiensten. DTP is in de eerste fase van ontwikkeling.

§ 4.3.4 Witte vlekken

Voor data opgeslagen in databases is geen vastgestelde standaard wat gestandaardiseerde uitwisseling beperkt. De volgende typen database-onafhankelijke bestandsformaten worden genoemd die ook opgenomen zijn op de lijst van aanbevolen standaarden van de Forum Standaardisatie:

- CSV (Comma-Separated Values),
- JSON (JavaScript Object Notation)
- XML(eXtensible Markup Language)
- SQL ISO/IEC 9075 (Standaard SQL)

Dit zijn veelgebruikte formaten voor het exporteren en importeren van gegevens tussen verschillende systemen. Ze worden breed ondersteund en maken het eenvoudig om gestructureerde gegevens te verplaatsen.

Een aantal geïnterviewden opperde om een lijst van veel gebruikte opensource databases vast te stellen en de exportformaten van die databases als de standaard vast te stellen. Veel genoemde databases in dit verband zijn: Postgres, MySql, MariaDb, Mongo en Redis.

§ 4.4 Interoperabiliteitsstandaarden

Interoperabiliteitstandaarden in de context van cloudcomputing zijn cruciaal voor het waarborgen van een naadloze, effectieve interactie tussen verschillende cloudsystemen en -diensten van diverse aanbieders. Interoperabiliteit bevordert dus een meer open, flexibele en schaalbare cloudomgeving, waar gebruikers de vrijheid hebben om diensten van verschillende leveranciers te kiezen en te combineren op basis van hun specifieke behoeften.

In de context van cloudcomputing zijn portabiliteitstandaarden en interoperabiliteitstandaarden nauw met elkaar verbonden, maar ze dienen verschillende doelen. Portabiliteitstandaarden zijn gericht op het mogelijk maken van de overdracht van applicaties, data en diensten tussen verschillende cloudomgevingen zonder significante wijzigingen of verlies van functionaliteit. Interoperabiliteitstandaarden focussen op het waarborgen van de compatibiliteit tussen verschillende cloudsystemen en -services, zodat ze naadloos met elkaar kunnen samenwerken. Interoperabiliteit is cruciaal voor het creëren van een coherente, functioneel rijke cloudomgeving waar verschillende cloudservices en -componenten van verschillende leveranciers kunnen integreren en effectief samenwerken.

Hoewel beide beschouwingsgebieden van standaarden verschillende doelen hebben, zijn ze complementair. Goede portabiliteit vergemakkelijkt interoperabiliteit, omdat systemen die gemakkelijk van het ene naar het andere platform kunnen worden verplaatst, doorgaans ook beter kunnen samenwerken met systemen op die platforms. Er is echter wel overlap tussen beide type standaarden. Overlappende standaarden zijn in paragraaf 4.3 (Portabiliteitstandaarden) opgenomen.

§ 4.4.1 Standaarden op de lijst van Open standaarden

De volgende interoperabiliteitstandaarden die al op de **‘pas toe of leg uit’-lijst** staan kwamen tijdens het onderzoek naar voren:

1. REST (als onderdeel van Digikoppeling): Representational State Transfer (REST) is een architecturale stijl voor het ontwerpen van netwerktoepassingen. Het wordt veel gebruikt voor het bouwen van interactieve applicaties die gebruikmaken van webdiensten. Een RESTful systeem gebruikt HTTP-verzoeken om data te verkrijgen, te creëren, te wijzigen en te verwijderen, wat het geschikt maakt voor gebruik in internettoepassingen. REST is eenvoudig, lichtgewicht en gemakkelijk te begrijpen en te implementeren, waardoor het een populaire

keuze is voor het ontwikkelen van API's (Application Programming Interfaces) in webapplicaties.

2. REST API Design Rules: De standaard REST-API Design Rules geeft een verzameling basisregels voor structuur en naamgeving waarmee de overheid op een uniforme en eenduidige manier REST-API's aanbiedt. Dit maakt het voor ontwikkelaars gemakkelijker om betrouwbare applicaties met te ontwikkelen met API's van de overheid.

3. OpenAPI Specification (OAS): OAS geeft ontwikkelaars van applicaties een eenduidige en leesbare beschrijving van een REST API waarmee zij de API kunnen gebruiken zonder te hoeven weten hoe deze geïmplementeerd is. OAS 3.0 zorgt voor gemakkelijker (her)gebruik van API’s en minder leveranciersafhankelijkheid.

Ook kwam de standaard SCIM naar voren die al op de lijst open standaarden is opgenomen met de status ‘aanbevolen’. SCIM zorgt ervoor dat identiteitsinformatie van gebruikers systeem overstijgend op de juiste plek aanwezig is. Hierdoor kunnen gegevens die niet meer in systemen horen te staan, omdat een gebruiker bijvoorbeeld niet langer in dat systeem hoeft te zijn opgenomen, worden verwijderd. Doordat dit geautomatiseerd gebeurt is relatief weinig inspanning nodig om de gewenste toevoeging of verwijdering van gegevens te realiseren. Deze standaard is gericht op het reduceren van kosten en complexiteit én het voortbouwen op bestaande protocollen. SCIM heeft als doel om gebruikers snel, goedkoop en eenvoudig in, uit en tussen clouddiensten te brengen.

§ 4.4.2 Standaarden niet op de lijst van Open standaarden

De volgende interoperabiliteitstandaarden kwamen tijdens het onderzoek naar voren die nog niet op de lijst Open Standaarden staan:

1. FSC NLX: De software van Federated Service Connectivity NLX stelt (overheids)organisaties in staat om FSC compliant op een eenvoudige, veilige en toegankelijke manier data uit te wisselen. Dit helpt overheidsorganisaties onder andere om aan de nieuwe privacywetgeving te voldoen en om inwoners inzicht te geven in hun gegevens. FSC NLX regelt de volgende zaken:

    1. opzetten van veilige verbindingen;

    2. vindbaar en toegankelijk maken van diensten;

    3. monitoren en beheren van verbindingen binnen een organisatie;

    4. centraal monitoren van gebruik en beschikbaarheid van diensten;

    5. lokaal bijhouden van het gebruik van diensten (logging).

FSC NLX is onderdeel van Common Ground.

2. Open Cloud Computing Interface (OCCI): OCCI is een set van open specificaties voor cloudcomputing, ontwikkeld door de Open Grid Forum. Het biedt een API-standaard voor het beheren van allerlei cloudinfrastructuur, waaronder IaaS (Infrastructure as a Service).

3. Cloud Infrastructure Management Interface (CIMI): Ontwikkeld door de Distributed Management Task Force (DMTF), richt CIMI zich op het beheer van cloudinfrastructuur en streeft het naar een uniforme interface voor de interactie met infrastructuur als een service (IaaS) modellen.

4. Cloud Data Management Interface (CDMI): CDMI is een standaard die specifiek is ontworpen voor dataopslag en datamanagement in de cloud. Het stelt gebruikers in staat om data en bijbehorende metadata in de cloud te creëren, te verwijderen, bij te werken en op te halen.

