Ministerie van Economische Zaken
en Klimaat

Herziening rijksbreed cloudbeleid 2026

Datum 3 juli 2026
Status Definitief

Inhoud

1. Inleiding

In 2022 is het Rijksbrede Cloudbeleid ingevoerd. Dit beleid stelde voorwaarden en grenzen aan het gebruik van publieke cloud door de Rijksdienst. Op basis van voortschrijdend inzicht, de onderzoeken in 2024 door de Auditdienst Rijk en de Algemene Rekenkamer,[1] relevante Kamermoties, gewijzigde geopolitieke verhouding en de ontwikkelingen in de (cloud)markt, is er een noodzaak dit beleid te herzien en op een aantal punten aan te scherpen. Op grond van het Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst en op basis van het Besluit CIO-stelsel Rijksdienst 2026 stelt dit beleid kaders aan het gebruik van cloud.

De rijksoverheid maakt in toenemende mate gebruik van diverse vormen van cloud. Dit betreft onder meer publieke cloud, hybride cloud en private cloud. In het geval deze diensten worden aangeboden door een externe leverancier, is dit beleid van toepassing.

Dit Cloudbeleid is leidend voor alle onderdelen van de Rijksoverheid, exclusief de Hoge Colleges van Staat. Het Ministerie van Defensie is uitgezonderd van dit cloudbeleid vanwege het afwijkende dreigingsbeeld en er in sommige situaties ook hogere eisen aan beschikbaarheid en inzetbaarheid worden gesteld. Waar mogelijk zal Defensie het beleid wel volgen. Overige uitzonderingen staan in hoofdstuk 5 vermeld.

Voor de herziening van het cloudbeleid zijn in het coalitieakkoord geen extra middelen beschikbaar gesteld. Daarnaast kent de Rijksoverheid een rijksbrede taakstellingen uit het coalitieakkoord, die de komende jaren impact hebben op de beschikbare capaciteit en middelen. Dit betekent dat het herziene cloudbeleid ingepast moet worden binnen de bestaande IV-mogelijkheden en de huidige kaders van de departementale begrotingen. Dit betekent dat de implementatie langere tijd in beslag kan nemen en scherpe keuzes gemaakt moeten worden en waar nodig, herprioritering plaats moet vinden. De overgangstermijn geeft ook de kans om, waar mogelijk, te profiteren van het groeiende aanbod van soevereine cloudoplossingen.

Voor bestaand cloudgebruik geldt een overgangstermijn van 4 jaar, of eventueel langer als er een bestaande overeenkomst is met een langere looptijd, of als de invoering, en daarmee gepaard gaande aanpassingen, hoge kosten of risico's met zich meebrengen. In dat geval kunnen de benodigde aanpassingen worden ingepast in een logisch moment van de levenscyclus van de applicatie of portfolio van applicaties.

Hoge colleges van staat en andere overheidsorganisaties wordt geadviseerd om dit beleid te volgen. Zelfstandige bestuursorganen worden geacht dit beleid te volgen[2]. Aan de departementen wordt gevraagd dit beleid voor de onder hun minister vallende zelfstandige organisaties verder te stimuleren

[1] Betreffende 'Bevindingen onderzoeksopdracht 'Evaluatie public cloudbeleid Rijksoverheid'' door de Auditdienst Rijk en het rapport 'Het Rijk in de cloud' van de Algemene Rekenkamer.
[2] Dit beleid betreft het "ter zake voor de Rijksdienst geldende voorschriften" als bedoeld in Art 41.1. van de Kaderwet Zelfstandige Bestuursorganen. ZBO's die onder deze wet vallen, volgen dus dit beleid.

Ontwikkelingen die het cloudbeleid concreet sturen zijn:

1. Gewijzigde geopolitieke verhoudingen en de wens om digitale soevereiniteit en autonomie van de rijksoverheid te vergroten, in lijn met de NDS en de Visie Digitale Autonomie en Soevereiniteit van de Overheid.
2. De publieke cloud markt wordt gekenmerkt door een steeds grotere concentratie van een kleine groep leveranciers. Deze toenemende afhankelijkheid kan leiden tot een monocultuur die risico's met zich meebrengt (minder invloed op technologische keuze, leveranciersafhankelijkheid, beschikbaarheid, weerbaarheid).
3. Publieke cloud wordt met name van niet-Europese ondernemingen afgenomen. Dit brengt een risico met zich mee dat buitenlandse bedrijven of statelijke actoren toegang krijgen tot vertrouwelijke data en processen of dat deze als drukmiddel door een buitenlandse overheid kunnen worden gebruikt,[3] zoals ook gesignaleerd in het CSBN 2025.
4. De Tweede Kamer de wens heeft uitgesproken om per 2029 minstens 30% van alle cloudopslagdiensten en -applicaties die de Rijksoverheid afneemt van Nederlands-Europese bodem te laten komen.[4]

Na de verwachte realisatie van een soevereine overheidscloud, die geschikt is voor kritieke digitale infrastructuur, zal dit beleid worden aangepast.

