



Ministerie van Justitie en Veiligheid
Ministerie van Asiel en Migratie

Bestuurlijke Beleidslijn Cloud
Ministerie van Justitie en Veiligheid
Ministerie van Asiel en Migratie

“Op gecontroleerde, veilige en zorgvuldige wijze de publieke cloud in”

Inhoud

1	Achtergrond en aanleiding.....	3
1.1	<i>Aanleiding Bestuurlijke Beleidslijn Cloud JenV AenM</i>	3
1.2	<i>Aanpassing Rijksbreed Cloudbeleid.....</i>	3
1.3	<i>Het belang van publieke clouddiensten voor JenV AenM.....</i>	4
1.4	<i>Digitale onafhankelijkheid</i>	4
2.	Beleidskader	5
2.1	<i>Beleidskader Overheid</i>	5
2.2	<i>Beleidslijn JenV AenM.....</i>	5
2.2.1	<i>Beleidslijn gebruik Cloud Service Providers.....</i>	6
2.2.2	<i>Beleidslijn gebruik MS365 werkplek.....</i>	6
2.2.3	<i>Beleidslijn gebruik MS Teams</i>	7
2.2.4	<i>Beleidslijn gebruik Exchange</i>	7
2.2.5	<i>Beleidslijn gebruik One-Drive On-line Sharepoint On-line</i>	7

1 Achtergrond en aanleiding

1.1 Aanleiding Bestuurlijke Beleidslijn Cloud JenV | AenM

In de afgelopen periode vindt er veel discussie plaats rond het gebruik van Publieke Cloud voorzieningen. Dit naar aanleiding van verschuivingen in de huidige geopolitieke verhoudingen, als ook door recente rapporten van de Algemene Rekenkamer “Rijk in de Cloud” en de initiatiefnota “Wolken aan de Horizon” van de kamerleden Kathmann en Six Dijkstra. Recent is eveneens het plenaire Kamerdebat Cloud gevoerd (13 maart 2025).

Op basis van het Kamerdebat Cloud heeft de Tweede Kamer de volgende moties aangenomen:

- Stoppen met onnodige ICT-migraties naar Amerikaanse Techgiganten; (ontraden)
- Aanbesteding voor een Rijkscloud in volledig Nederlands beheer; (ontraden)
- Het .nl domein weer volledig in Nederland krijgen;
- Risicoanalyse en Exit-strategie voor clouddiensten van Amerikaanse Techgiganten;
- In EU-verband pleiten voor versnelde investeringen in Cloudinitiatieven;
- Doelstelling hanteren dat de continuïteit van de Nederlandse overheid niet rechtstreeks afhankelijk is van partijen uit de VS; (ontraden)
- Europese bedrijven op één te zetten bij aanbestedingen van vitale ICT-diensten door middel van soevereiniteitseisen voor de opslag van gevoelige gegevens en vitale infrastructuur; (ontraden)
- Alternatieven ontwikkelen voor de grote Amerikaanse techbedrijven voor de ICT-infrastructuur van de overheid.

7 april jl. is middels de Kamerbrief¹ ‘uitvoering ontraden aangenomen moties debat migraties overheids-ICT naar het buitenland’ de kamer geïnformeerd door Staatssecretaris Szabó (Digitalisering en Koninkrijksrelaties) hoe hij de 3 aangenomen moties uitvoert die hij tijdens het plenaire debat op 13 maart 2025 had ontraden.

1.2 Aanpassing Rijksbreed Cloudbeleid

Het vastgestelde Rijksbreed Cloudbeleid in de Ministerraad van 29-8-2022 wordt momenteel herzien. De verwachting is dat met name op de punten van uitvoeren van Risico Analyses en creëren van uitvoerbare Exit strategieën deze zal worden aangescherpt. Dit ook naar aanleiding van de volgende aanbevelingen uit het rapport van de Algemene Rekenkamer;

Hoofdaanbeveling aan alle ministers:

Om soevereine, continue en veilige overheidsdienstverlening te borgen is het zaak dat het Rijk richting de grote clouddienstverleners als één samenwerkende overheid kaders stelt, regels hanteert, risico's mitigeert en zijn positie ten opzichte van leveranciers en andere gebruikers van de cloud versterkt. Hiervoor is het nodig dat het Rijk beter zicht heeft op het eigen cloudgebruik en veel gerichter kansen, risico's en alternatieven afweegt voorafgaand aan, maar ook tijdens cloudgebruik.

¹ [Brief - Plan van aanpak ontraden aangenomen moties debat migraties overheids-ICT naar het buitenland](#)

Aan de minister van BZK:

1. Maak het Rijksbreed cloudbeleid uniformer en concreter, en houd hier toezicht op.
2. Richt de handhaving van het Rijksbreed cloudbeleid beter in.
3. Zie bij alle ministeries toe op het verbeteren van het zicht op gebruikte clouddiensten en het alsnog maken van risicoafwegingen voor materieel public clouddiensten.