5. GraphQL: GraphQL is een querytaal voor API’s en een server-side runtime voor het uitvoeren van query’s. GraphQL is niet gebonden aan een specifieke database of opslagsysteem en wordt in plaats daarvan gebruikt om bestaande code en gegevens in termen van een API te beschrijven. Het biedt een efficiëntere, krachtigere en flexibelere aanpak van API-design dan traditionele REST-API's. Met GraphQL kan een client precies specificeren welke gegevens het nodig heeft, wat over- of onder-fetching van gegevens vermindert. Het stelt ook gebruikers in staat om complexe query’s samen te stellen, waarbij gegevens uit meerdere bronnen in een enkel verzoek kunnen worden samengevoegd. Hierdoor is het bijzonder nuttig in moderne web- en mobiele toepassingen, waar het efficiënt beheren van data-overdracht en het verminderen van netwerkverzoeken cruciaal is voor de prestaties.

§ 4.4.3 Witte vlekken

Clouddiensten en met name de hyperscalers bieden allerlei makkelijk toegankelijke proprietary diensten aan ondersteund door proprietary standaarden. Andere cloudaanbieders hebben andere proprietary diensten en standaarden, dit bemoeilijkt de gewenste naadloze, effectieve interactie tussen verschillende cloudsystemen en -diensten van diverse aanbieders. De hierboven genoemde standaarden bevorderen de interoperabiliteit, maar zijn niet afdoende om dit volledig af te dekken. Het gebruik van proprietary standaarden door de verschillende hyperscalers en de vervlechting van deze standaarden, maakt het niet eenvoudig om open standaarden te implementeren. Hier ligt dus een grote uitdaging. Europese wetgeving zal dit op termijn moeten afdwingen.

§ 4.5 Overige standaarden

Ondanks dat het onderzoek zich richt op standaarden voor beveiliging en privacy, portabiliteit en interoperabiliteit met betrekking tot cloudcomputing kwam een aantal aanpalende standaarden en normen ter sprake. Het betreft de volgende standaarden, normen en frameworks:

1. **NIST SP 500-292**: Het NIST Cloud Computing Reference Architecture is een generiek high-level conceptueel model dat dient als een gebruikersgericht referentiepunt.

2. **ISO/IEC 22123-1:** Information technology — Cloud computing — Part 1: Vocabulary

> Bevat definities voor termen die in het kader van cloud gebruikt worden zoals: IaaS, PaaS en SaaS. Heeft overlap met NIST SP 500-292.

3. **ISO/IEC 22123-2:** Information technology — Cloud computing — Part 2: Concepts

> Deze norm, getiteld "Deel 2: Concepten", heeft als doel het definiëren en specificeren van concepten die gebruikt worden op het gebied van Cloudcomputing. Het dient als een uitbreiding van de cloudcomputing vocabulaire die oorspronkelijk gedefinieerd werd in ISO/IEC 22123-1. Door deze concepten verder uit te werken, legt ISO/IEC 22123-2:2023 een fundament dat andere documenten en normen ondersteunt die geassocieerd zijn met cloudcomputing.

4. **ISO/IEC 22123-3:** Information technology — Cloud computing — Part 3: Reference architecture. Deze norm, getiteld "Deel 3: Referentiearchitectuur", specificeert de referentiearchitectuur voor cloudcomputing (CCRA). Dit document is van belang omdat het richtlijnen en standaarden vastlegt die betrekking hebben op de structuur en organisatie van systemen en diensten binnen de cloudcomputing omgeving. De referentiearchitectuur die in dit document wordt beschreven, biedt een gestructureerde en gedetailleerde blauwdruk voor het opzetten en beheren van cloudgebaseerde systemen, waardoor het een essentiële bron is voor professionals in het veld van cloudcomputing.

5. **NIST SP 800-154:** Het Nationale Instituut van Standaarden en Technologische definities van cloudcomputing, dat een duidelijk beknopt raamwerk biedt voor het begrijpen van cloudtechnologie.

6. **ETSI cloud standards:** De Europese Telecommunicatie Standaarden Instituut hanteert verschillende standaarden en specificaties voor clouddiensten, gericht op interoperabiliteit, veiligheid en SLA’s.

7. **ENISA Cloud Computing Risk Assessment**: De Cloudcomputing Risk Assessment van ENISA (European Union Agency for Cybersecurity) is een uitgebreid document dat de potentiële risico's evalueert die samenhangen met de adoptie van cloudcomputingdiensten.

8. **ISO/IEC 38500:** ISO 38500 is een internationale norm die richtlijnen biedt voor effectief corporate governance van informatie- en communicatietechnologie (ICT).

9. **FinOps-framework**: Het FinOps-framework is een reeks principes ontworpen om organisaties te helpen hun cloudkosten effectiever te beheren en te optimaliseren.

10. **ISO/IEC 19086**: ISO/IEC 19086 is een reeks internationale normen die richtlijnen en best practices biedt voor cloud service level agreements (SLA's). Deze normen helpen bij het definiëren, documenteren en overeenkomen van service level doelstellingen, metingen en verantwoordelijkheden tussen cloud service providers en hun klanten.

11. **ISO/IEC 19944:** ISO/IEC 19944 (Deel 1 en 2) is een internationale standaard die zich richt op cloudcomputing en distributed platforms, met speciale aandacht voor het vaststellen van een raamwerk voor data flow en data categorieën in de cloud. Deze norm biedt richtlijnen voor het classificeren van data, inclusief de oorsprong, beweging, en het gebruik ervan binnen cloud en gedistribueerde computing omgevingen. Het helpt organisaties bij het identificeren van de verschillende soorten data die in de cloud worden verwerkt, zoals gebruikersgegevens, operationele data en metadata, en geeft aanbevelingen voor het beheer en de behandeling van deze data, rekening houdend met zaken als privacy, beveiliging en compliance.

§ 4.5.1 Witte vlekken

Voor de algemene standaarden zijn geen witte vlekken gedefinieerd.

§ 5. Bijlage 1: Gebruikte bronnen bij het onderzoek

De volgende bronnen zijn gebruikt als input voor dit rapport:

- Handreiking risicobeheersing toepassing publieke clouddiensten
- Kamerbrief over rijksbreed cloudbeleid 2022
- Preparatory work in view of the procurement of an open source cloud-to-edge middleware platform (30 maart 2022)
- 20230322-bio-thema-uitwerking-clouddiensten-v22-def

- Cloud cybersecurity market analyses
- Study presenting assessments of codes of conduct on data porting and cloud switching
-
- Factsheet-verwerkersovereenkomst IBDHandreiking cloudcomputing
- Implementatiekader risicoafweging cloudgebruik
- Marktstudie clouddiensten door ACM
- The NIST Cloud Federation Reference Architecture
- Analyse cloud ontwikkelingen gemeenten
- Cloud governance whitepaper Microsoft (mei 2021)
- Cloud afwegingskader J&V versie 1.2 (juli 2021)
- Cloud services market study
- Cloud computing autorite de la concurrence Frankrijk
- Data Act
- Eindrapportage onderzoek Behoefte gemeentelijke cloudondersteuning VNG (26 april 2023)
- CSPCERT WG (Milestone 3) Recommendations for the implementation of the CSP certification scheme
- CSA STAR programme 2022

§ 6. Bijlage 2: De betrokken experts

Onderstaande experts zijn geïnterviewd tijdens het onderzoek. In de selectiecriteria is rekening gehouden met een representatie van experts vanuit diverse (overheids)organisaties en aanverwante organisaties die betrokken zijn bij het thema standaarden voor de cloud.