Naast dit cloudbeleid is ook de Cyber Beveiligingswet (Cbw) van toepassing of kan de Wet weerbaarheid kritieke entiteiten (Wwke) van toepassing zijn. De maatregelen van dit beleid moeten dan worden toegepast binnen de eisen van die wetten.

[3] Cybersecuritybeeld Nederland 2025, hoofdstuk 4.
[4] Kamerstukken II, 2024/25, 36 574, nr. 5.

2. Beleid

Cloud is primair een flexibele manier van IT Infrastructuur leveren die voordelen biedt aan de overheid. Naast flexibiliteit, leveren clouddiensten schaalbaarheid, robuustheid en cyberveiligheid en ondersteunen daarmee innovatie en de betrouwbare levering van overheidsdiensten. Gelijktijdig brengt het gebruik van cloud ook nieuwe risico's met zich mee.

Dit beleid beoogt de Rijksoverheid te ondersteunen in het gebruik van deze technologie, op een manier die de publieke belangen beschermt. Het beleid Dit betekent dat Rijksoverheid organisaties:

- Continuïteit van diensten borgen door duidelijke afspraken over beschikbaarheid, exit-mogelijkheden en noodscenario's.
- Inzicht en controle houden over gegevens, inclusief waar data wordt opgeslagen en wie er toegang toe kan krijgen.
- Autonomie van het land en van het departement versterken, door afhankelijkheden van specifieke leveranciers[5] te beperken en waar mogelijk gebruik te maken van soevereine of Europese cloudoplossingen.
- Veilig, schaalbaar en efficiënt IT-gebruik mogelijk maken, zonder in te leveren op privacy, veiligheid en wettelijke kaders.

Het gebruik van cloud diensten is toegestaan voor overheidsorganisaties van de rijksoverheid, binnen de kaders van dit beleid. Er geldt een aantal beperkingen en voorwaarden en een beperkt aantal uitzonderingen op dit beleid.

Dit beleid geldt voor publieke cloud, hybride cloud, community en private cloud, wanneer afgenomen van een externe leverancier. Bij Software-as-a-Service is dit beleid van toepassing als de software draait op een publieke cloud voorziening of anderszins gebruik maakt van een gedeelde infrastructuur die door een niet-overheidspartij wordt geleverd.

2.1 Eigen beleid

Binnen de kaders van dit Rijksoverheidsbrede cloudbeleid formuleren alle departementen en andere Rijksoverheidsorganisaties hun eigen cloudbeleid en cloudstrategie.[6] Daarin hebben de departementale (of de overheidsorganisatie) CIO en CISO hun verantwoordelijkheid, zoals ook in CIO Stelsel is vastgelegd.
De cloud strategie van de organisatie geeft aan wanneer cloud de voorkeur heeft, welke voordelen daarmee worden beoogd te halen en hoe deze worden geborgd. Gezien de specifieke karakteristieken van cloud wordt een generiek "cloud-tenzij" beleid afgeraden.

Het hebben van een goede cloud-architectuur is essentieel om cloud succesvol te gebruiken. Een dergelijke architectuur koppelt de applicatie en data zoveel mogelijk los van het onderliggende platform, waardoor meer flexibiliteit ontstaat in waar een applicatie kan draaien.

[5] Leveranciersafhankelijkheid is een risico dat niet alleen bij cloud voorkomt maar bij elke technologie keuze een rol speelt. Maar doordat bij cloud de leverancier een directe impact heeft op onder andere de beschikbaarheid van de dienst, is de afhankelijkheid zeer direct. Het Rijksbrede Strategie IT-sourcing vraagt hier ook aandacht voor. Dit zal in het inkoopbeleid verder uitgewerkt moeten worden.
[6] Dit is ook conform de Amvb Cyberbeveiligingsbesluit.