Aan alle ministers:

1. Overweeg als Rijk realistische EU-alternatieven in combinatie met een uitvoerbare exitstrategie.
2. Actualiseer risicoafwegingen van reeds gecontracteerde clouddiensten. De afweging moet in ieder geval ingaan op de principes soevereiniteit, continuïteit van dienstverlening en gegevensbescherming.
3. Verbeter het zicht op gebruikte clouddiensten.

1.3 Het belang van publieke clouddiensten voor JenV | AenM

Het belang van het inzetten van publieke clouddiensten als aanjager van nieuwe technologieën is door deze adviezen en geopolitieke verschuivingen niet veranderd. Deze liggen op het vlak van data-analyse, de inzet van Artificiële Intelligentie (AI), en inzet van (nieuwe) toepassingen die enkel nog in de cloud worden aangeboden. Hierbij gaat het niet alleen om innovatieve technologieën, maar ook om bestaande applicaties die steeds vaker enkel nog worden aangeboden als clouddienst.

1.4 Digitale onafhankelijkheid

Met de inzet van publieke clouddiensten ontstaan relaties met publieke IT-dienstenleveranciers van buiten het (Rijks)overheidsdomein. Dergelijke afhankelijkheden moeten worden beoordeeld met betrekking tot aandachtspunten om bedreigingen van de digitale soevereiniteit van JenV | AenM uit te sluiten of op zijn minst te beperken. Digitale soevereiniteit en data-autonomie dienen ook in de publieke cloud te worden gewaarborgd. De huidige ontwikkelingen vergroten de noodzaak om de onafhankelijkheid van grote cloud leveranciers te behouden en te versterken. Door de toenemende concentratie van ICT-leveranciers op de markt zullen dergelijke afhankelijkheden nog verder worden vergroot.

Digitale soevereiniteit wordt door JenV | AenM als volgt gedefinieerd:

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

2. Beleidskader

2.1 Beleidskader Overheid

Vanuit CIO-Rijk wordt momenteel hard gewerkt aan het opstellen van de volgende documenten.

- Visie Digitale autonomie en soevereiniteit Overheid
- Beleidskader Digitale autonomie en soevereiniteit Overheid
- Operationeel afwegingskader Digitale autonomie en soevereiniteit Overheid

De verwachting is dat deze stukken voor het zomerreces aan de Tweede Kamer worden aangeboden. In het concept beleidskader is o.a. het volgende opgenomen:

*“**Strategische afhankelijkheden beheren:** hoewel sommige afhankelijkheden onvermijdelijk zijn, kan de overheid deze beheersen door duidelijke randvoorwaarden en principes te hanteren, zoals het voorkomen van vendor lock-in en het stimuleren van interoperabiliteit tussen systemen.*

In lijn met de Agenda Digitale Open Strategische Autonomie (DOSA) benadrukt digitale autonomie het belang van Europese samenwerking. De overheid werkt toe naar een situatie waarin zij gefaseerd meer zelfstandigheid bereikt, terwijl zij tegelijkertijd haar internationale partnerschappen benut om veerkrachtige digitale oplossingen te realiseren.

Het beleidskader is gebaseerd op drie leidende principes en vier strategische bouwstenen:

Leidende principes:

1. **Autonomie:** Zelfbeschikking en onafhankelijkheid bij strategische keuzes
2. **Soevereiniteit:** Juridische en operationele controle over technologieën, systemen en data
3. **Weerbaarheid:** Vermogen om te anticiperen op risico's en veerkrachtig te reageren op dreigingen

Strategische bouwstenen:

1. **Innovatie:** Katalysator voor vooruitgang en technologische onafhankelijkheid
2. **Datasoevereiniteit:** Grip op informatie en processen binnen Europese jurisdictie
3. **Samenwerking:** Kracht door verbinding binnen Nederland en Europa
4. **Waardegedreven:** Technologie in dienst van publieke waarden”

2.2 Beleidslijn JenV | AenM

Naar aanleiding van bovenstaande ontwikkelingen en het feit dat er op korte termijn een aanscherping komt van het ‘Rijksbreed Cloudbeleid’ en het opstellen van het ‘Beleidskader Digitale autonomie en soevereiniteit’, hanteert JenV | AenM de volgende Cloud beleidslijn. **Deze (tijdelijke) beleidslijn blijft van kracht tot er meer duidelijkheid is in het Rijksbreed cloudbeleid en Beleidskader Digitale autonomie en soevereiniteit.**

2.2.1 Beleidslijn gebruik Cloud Service Providers

Het gebruik van publieke Cloud Service Providers voor het gebruik van IAAS-, PAAS- en SAAS-diensten blijft toegestaan. Wel dienen hiervoor zoals het huidige 'Rijksbreed Cloudbeleid' voorschrijft per dienst een gedegen risicoanalyse te worden uitgevoerd als ook een Exit strategie te worden opgesteld.

Artikel 4 - Risicoafweging

Publieke clouddiensten mogen worden gebruikt op basis van een in een gegevensbeschermingseffectbeoordeling opgenomen relevante risicoafweging, conform de implementatierichtlijn opgenomen in Implementatiekader risicoafweging cloudgebruik.