- Henrique Barnard Strategisch Leveranciersmanager Microsoft, Google Cloud en AWS rijksoverheid
- Frank van Dam Architectuur e-Government ICTU
- Edward van Gelderen Scrummaster Common Ground/Haven VNG
- Roderick Schaefer Adviseur en initiatiefnemer Haven VNG (inmiddels Binnenlandse Zaken)

- Peter Wiggers Kubernetes engineer VNG
- Mathijs Hoogland Kubernetes engineer VNG
- Sander Booij Enterprise architect IBM
- Michiel Steltman Managing director DINL
- Jacques Eding Portefeuillehouder Cloud, Adviseur CISO Rijk
- Artan van Hooijdonk Principal customer succes accountmanager Microsoft
- Benjamin Tissink Cloud Security Architect Microsoft
- Erwin van Essen Customer Succes Director Microsoft
- Jelle Niemantsverdriet National Security Officer Microsoft
- Linda Durand National Security Officer Microsoft
- Inge Piek Consultant ICT Standaarden NEN
- Edwin Harmsma Research consultant Cloud - TNO & Centre of Excellence for Data Sharing and Cloud
- Harro Kremer Enterprise Architect Ministerie van Justitie en Veiligheid
- Chris Eyzenga Technisch CISO Ministerie van Justitie en Veiligheid
- Ruben Faber Strategisch Adviseur Cyber Security NCSC
- Femke Nagelhoud Projectmanager en Senior Enforcement Official ACM
- Christiaan Waters Medewerker Toezicht
- Jacco Hakfoort Senior medewerker toezicht
- Pieter Bas Nederkoorn Productmanager GGI VNG
- Geeske Logtmeijer Implementatie Adviseur GGI
- Bas Huisman Technisch consultant Sociodome
- Linda Strick Director Cloud Security Alliance
- Ruud Kerssens Lead security expert EU Cybersecurity Certification

7. Bijlage 3: Aanpak en planning onderzoek

Wat	Activiteit	Resultaat	Wanneer
Voorbereiding	Gesprekken met opdrachtgever en adviseurs van deze voor afkadering Desk research Benaderen experts	Duidelijke focus en afkadering onderzoek	Juli/aug. 2023
Onderzoek	Individuele (online) gesprekken met meer dan 10 experts	Kennis, meningen en ideeën experts ophalen	Sept.-Nov. 2023
Analyse en opmaak conceptrapport	Analyseren en verwerken resultaten interviews en deskresearch	Beeld van de huidige stand van zaken	Nov. 2023
Toetsing en validatie	Delen conceptrapport met experts voor feedback	Verdieping op de resultaten, aanvullende inzichten en validatie door experts	Dec. 2023/jan 2024

8. Bijlage 4: Wat is cloud?

In deze bijlage een toelichting op de cloud. Waar is het cloudbeleid op gericht? De verschillende clouddiensten en cloudvarianten worden toegelicht, een toelichting van het toenemende belang van cloudcomputing en een opsomming van belangrijke cloudleveranciers.

8.1 Clouddiensten

Als referentiemodel voor de definities van cloudcomputing hanteren wij in dit rapport The NIST Definition of Cloud Computing. Deze referentie onderscheidt vijf essentiële karakteristieken van clouddiensten:

1. **On-Demand Self-Service**: Een afnemer van clouddiensten kan eenzijdig computercapaciteiten naar behoefte verkrijgen, zoals servertijd en netwerkopslag; automatisch zonder menselijke interactie met clouddienstverleners.

2. **Broad Network Access**: Functionaliteiten zijn via standaard mechanismen over netwerken beschikbaar voor verschillende type clients zoals: mobiele telefoons, tablets, laptops en werkstations.

3. **Resource Pooling**: De computerbronnen (zoals: opslag, verwerking, geheugen en netwerkbandbreedte) van de aanbieder kunnen worden verdeeld om meerdere afnemers te bedienen met behulp van een multi-tenant model, waarbij verschillende fysieke en virtuele bronnen dynamisch worden toegewezen op basis van de vraag van de afnemers. Er is een gevoel van locatieonafhankelijkheid in die zin dat de afnemer over het algemeen geen controle of kennis heeft over de exacte locatie van de geboden bronnen, maar wellicht de locatie op een hoger abstractieniveau kan specificeren (bijv. land, staat of datacenter).

4. **Rapid Elasticity**: Computerbronnen kunnen ‘elastisch’ worden geleverd en vrijgegeven, in sommige gevallen automatisch, om snel op en af te schalen. Voor de afnemers lijken de beschikbare computerbronnen vaak onbeperkt te zijn en kunnen op elk moment in elke hoeveelheid worden toegeëigend

5. **Measured Service**: Cloudsystemen meten en optimaliseren automatisch het gebruik van computerbronnen. Dit op een bepaald abstractieniveau (bijvoorbeeld opslag, verwerking, geheugen en netwerkbandbreedte). Het gebruik van computerbronnen kan worden gecontroleerd, beheerd en gerapporteerd, wat transparantie biedt voor zowel de aanbieder als de consument van de gebruikte dienst.

§ 8.2 Varianten van clouddiensten

NIST onderscheidt drie servicemodellen van clouddiensten. Deze verschillende servicemodellen worden afgenomen door overheidsorganisaties. 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, ontwikkeltools, toegangsbeheer,

identiteitenbeheer, portaalfunctionaliteiten en integratiefaciliteiten. 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, zoals: bijvoorbeeld kantoorapplicaties (bijv. Microsoft365), cliëntenbeheer (CRM, bijv. Salesforce), softwareontwikkeling (bijv. GitHub). 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.

Opmerking: in het komende EUCS (en ook ISO 22123) wordt de term ‘as a service’ vervangen door ‘Cloud Capability Types’, dus ‘Infrastructure Capability’, ‘Platform Capability’ en ‘Application Capability’. In dit rapport hanteren we de terminologie die op het moment van schrijven vigeerde.

Voor de overheid kunnen de drie modellen onder meer 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 ten behoeve van primaire processen en binnen kaders standaarden.