Een lift-en-shift migratie naar de cloud, dus zonder gebruik van de juiste architectuur, realiseert zelden de gewenste voordelen, maar creëert wel nieuwe cloud-gerelateerde risico's.

Goed gebruik van cloud vereist dat er binnen de organisatie voldoende kennis en kunde in huis is om dit in goede banen te leiden. Het gaat dan om veiligheid, maar ook om operationele beschikbaarheid en het beheersen van de vaak variabele kosten van cloud.

Indien organisaties besluiten af te wijken van dit beleid dan wordt, in overleg met het kerndepartement, vooraf melding gedaan aan CIO Rijk.[7] Meldingen aan CIO Rijk kunnen, na inhoudelijke afstemming en beoordeling, leiden tot aanwijzingen van de CISO Rijk[8] om aanvullende maatregelen te nemen.

[7] Via cisorijk@minbzk.nl
[8] Op basis van het Besluit CIO-stelsel Rijksdienst 2026, art 21. Dit heeft alleen betrekking op de Rijksdienst.

3. Risico’s

3.1 Risicoafweging

De cloud leverancier wordt een essentieel onderdeel van de dienstverlening. De cloud leverancier neemt een deel van de verantwoordelijkheid voor de continuïteit en veiligheid voor haar rekening (vaak uitgedrukt in het Shared Responsibility Model). Controle of de leverancier die verantwoordelijkheid correct invult is niet altijd goed mogelijk en is soms afhankelijk van reguliere audits van derden. SLM Rijk kan in sommige gevallen aanvullende informatie achterhalen.

Voor materieel cloudgebruik (zie 4.1) is een integrale risicobeoordeling noodzakelijk. Deze risico beoordeling vindt plaats op basis van de classificatie van de toepassing (bijvoorbeeld op basis van BIV eisen of een TBB classificatie).[9] De aard van de data en de verwerking (mate van vertrouwelijkheid, integriteit en het belang van continuïteit) moeten daarbij het uitgangspunt van de analyse zijn.
Worden er persoonsgegevens verwerkt, dan moet ook een pre-scan DPIA en DPIA opgesteld worden. Bij gegevensoverdracht naar een derde land, waar geen adequaatsheidsbesluit voor bestaat, is een DTIA verplicht.

Naast de beoogde voordelen van cloud gebruik, moeten in de analyse ook de risico’s van cloud worden meegewogen. Hoe wordt bijvoorbeeld mogelijke toegang van de cloudleverancier tot vertrouwelijke data gemitigeerd? Wanneer moet de leverancier inzage geven in veiligheidsincidenten of mogelijke datalekken. Hoe kan dit worden gecontroleerd? Valt de leverancier mogelijk ook onder buitenlandse jurisdictie? Hoe zijn dergelijke risico’s te mitigeren?

Daarnaast zijn er mogelijke risico’s van toepassing vanwege marktconcentratie. De overheid is in grote mate afhankelijk van een kleine groep leveranciers. Hoe draagt het geplande cloudgebruik bij aan vermindering of juist toename van die afhankelijkheid?

Voor iedere geplande inzet van materieel cloudgebruik voor overheidsdiensten wordt een risicoanalyse gemaakt. Deze betreft, naast de reguliere onderwerpen zoals beveiliging, continuïteit, privacy, ook de volgende aspecten:

1. De karakteristieken van het gebruik van de clouddienst, zoals de (hoofd-) dienstverlener en eventuele onder-dienstverleners, het type dienstverlening (publieke/private/hybride/community cloud[10]), de geografische regio van verwerking en opslag van gegevens.
2. Welke rol in beveiliging en continuïteit heeft de cloudleverancier en hoe is deze geborgd?
3. Hoe is geregeld dat de dienstverlener controle en verantwoordings-onderzoeken toelaat of daarover rapporteert?

[9] Dit is ook een invulling van de verplichting vanuit de Cyberbeveiligingregeling overheid (Cbro), paragraaf 2, identificeren essentiële diensten.
[10] Voor community of private clouds, geleverd door een overheidsorganisatie, zijn er onderdelen van dit beleid nog steeds van toepassing. Dit wordt in het Implementatiekader nader aangegeven.

4. Als er sprake is van een risico op inmenging door een buitenlandse overheid op de vertrouwelijkheid en beschikbaarheid moet dit expliciet worden meegewogen en zoveel als mogelijk worden gemitigeerd.[11]
5. De kans dat een cloud leverancier misbruik maakt van een grote leveranciersafhankelijkheid, onder meer door ongewenste technologische keuzes af te dwingen of ongewenste commerciële condities te stellen.