Artikel 7 - Exit-strategie

Een exit-strategie in het kader van het cloudbeleid borgt de continuïteit van bedrijfsprocessen en het opruimen van data bij beëindiging van de dienstverlening. De borging gaat zowel via maatregelen voor de eigen organisatie, waaronder budget, als via contractuele afspraken met de leverancier. Onderdelen in de exit-strategie zijn:

- 1. Voorwaarden aan de leverancier (en toeleveranciers) met aandacht voor dataportabiliteit, serviceportabiliteit en datavernietiging inclusief de processen en voorzieningen die daarvoor nodig zijn;*
- 2. Een alternatieve leverancier of interne landingsplaats;*
- 3. Een strategie, voorwaarden en budget, voor direct vertrek in verband met een crisis of plotselinge (geopolitieke) ontwikkelingen; en*
- 4. Een strategie en budget bij de reguliere afloop van de overeenkomst.*

Bij het gebruik van Cloud Service Providers (CSP) is het advies om op het gebied van security architectuur, CSP onafhankelijke producten de voorkeur te geven boven de CSP eigen security producten, dit om vendor lockin te voorkomen.

2.2.2 Beleidslijn gebruik MS365 werkplek

Veel van het parlementaire debat gaat over het gebruik van de Microsoft365 werkplek en het 'verplaatsen' van overheidsinformatie van on-prem. (eigen infrastructuur) naar een publieke cloud omgeving. De Staatssecretaris Digitalisering stelt daarin in de brief van 18 februari 2025.

“Met deze brief informeer ik u specifiek over de voorgenomen vernieuwing van de digitale werkplek door SSC-ICT, ter zake waarvan het lid Kathmann heeft verzocht voorlopig geen onomkeerbare stappen te nemen. Ik beoog daarmee om u – rechtdoende aan de zorgen van uw Kamer en de veranderde geopolitieke situatie - een beter beeld te geven van de beoogde migratie, de overwegingen en de voorgenomen maatregelen om ongewenste risico's te mitigeren. Zo heeft SSC-ICT naar aanleiding van de veranderende situatie en uw zorgen het ontwerp van de werkplek aangepast, waardoor de afhankelijkheid van de public cloud sterk is gereduceerd.”

Vanuit JenV | AenM wordt eveneens dezelfde zorgvuldigheid betracht, wat concreet betekent dat er geen onomkeerbare stappen worden ondernomen betreffende het verplaatsen van mailboxen (Zie ook beleidslijn Exchange), opslag van documenten en bestandsdelingsfunctionaliteit.

Het gebruik van de lokale/decentrale MS365 Business Apps zoals Word, Powerpoint, Excel, Outlook etc. zijn toegestaan.

2.2.3 Beleidslijn gebruik MS Teams

Het gebruik van MS Team als webconferencing- en chat-tool is toegestaan (Videovergaderen). Het gebruik van de samenwerkingsfunctionaliteit binnen teams, bestandsdeling en inrichting van teamkanalen e.d. is vooralsnog niet toegestaan. Hiermee wordt voorkomen dat bestanden op One-Drive online en Sharepoint online worden geplaatst. Afhankelijk van de ontwikkelingen Rijksbreed kan verruiming worden toegepast onder de nog vast te stellen voorwaarden.

2.2.4 Beleidslijn gebruik Exchange

Het gebruik van **enkel** Exchange Online is niet toegestaan, vanwege het feit dat hiermee alle outlook-postbussen inclusief documenten in de publieke cloud worden geplaatst. Vanwege het out-of-support (14 oktober 2025) van Exchange Server 2019, dient deze vervangen te worden door Exchange Server Subscription Edition (SE), waardoor de on-premise voorziening van Exchange kan worden gecontinueerd. Dit kan in een **hybride** model met Exchange online worden ingezet, wat betekent dat de mailboxen en agenda op de Exchange Server on-premise blijven en gericht besloten kan worden, of en welke mailboxen en agenda's naar de cloud mogen worden verplaatst. Dit hybride model maakt het eveneens mogelijk om agendadeling met andere organisaties in te richten (agendafederatie).

2.2.5 Beleidslijn gebruik One-Drive Online Sharepoint Online

Het gebruik van OneDrive Online en Sharepoint Online zijn vooralsnog niet toegestaan. Indien documentdeling en samenwerking op documenten noodzakelijk is, wordt verwezen naar de beschikbare functionaliteiten van de Rijksbrede Samenwerkingsruimten en de eigen Nextcloud/OwnCloud oplossing die JenV | AenM lokaal beschikbaar heeft, deze is te bereiken onder www.bestandenpostbus.nl met een bewerkingsmogelijkheid Collabora. Accounts hiervoor kunnen worden aangevraagd via info@justid.nl en voor medewerkers van het bestuursdepartement via fb.dwo@minjenv.nl

Vanwege het out-of-support lopen van Sharepoint 2019 (14 juli 2026) dient indien noodzakelijk deze vervangen te worden Sharepoint Server Subscription Edition, de on-premise opvolger van Sharepoint Server 2019.