Tijdens het onderzoek gaven geïnterviewden aan dat er in de praktijk eigenlijk geen duidelijke splitsing is tussen IaaS en PaaS. De drie hyperscalers (Google, Microsoft en AWS) en de overige cloudleveranciers leveren een mix van deze twee dienstensoorten. Over het algemeen worden in een IaaS-omgeving via appstores allerlei aanvullende diensten geleverd, zoals: databasetoegang, AI-capaciteit en authenticatie en autorisatiediensten.

§ 8.3 Implementatievarianten van clouddiensten

NIST onderscheidt 4 typen implementatie van clouddiensten bij een cloudleverancier:

1. **Public**: De software en data staan dan volledig op de servers van de cloudprovider en er wordt een generieke (voor alle afnemers gelijke) functionaliteit geleverd.

2. **Gemeenschappelijk**: De cloudvoorziening is toegankelijk voor een beperkte groep afnemers, die elkaar onderling voldoende vertrouwen.

3. **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.

4. **Hybride**: een samenstelling uit meerdere van bovengenoemde implementatievarianten.

In het Cloud Cybersecurity Market Analysis van Enisas en andere achtergronddocumenten spreekt men ook de volgende implementatievariant, een variant die ook door de geïnterviewden werd genoemd: **multi-cloud.** Bij multi-cloud gaat het om een implementatievariant die net als de hybride-variant verschillende implementatievarianten combineert, en daarbij de implementatie van verschillende aanbieders combineert.

§ 8.4 Waarom Cloud?

Cloudcomputing biedt een scala aan voordelen voor zowel individuen als organisaties. Hier zijn enkele van de meest prominente voordelen:

1. **Kostenbesparing:** Door gebruik te maken van de cloud kunnen afnemers besparen op de kosten van aanschaf en onderhoud van hardware. Ze betalen vaak alleen voor wat ze daadwerkelijk gebruiken. De Marktstudie Clouddiensten van het ACM bevestigt dit beeld omdat grote datacenters duidelijke schaalvoordelen hebben en dus in staat zijn goedkoper diensten aan te bieden dan kleine datacenters.

2. **Schaalbaarheid en flexibiliteit:** Een van de grootste voordelen van cloudservices is de mogelijkheid om gemakkelijk en snel op te schalen naarmate de behoefte van een organisatie groeit op het gebied van volume voor het optimaal laten werken van digitale toepassingen, zonder dat er grote investeringen in fysieke hardware nodig zijn. Bovendien maakt de enorme rekenkracht van de cloudtoepassingen toegankelijk die deze rekenkracht vereist. Denk hierbij aan Artificial Intelligence (AI) met als bekendste toepassing ChatGPT.

3. **Toegankelijkheid en mobiliteit:** Gegevens en applicaties in de cloud kunnen vanaf elke locatie met internettoegang worden benaderd. Dit maakt telewerken en toegang onderweg gemakkelijker. Bovendien biedt het de mogelijkheid beter samen te werken, zoals bijvoorbeeld het gezamenlijk werken aan een document.

4. **Beveiliging en Compliance:** Hoewel beveiliging in de cloud een veelbesproken onderwerp is, bieden veel cloudproviders geavanceerde beveiligingsfuncties die bedrijven wellicht niet zelf zouden kunnen implementeren omdat kennis of andere middelen ontberen. Gerenommeerde cloudaanbieders bieden geavanceerde beveiligingsfuncties en kunnen helpen om te voldoen aan strenge regelgevingsnormen.

§ 8.5 Cloudleveranciers

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

De top-3 hyperscalers verdelen met elkaar het grootste deel van clouddiensten. De volgende hyperscalers zijn actief voor de Nederlandse overheid:

1. Amazon Web Services (AWS
2. Microsoft
3. Google Cloud

Naast bovengenoemde hyperscalers zijn de volgende bedrijven actief op de Nederlandse cloudmarkt:

1. IBM Cloud
2. Oracle Cloud
3. VMWare
4. Red Hat
5. OVHcloud

Naast bovengenoemde mondiale spelers zijn er op het gebied van cloud een aantal Nederlandse bedrijven te noemen:

1. KPN Cloud
2. TransIP
3. LeaseWeb
4. Interxion

Opvallend is dat de grote internationaal opererende cloudleveranciers bijna allemaal van Amerikaanse afkomst zijn met vestigingen in Europa, OVHCloud is de enige Europese speler. Nu de public cloud onder voorwaarden ook te gebruiken is door overheidsorganisaties neemt het marktaandeel van deze hyperscalers bij de overheid toe. De dreigende beperkte verdeling van de markt en de afkomst van de grote leveranciers buiten Europa, vereist regulering middels (Europese) wetgeving en onderliggende normen en standaarden.

9. Bijlage 5: Scope en uitgangspunten

Een belangrijk uitgangspunt voor het onderzoek is de brief van de Staatssecretaris van Huffelen van 29 augustus 2022 aan de Tweede Kamer, waarin zij een wijziging definieert ten opzichte van het tot dan toe geldende rijksbeleid van de overheid. In deze brief wordt geïnformeerd over het Rijksbrede cloudbeleid 2022. Dit beleid richt zich op het gebruik van public clouddiensten door de Rijksoverheid, als vervanging van het eerdere beleid uit 2011 dat de focus legde op private clouddiensten. De brief van de Staatssecretaris maakt het voor overheidsorganisaties mogelijk om gebruik te maken van de public cloud.

9.1 Hoofdpunten Rijksbreed Cloudbeleid 2022

Hoofdpunten van het cloudbeleid zoals gedefinieerd in de brief van de Staatssecretaris:

1. **Overheidsdiensten** mogen onder bepaalde voorwaarden en uitzonderingen gebruik maken van public clouddiensten. Onderdelen van de overheid die niet tot de Rijksdienst behoren wordt geadviseerd om dit Rijksbeleid te volgen.
2. **Verwerking van persoonsgegevens** in public clouddiensten vereist een goedgekeurde pre-scan gegevens-beschermingseffectbeoordeling. Bij een hoog risico is een volledige Data Protection Impact Assessment (DPIA) noodzakelijk.
3. Elk **departement** is zelf verantwoordelijk voor het inzicht in de risico's van het gebruik van public cloudtoepassingen.
4. Er komt een 'implementatierichtlijn risicoafweging cloudgebruik' voor het einde van 2022. Deze bestaat inmiddels, en is een implementatiekader geworden in plaats van een richtlijn.
5. **Uitzonderingen**: Public clouddiensten mogen niet worden gebruikt voor staatsgeheim gerubriceerde informatie. Het Ministerie van Defensie valt niet onder dit beleid.
6. **Voorwaarden**:
    - Departementen moeten hun eigen cloudbeleid formuleren.
    - Een relevante risicoafweging is vereist.
    - Jaarlijkse rapportage over het gebruik van public clouddiensten aan CIO Rijk.
    - Er moet een 'exit strategie' zijn in overeenkomsten met cloudleveranciers.