Het implementatiekader risicobeheersing cloudgebruik moet hierbij worden gevolgd. Resterend risico moet worden gedocumenteerd en formeel geaccepteerd binnen de eigen organisatie. Besluitvorming door de verantwoordelijk bestuurder moet toetsbaar en auditeerbaar zijn. Mitigerende maatregelen die mede afhangen van activiteiten die de beoogd leverancier moet nemen (of juist niet moet doen), moeten in de overeenkomst worden opgenomen.

3.2 Exit-plan

Bij materieel cloudgebruik is een gedocumenteerd en door de organisatie zelf getoetst exit-plan verplicht.[12] Dit plan houdt rekening met twee scenario's:

1. Geplande exit: Dit plan beschrijft hoe de betrokken dienst zonder ongeplande verstoring van activiteiten, kan worden verplaatst naar een andere leverancier of eventueel in eigen beheer kan worden genomen. In de overeenkomst met de cloud leverancier is opgenomen hoe bij beëindiging van de overeenkomst, data, metadata en eventueel applicaties worden overgedragen.[13] Doel van dit plan is onder meer dat de organisatie duidelijk heeft welke kritische randvoorwaarden geregeld moeten zijn voor een exit en welke minimale termijn noodzakelijk is.
2. Disruptieve onderbreking van de dienstverlening: Dit plan geeft aan welke stappen genomen worden, als de cloud dienstverlening onverwacht niet meer beschikbaar is, om de betrokken overheidstaak of dienstverlening te kunnen continueren. Het geeft aan welke maatregelen al vooraf genomen moeten zijn, zoals het eventueel beschikbaar hebben van een back-up buiten de cloud- omgeving. Het beschrijft de noodzakelijke stappen hoe de meest kritieke processen in dit scenario kunnen worden hersteld.

In beide gevallen wordt ook meegenomen hoe ervoor wordt gezorgd dat de data bij de leverancier, na afronding van de migratie, wordt vernietigd. Beide plannen worden jaarlijks op actualiteit beoordeeld en zo nodig aangepast.

3.3 Melding en beoordeling

Bij materieel cloudgebruik wordt voorafgaande aan de daadwerkelijke implementatie een melding gedaan aan CISO Rijk. Bij voorkeur wordt dit gedaan in combinatie met de risicoanalyse en het exitplan via (cisorijk@minbzk.nl). Indien de risicoanalyse of exitplan nog niet gereed zijn, kunnen deze op een later moment gedeeld worden. Door de melding zijn CIO- en CISO Rijk beter in staat het overzicht te bewaren van waar cloud wordt toegepast, kunnen eventuele stapelingsrisico's worden gesignaleerd en kan beoordeeld worden of het cloudgebruik ook voldoet aan de eisen van dit beleid.

[11] Het EU Cloud Sovereignty Framework geeft handvatten om in een leverancierselectie het risico van buitenlandse inmenging in te perken https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en

[12] Voor reeds bestaand materieel cloudgebruik geldt een overgangstermijn van 12 maanden, na vaststelling van dit beleid, om een exitplan te maken.

[13] De Data Act borgt dit bij nieuwe overeenkomsten. Als gebruik wordt gemaakt van bestaande overeenkomsten, moet dit expliciet worden opgenomen.

De melding en mogelijke beoordeling van de risicoanalyse en exitplan, is geen vervanging van de eigen verantwoordelijkheid van het departement of organisatie. Die blijft zelfstandig verantwoordelijk.

CISO Rijk beoordeelt of het cloudgebruik past binnen dit cloudbeleid en of risico's op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid voldoende zijn afgewogen en waar nodig afdoende gemitigeerd. Ook het exitplan wordt in deze beoordeling meegenomen. Op basis van de risicoanalyse en mogelijk aanvullend overleg, kunnen er aanwijzingen[14] gegeven worden als de risicoanalyse of de mitigaties onvoldoende worden geacht.

3.4 Gekend gebruik

Materieel publiek cloudgebruik en de bijbehorende risicoanalyse wordt geregistreerd door de organisatie. Jaarlijks rapporteren departementen over het gebruik van materieel publieke cloud gebruik van henzelf en de onder het ministerie vallende organisaties, inclusief de gekozen cloud leverancier, aan CIO Rijk.
CIO Rijk monitort de naleving van dit cloudbeleid en het bijbehorende implementatiekader, op basis van de melding en het jaarlijkse overzicht.