- Clouddienstverlening moet voldoen aan bestaande ICT-voorwaarden.
- Cyberveiligheid is essentieel, vooral met betrekking tot gegevensverwerking in andere landen. De overheid hanteert bij het cloudgebruik daarom ook de C2000 criteria, waardoor leveranciers of diensten uit landen met een actief cyberprogramma dat gericht is tegen Nederlandse belangen worden uitgesloten.
- Besluitvorming moet openbaar zijn volgens de Wet Open Overheid.
- Opslag en verwerking van persoonsgegevens moet in lijn zijn met de AVG.
- Extra bescherming is vereist voor bijzondere persoonsgegevens.
- In geval van de opslag en verwerking van een basisregistratie, of een bron van een basisregistratie wordt, in principe géén gebruik gemaakt van public cloudvoorzieningen.

De brief benadrukt het belang van een evenwichtige benadering, waarbij gebruik wordt gemaakt van de voordelen van public clouddiensten terwijl de risico's worden beheerst.

§ 9.2 Doelstellingen en uitgangspunten van het Forum voor het onderzoek

De onderzoeksvraag is geformuleerd door het Forum Standaardisatie. Het Forum Standaardisatie adviseert de publieke sector over het gebruik van open standaarden. Het Forum hanteert daarbij diverse doelstellingen en uitganspunten. Deze doelstellingen en uitgangspunten vormen de basis van dit onderzoek:

1. **Open standaarden**: Het Forum promoot het gebruik van open standaarden. Een open standaard is een specificatie die beschikbaar is en waarvan het gebruik niet beperkt is door patenten of licentierechten.
2. **Level playing field**: Door het gebruik van open standaarden wordt een gelijk speelveld gecreëerd voor aanbieders van ICT-producten en -diensten. Dit stimuleert innovatie en voorkomt dat overheidsorganisaties afhankelijk worden van één leverancier.
3. **Interoperabiliteit**: Eén van de belangrijkste doelstellingen van het Forum is het waarborgen van interoperabiliteit. Dit betekent dat verschillende diensten van verschillende cloudproviders probleemloos met elkaar kunnen communiceren en gegevens kunnen uitwisselen.

Cloudcomputing heeft een scala aan standaarden nodig om interoperabiliteit, veiligheid, privacy en portabiliteit te bevorderen. In het onderzoek wordt onderscheid gemaakt in de volgende soorten cloudstandaarden:

1. **Beveiligings- en privacystandaarden:** De beveiliginsstandaarden zorgen voor een veilige omgeving die niet toegankelijk is voor onbevoegden. De standaarden hebben betrekking op

aspecten zoals data-encryptie, authenticatie, autorisatie en auditlogboekregistratie. Privacystandaarden richten zich op de bescherming van persoonlijke gegevens die worden opgeslagen of verwerkt in de cloud. Hierbij kan gedacht worden aan standaarden die betrekking hebben op gegevensmaskering, anonimisering en pseudonimisering.

2. **Portabiliteitsstandaarden:** Deze standaarden maken het gemakkelijker om applicaties en gegevens van de ene cloudomgeving naar de andere te verplaatsen. Denk hierbij aan standaarden voor containerization.

3. **Interoperabiliteitsstandaarden:** Deze standaarden zorgen ervoor dat verschillende cloudservices en -componenten met elkaar op een gestandaardiseerde wijze kunnen communiceren en gegevens kunnen uitwisselen. Ze kunnen helpen bij het vermijden van vendor lockin en het ondersteunen van multi-cloudstrategieën.

4. **Overige standaarden:** Standaarden die niet passen in bovenstaande classificatie maar wel relevant zijn en daarom niet ongenoemd mogen blijven.

In het onderzoek onderscheiden we naast standaarden ook normen en technologieën die gelden als de facto-standaard:

- **Standaarden**: 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.

- **Technologieën** die als de facto-standaard opgevat kunnen worden. Hierbij gaat het niet om technische specificaties maar om werkende technische oplossingen die zo breed in de markt worden toegepast dat ze als standaard opgevat kunnen worden.

In hoofdstuk 4 wordt per soort cloudstandaard een opsomming gegeven van bestaande of standaarden die worden ontwikkeld. Indien mogelijk worden ‘witte vlekken’ beschreven.

§ 10. Bijlage 6: Cloudontwikkelingen en trends

Cloudcomputing heeft de manier waarop bedrijven, overheden en individuen technologie gebruiken en benaderen getransformeerd. Dit dynamische topic blijft evolueren met nieuwe innovaties, gebruikspatronen en businessmodellen. In dit hoofdstuk een overzicht van de mondiale trends op het gebied van cloudcomputing. Daarnaast een opsomming van cloudontwikkelingen in Europa en in Nederland.

§ 10.1 Mondiale trends

Hier onder een overzicht van de belangrijkste mondiale trends in cloudcomputing:

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 en benodigde diensten. Deze onderliggende infrastructuur en benodigde diensten worden geboden door clouddiensten Dit leidt tot snellere ontwikkeling en kan kosten verminderen.

3. **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. Hier zijn alle hyperscalers mee bezig én er wordt veel van verwacht gezien de investeringen die deze partijen nu doen.

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

5. **Containers en Orkestratie**: Ontwikkeling op basis van 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 wat de portabiliteit vergroot.

6. **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.

7. **Data-soevereiniteit en lokale Regulaties**: Met strengere gegevensbeschermingswetten in verschillende landen en regio's werken cloudproviders aan regionale datacenters en het aanbieden van specifieke oplossingen om aan de regelgeving te voldoen.

De mondiale trends in cloudcomputing zijn een reflectie van het snel veranderende technologische landschap en de behoeften van organisaties en individuen. Terwijl cloudcomputing blijft evolueren, zullen de fundamentele principes van flexibiliteit, schaalbaarheid en on-demand toegang de drijvende krachten achter deze transformatie blijven.

§ 10.2 Europese ontwikkelingen

We hebben eerder vastgesteld dat de cloud ons veel voordelen gaat bieden. Om te zorgen voor een gecontroleerde ontwikkeling conform de normen en waarden die gelden in de Europese samenleving is het van belang om passende maatregelen te nemen. Deze maatregelen moeten leiden tot passende wet en regelgeving met daarin een verwijzing naar de verplichte toepassing van open standaarden door cloudleveranciers.

De EU ziet wetgeving en standaardisatie als een strategisch instrument om de markt voor clouddiensten gezonder en veiliger te maken. Acties voor cloudcomputing in het Rolling Plan 2022:

> "Action 1 - Identify needs for ICT standards and open source technologies to further improve the interoperability, data protection and portability of cloud services and continue or start respective development activities…
>
> Action 2 - Promote the use of the ICT standards needed to further improve the interoperability, data protection and portability of cloud services as well as multi-cloud management."

Hieronder een opsomming van interessante Europese ontwikkelingen die van invloed zijn op de manier waarop gegevens worden opgeslagen, verwerkt en gedeeld op Europees niveau en die van invloed zijn op de vormgeving van clouddiensten:

1. **Data Governance Act:** Op 24 september 2023 is de Data Governance ACT in werking getreden. De verordening creëert een nieuwe Europese manier van data governance, gebaseerd op een toenemend vertrouwen in het delen van data. Het heeft tot doel een veilige omgeving te creëren voor het delen van gegevens tussen sectoren en lidstaten, ten behoeve van de samenleving en de economie. Deze strategie heeft directe implicaties voor cloudcomputing, 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. **Data Act:** Deze Europese Verordening verplicht aanbieders van clouddiensten om het voor gebruikers mogelijk te maken om gemakkelijk over te stappen naar een andere aanbieder zonder verlies van gegevens en functionaliteit (portabiliteit). De Verordening schrijft geen specifieke standaarden voor die aanbieders hiervoor moeten gebruiken; wel worden een aantal functionele eisen gedefinieerd waaraan zijn moeten voldoen. Naast de verplichting om portabiliteit mogelijk te maken, moeten aanbieders van clouddiensten ook interoperabiliteit mogelijk maken; dat wil zeggen dat gebruikers ervoor moeten kunnen kiezen om zonder problemen parallel gebruik te maken van twee of meer aanbieders van clouddiensten. Op het laatste punt heeft de ACM ook aangedrongen, naar aanleiding van de bevindingen die zij heeft

opgedaan in de marktstudie naar clouddiensten. Hoewel de Data Act geen specifieke standaarden voorschrijft voor portabiliteit en interoperabiliteit, biedt de Data Act wel de mogelijkheid dat de Europese Commissie dergelijke standaarden in de toekomst alsnog opstelt in de vorm van gedelegeerde wetgeving. Het Europees Parlement en de Europese raad hebben de Data Act inmiddels aangenomen. Daarna kan de Data Act gepubliceerd worden. Vanaf het moment van publicatie duurt het dan nog twintig maanden voor de Data Act van toepassing wordt. Dat is dus in het najaar van 2025.. Een Europese focus groep gaat beoordelen welke kaders en voorzieningen moeten worden ontwikkeld om de lidstaten te ondersteunen bij de invulling van de Data Act. De groep gaat zich o.a. richten op open standaarden en data spaces.

3. **GAIA-X**: Dit initiatief, voornamelijk aangestuurd door Duitsland en Frankrijk, streeft of streefde 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. GAIA-x lijkt de doelstelling om te komen tot een concurrerend cloudaanbod te hebben verschoven naar het gezamenlijk ontwikkelen van een digitale governance laag die (overheids)organisaties in staat stelt grip te houden op de public cloudvoorzieningen, waarbij de interactie tussen cloudvoorzieningen en de migratie van een cloudplatform naar een ander cloudplatform eenvoudiger wordt. Grip betekent ook het voldoen aan allerlei beveiligingsstandaarden. Diverse experts zijn kritisch over de resultaten die tot nu toe zijn gerealiseerd vanuit GAIA-x. De Nederlandse overheid moet de ontwikkelingen rondom GAIA-X nauwlettend volgen, gezien de potentiële implicaties voor interoperabiliteit en data-soevereiniteit.

4. **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.

5. **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 clouddiensten.

6. **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 cloudsector, wat relevant is voor de Nederlandse overheid bij het selecteren van cloud partners.

7. **Europese Cybersecurity Act**: Ingesteld in 2019, deze wet introduceert een EU-breed kader voor cybersecurity-certificering. Het is een framework met toetsbare criteria. Diverse organisaties zijn gemandateerd om te certificeren. De certificering kent verschillende niveau’s. Onderdeel van de Europese Cybersecurity Act is de NIS2 (opvolger van de NIS1). Net als de Europese GDPR voor privacywetgeving wordt de Europese NIS2 ook verplichte wetgeving.

De GDPR is in Nederland de AVG geworden, de NIS2 heeft ook een Nederlandse naam, de NIB2 (Netwerk- en Informatiebeveiligingsrichtlijn). Deze zal als Nederlandse wetgeving in de tweede helft (september) van 2024 geïmplementeerd moeten zijn (21 maanden na goedkeuring). Overigens geldt dit voor alle 27 Europese lidstaten. De NIS2 moet de cyberweerbaarheid versterken door het beveiligingsniveau te verhogen en het nemen van “basismaatregelen” afdwingen om cyberaanvallen te voorkomen en de impact ervan te verkleinen. Als de Nederlandse overheid gebruik maakt van clouddiensten, is het belangrijk te waarborgen dat deze diensten voldoen aan de Europese cybersecurity-normen en aan de Nederlandse versie van de NIS2.

8. **European cloud rulebook:** Om Europese bedrijven en publieke organisaties, die in toenemende mate afhankelijk zijn van cloudtechnologieën, te beschermen, is het belangrijk dat cloud- en edgediensten die in Europa worden aangeboden volledig voldoen aan de relevante (algemene en sectorale) wetten, maar ook aan de belangrijkste Europese zelfregulerende normen en standaarden met betrekking tot veiligheid, energie-efficiëntie, gegevensbescherming, interoperabiliteit en eerlijke concurrentie. De afgelopen jaren hebben belanghebbenden uit de sector in Europa samengewerkt om dergelijke zelfregulerende normen en standaarden te ontwikkelen. Het komende EU Cloud Rulebook zal een uitgebreide catalogus van dergelijke regelingen bieden en de mechanismen beschrijven om de naleving ervan aan te tonen.

9. **Simpl-project:** Met het Smart Middleware Platform (Simpl) kunnen EU-belanghebbenden middelen bundelen om meer bedrijfswaarde en efficiënt gebruik van hulpbronnen te creëren, de kosten te verlagen en dubbel te vermijden. Deze middleware vergemakkelijkt de verbinding tussen geïsoleerde datacentra en EU-actoren die kunnen profiteren van onderbenutte infrastructuur. Ook zal deze databronnen openstellen voor publieke instellingen, kmo's, organisaties en de industrie om de dienstverlening in het algemeen publiek belang te verbeteren. De middleware kan worden benut in de ambitie van de commissie om een open marktplaats voor EU-middelen te creëren, wat leidt tot efficiënt hergebruik van inspanningen van andere EU-partijen. In lijn met de Europese Green Deal zal het Smart Middleware Platform gebaseerd zijn op energiezuinige software. De diensten zijn ook gericht op het optimaliseren van het energieverbruik in alle sectoren**.**

10. **DOME-marketplace:** DOME is een ecosysteem dat alle belanghebbenden van Cloud & Edge-diensten verenigt, inclusief infrastructuur- en platformaanbieders, dienstenintegrators, certificeringsbureaus en klanten uit elke sector. Het doel is om de huidige praktijken te vereenvoudigen en een continuüm van gebundelde diensten aan te bieden die de nationale grenzen overschrijden.

De ontwikkelingen en uitdagingen op het gebied van cloudcomputing zijn groot. Te groot voor een land als Nederland alleen. Het is daarom essentieel voor de Nederlandse overheid om op de hoogte te blijven en bij te dragen aan de ontwikkelingen op Europees niveau. Door proactief te zijn en een weloverwogen benadering van cloudadoptie te handhaven en op Europees niveau gezamenlijk op te

trekken, kan Nederland bijdragen aan een veilige, efficiënte en conform de regelgeving functionerende cloudinfrastructuur voor zijn burgers en instellingen.

§ 10.3 Cloudontwikkelingen binnen de Nederlandse Overheid

De cloudtransitie heeft zich wereldwijd volop ingezet, ook bijde Nederlandse. De Nederlandse overheid realiseert zich dat ze bij het stellen van voorwaarden aan het gebruik van de cloud moet optrekken met de Europese bondgenoten, vallend onder de paraplu van de Europese Unie.

Nederland levert de nodige kennis en inbreng bij diverse eerder toegelichte Europese ontwikkelingen. Naast deze inbreng in Europa heeft de Nederlandse overheid verschillende cloudinitiatieven ontplooid. Hier volgt een overzicht van de belangrijkste cloudontwikkelingen binnen de Nederlandse overheid:

1. **Gebruik van de public cloud onder bepaalde voorwaarden:** Aangezien de cloud veel voordelen biedt en de publiccloud met de opkomst van onder andere AI, waar de benodigde rekenkracht alleen te verkrijgen is middels gebruik van de public cloud, heeft de Nederlandse overheid het gebruik hiervan mogelijk gemaakt onder strikte voorwaarden. De Kamerbrief Rijksbreed cloudbeleid 2022 van Staatssecretaris van Huffelen beschrijft de voorwaarden en is een opmaat tot gecontroleerd gebruik van de public cloudvoorzieningen.

2. **Handreiking risicobeheersing toepassing publieke clouddiensten:** In 2022 is het cloudbeleid, en het ‘Implementatiekader risicoafweging cloudgebruik’ vastgesteld. Daarin zijn de kaders bepaald voor public en hybride cloudgebruik. De handreiking is bedoeld voor specialisten in projectteams, opdrachtgevers (CIO’s) en specifieke functionarissen (CISO, CPO) die aan de slag gaan met een traject waarbij public cloudgebruik een rol speelt. Daarnaast krijgen opdrachtgevers beter inzicht op het beheersen van risico’s van public cloudgebruik. Het cloudbeleid en het implementatiekader zijn verplicht voor de Rijksdienst voor materieel gebruik van de public cloud.

3. **Strategisch leveranciersmanagement (SLM):** Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services is sinds 2014 initiatiefnemer van rijksbrede contractafspraken en inkoopvoorwaarden voor software en clouddienstverlening met genoemde partijen. Taken o.a.: Overheidsinstellingen adviseren bij de aanschaf van software en cloudproducten en -diensten. Het evalueren van de risico’s van cloudproducten en -diensten voor onder meer het naleven van privacywetgeving (AVG/GDPR). Het organiseren van nationale en internationale netwerken van inkopers en contractmanagers van cloudproducten en -diensten. Het afsluiten van contracten namens de Nederlandse overheid een overeenkomst tussen de Rijksoverheid en de hyperscalers om te komen tot passende voorwaarden, zoals AVG en BIO compliancy.

4. **Common ground-Haven:** Iedere gemeente heeft zijn IT-infrastructuur anders georganiseerd. Bij de ene gemeente draait bijvoorbeeld veel lokaal en bij de ander juist meer in de cloud. Applicaties moeten worden aangepast aan de infrastructuur waarop ze draaien. Dat maakt het voor gemeenten lastig om samen applicaties te ontwikkelen en deze snel in te zetten bij alle gemeenten. Haven is een standaard voor platform-onafhankelijke cloud hosting. Met Haven kunnen gemeenten applicaties overal hosten zonder dat zij daarvoor hun IT infrastructuur hoeven aan te passen. Dit zorgt onder meer voor uniformiteit, lagere kosten en minder afhankelijkheid van leveranciers. Haven schrijft een specifieke configuratie van Kubernetes voor die dient te worden geïmplementeerd op bestaande technische infrastructuur, bijvoorbeeld een cloud of on-premise platform. De voorgeschreven configuratie zorgt ervoor dat iedere Haven omgeving van iedere willekeurige cloudleverancier die de standaard heeft geïmplementeerd, functioneel gelijk is ongeacht de onderliggende technische infrastructuur. Zie het als een abstractielaag die resulteert in een gezamenlijk vertrekpunt. Dit brengt diverse voordelen met zich mee: uniformiteit in technische infrastructuur, uitwisselbaarheid van toepassingen, leveranciersonafhankelijkheid, platformonafhankelijkheid en kostenreductie. Haven heeft een eigen compliancy voorziening.

5. **Baseline Microsoft 365:** Steeds meer overheidsorganisaties maken gebruik van clouddiensten. Een bekend voorbeeld van een clouddienst is Microsoft Office 365. Ook binnen de overheid neemt het gebruik van deze clouddienst toe. Departementaal vertrouwelijke informatie van het niveau BBN2 mag alleen naar de cloud als voldaan is aan hogere eisen en maatregelen zoals versleuteling. Het moet voldoen aan bijvoorbeeld de AVG, het Voorschrift Informatiebeveiliging Rijk Bijzondere Informatie en diverse normen en standaarden zoals de Baseline Informatiebeveiliging Overheid. Vanwege het steeds groter wordende gebruik van de clouddienst Office 365 werkt de Nederlandse Overheid samen met Microsoft aan de Baseline voor de Microsoft suite.

Tenslotte heeft de NORA organisatie een beslisboom voor risicobeoordeling Clouddiensten als onderdeel van het BIO thema Clouddiensten. Daarnaast onderhoudt de NORA organisatie een Wiki over cloudcomputing. Hier staan vooralsnog oudere artikelen over Cloud, en de NORA organisatie is nog op zoek naar een expertgroep die deze Wiki actueel kan houden.

§ 11. Bijlage 7: Risico’s van de toepassing van cloud en clouddiensten

Hoewel cloudcomputing veel voordelen biedt, zijn er ook verschillende risico's en uitdagingen waarmee (overheids)organisaties en individuen rekening moeten houden. Vragen over dataprivacy, beveiliging en de integratie met bestaande systemen, maar ook de toenemende marktpositie en daarmee de macht van de hyperscalers zijn ontwikkelingen die in de gaten moeten worden gehouden. Een mogelijkheid hiertoe is de toepassing van wetgeving, normen en standaarden.

In het onderzoek kwamen de volgende uitdagingen en risico’s naar voren:

1. **Vendor-lockin:** de cloudmarkt heeft een groot risico op vendor-lockin. Als eenmaal voor een cloudleverancier is gekozen dan zijn er grote drempels om over te stappen naar een ander leverancier. Het grote risico op vendor lockin lijkt groter dan bij traditionele on-premise oplossingen en heeft de volgende oorzaken:

1. Clouddiensten worden binnen de overheid aanbesteed, waarna er één dienst overblijft en men zich daarop volledig richt. Een dergelijke aanbesteding kost veel tijd en moeite. Dit wordt nader onderbouwd in de Marktstudie clouddiensten door ACM:
   "Wanneer een gebruiker eenmaal heeft gekozen voor een specifieke clouddienst is de drempel om voor die dienst over te stappen naar een andere cloudaanbieder in veel gevallen zeer hoog. Uit de gesprekken die de ACM voor deze studie heeft gevoerd, komt het beeld naar voren dat er weinig overstap plaatsvindt tussen clouddiensten van verschillende cloudaanbieders. In het bijzonder gebruikers van PaaS- en SaaS-diensten kunnen moeilijkheden ervaren bij het overstappen. Voor gebruikers van IaaS-diensten geldt dit in iets mindere mate."

2. Clouddiensten en met name de hyperscalers bieden allerlei makkelijk toegankelijke proprietary diensten aan. Andere cloudaanbieders hebben andere proprietary diensten die moeilijk overdraagbaar zijn van de ene cloudleverancier naar de andere. Met name de proprietary diensten, maken een overstap lastig. Een voorbeeld is Office 365 van Microsoft. Eenmaal in gebruik genomen beperken die de mogelijkheden tot een overstap naar een andere cloudleverancier. Ook dit punt wordt bevestigd door de Marktstudie clouddiensten door ACM:
   "De lock-in van afnemers geldt in het bijzonder wanneer er ook PaaS- en SaaS-diensten worden afgenomen in een geïntegreerd dienstenaanbod. Overstappen is bij ICT-producten en diensten – die in de praktijk vaak sterk verweven zijn met de processen binnen de organisatie – complex. Dat geldt voor geïntegreerde clouddiensten des te meer omdat er in veel gevallen opnieuw koppelingen moeten worden gemaakt en een overstap op meerdere diensten tegelijkertijd noodzakelijk is"

3. Kosten van outbound data zijn veel hoger dan inbound. Het is dus goedkoop om data bij een cloudleverancier neer te zetten, maar de data verplaatsen naar een andere plek is duur. Dit kan organisatie ervan weerhouden om over te stappen naar een andere cloudleverancier. Dat zorgt voor onvoorspelbaarheid over de uiteindelijke totale kosten van gebruik van clouddiensten en de eventuele te realiseren besparingen als gevolg van een eventuele overstap. Vanuit de Data Act wordt beoogd dit tegen te gaan. Dit juist om switchen van de ene naar de andere provider niet te laten verhinderen door hoge kosten voor verplaatsen van data.

2. **"Winner takes all"-markt:** "Winner takes all" refereert aan een economisch principe waar de best performende platformen in staat zijn een hele markt of een zeer groot deel van een markt in handen te krijgen. De cloudmarkt heeft duidelijke kenmerken van een 'Winner takes all'-markt. Dit wordt bevestigd door de Engelse Cloud Services market study report:
   "There are two leading providers of cloud infrastructure services in the UK: Amazon Web Services (AWS) and Microsoft, who had a combined market share of 70% to 80% in 2022.2 Google is their closest competitor with a share of 5% to 10%."

> Er is geen reden aan te nemen dat deze situatie voor de Nederlandse markt anders is dan dat in dit rapport wordt aangegeven. Ook wordt dit beeld van consolidatie bevestigd in de Marktstudie clouddiensten door ACM. In dit rapport worden de mechanismen van deze consolidatie verder beschreven.

3. **Kosten moeilijk te voorspellen:** Terwijl initieel cloudservices kostenbesparingen kunnen opleveren, kunnen onverwachte kosten optreden bij verhoogd gebruik, met name als organisaties niet zorgvuldig hun verbruik monitoren. Uit het onderzoek komt naar voren dat de prijsstelling van clouddiensten vooraf vaak erg moeilijk is in te schatten. De prijsstructuur is vaak zeer complex opgezet waardoor deze moeilijk voorspelbaar is. Een van de geïnterviewden gaf aan dat cloudkosten vaak alleen empirisch te bepalen zijn, dus achteraf. Naast technisch/organisatorische zijn er ook financiële overstapbelemmeringen. Deze ontstaan met name door de tariefstructuur die veel cloudaanbieders hanteren. Deze tariefstructuur is complex: voor elke handeling, opgeslagen GB of seconde rekenkracht wordt betaald.

4. **Beveiligingsrisico's:** De data van een organisatie bevindt zich buiten de directe controle van die organisatie, wat kan leiden tot zorgen over datalekken, hackpogingen en andere cyberbeveiligingsbedreigingen. Clouddiensten kunnen potentieel veiliger worden ingericht dan bestaande on-premise-diensten doordat deze vaak meer geavanceerde beveiligingsmaatregelen kunnen nemen. Het inrichten van een cloudomgeving vergt wel specifieke kennis en ervaring met het betreffende cloudplatform. Juist hier schuilt de zorg van veel geïnterviewden. Deze kennis is schaars en dat introduceert onder andere beveiligingsrisico's.

5. **Risico's rond privacy van gegevens:** De opslag van gevoelige gegevens in de cloud kan leiden tot privacy zorgen, vooral als de cloudprovider gegevens opslaat in een ander rechtsgebied met andere privacywetten. Naast opslag van gevoelige gegevens gaat het ook om toegang tot de gegevens van buiten de EU, gebruik van telemetrie data etc. Zie ook de Handreiking risicobeheersing public clouddiensten - Rijksportaal (overheid-i.nl)

6. **Risico's rond gegevenseigendom en -toegang:** Dit risico geldt met name bij SaaS-diensten. Daar waar een dienst wordt afgenomen en de afnemer niet meer zelf direct toegang tot de gegevens heeft. Veelal betreft het diensten die eerder on-premise werden afgenomen, zoals een gemeentelijk vergunningensysteem of een gemeentelijke applicatie voor burgerzaken. Deze applicaties verschuiven steeds meer van on-premise naar clouddiensten. Hierna heeft de afnemer veelal niet direct toegang meer tot de gegevens omdat deze niet meer op de infrastructuur van de afnemer staat, en dienen daar aanvullende afspraken voor gemaakt te worden.

7. **Onvoldoende kennis en expertise**: Geïnterviewden geven aan dat deze op dit moment onvoldoende aanwezig bij de overheid en daardoor de overheid achter de feiten aanloopt. Inrichting van een cloudomgeving is vaak erg complex en vergt aanvullende kennis en ervaring boven on-premise-inrichting. Deze blijkt schaars bij de Nederlandse overheid.

Bovendien vergt het kennis van de omgeving van de verschillende cloudaanbieders, zo vergt inrichting van Microsoft Azure andere kennis dan de inrichting van Amazon Web Services.

Uit het onderzoek blijkt dat overheden veelal los van elkaar kennis opbouwen, en er met samenwerking te verbeteren valt.

§ 12. 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

↕