[14] Dit geldt alleen voor organisaties die tot de rijksdienst behoren.

4. Eisen voor ICT-dienstverlening

4.1 Voldoen aan eisen voor ICT-dienstverlening

Alle typen clouddienstverlening, dus ook publieke, moeten allereerst voldoen aan de bestaande voorwaarden voor ICT-dienstverlening. Risico's moeten voldoende gemitigeerd zijn en blijven. De verantwoordelijk Minister moet zich hiervan verzekeren en dit kunnen aantonen. Elk departement moet registreren voor welke verwerkingen, welke publieke cloud, wordt gebruikt. Er is daarmee een verplichting tot het bijhouden van materieel publieke cloudgebruik en de risico's daarvan.

Materieel publiek cloudgebruik is gebruik van publieke clouddiensten ten behoeve van het uitvoeren van de primaire of kerntaak van een organisatie. Met andere woorden, voor de organisatie is die (cloud)dienst van wezenlijk belang[15]. Belangrijke bedrijfsondersteunende processen kunnen hier ook deel van uitmaken.
Daarnaast is de grootschalige verwerking van persoonsgegevens materieel cloudgebruik[16].

4.2 Cyberveiligheid

Cyberveiligheid verdient apart aandacht, mede omdat ook statelijke actoren geïnteresseerd zijn in informatie over Nederland. Gezien het grote aanvalsoppervlak van publieke cloud, moeten voorzieningen die in de publieke cloud draaien, adequaat beveiligd en gemonitord worden.

Bij gebruik van publieke cloud diensten ontstaat veelal gegevensverwerking in andere landen, waaronder soms ook in landen buiten de EER. Wetgeving uit andere landen kan een impact hebben op de veiligheid van de informatie. We hanteren 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.

Naast de in de C2000 criteria genoemde landen, kunnen ook andere landen een risico vormen. Dit valt onder de geopolitieke risico's die in de risicoanalyse beoordeeld moeten worden.

Ook als een dienst niet onder de ABRO valt, kan er een risico zijn op dreiging van statelijke actoren. In dat geval wordt voortijdig dreigings- en beveiligingsadvies ingewonnen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en/of Militaire Inlichtingen- en Veiligheidsdienst (MIVD).

4.3 Kritieke of Essentiële Entiteiten

Het is ongewenst dat er voor kritieke processen een mogelijk beïnvloeding van buiten de EU kan plaatsvinden. Daarom wordt afgeraden voor organisaties die:

1. Als vitale aanbieder zijn aangemerkt,[17]
2. onder de Wet Weerbaarheid Kritieke Entiteiten vallen,
3. of die binnen de categorie Essentiële Entiteiten van de Cyber Beveiliging Wet vallen;

15 Kerntaken zijn vastgelegd in het betreffende organisatiebesluit of de relevante instellingswet bij ZBO's.
16 https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/verwerken-van-persoonsgegevens
17 Na inwerkingtreding van de Wwke gaan als vitaal aangewezen organisaties over naar de Wwke.

om voor hun primaire proces of onderdelen daarvan, gebruik te maken van diensten van leverancier die (deels) onder een jurisdictie van buiten de EU of de EER valt. Organisaties die niet onder deze wetgeving vallen, maar waarvan de beschikbaarheid en betrouwbaarheid van diensten en data, van nationaal belang is, worden geacht een vergelijkbaar veiligheidsniveau te hanteren

4.4 Openbaarheid

In het licht van de Wet Open Overheid (Woo) wordt uitgegaan van openbaarmaking van alle relevante besluitvorming door de eigenaar. De risicoanalyse en het exit-plan kunnen vanwege veiligheidsrisico's van een passende rubricering worden voorzien.

4.5 Email en bestandsopslag

Door de grote hoeveelheid documenten en (deels) vertrouwelijke mailberichten, worden werkplekdiensten van de overheid beschouwd als een nationaal belang, en *bij voorkeur* niet in de publieke cloud ondergebracht.

E-mail voorzieningen[18] en documenten mogen niet in de publieke cloud worden verwerkt, tenzij aan alle drie van de volgende voorwaarden is voldaan: [19]

a. onafhankelijk is vastgesteld dat de continuïteit van de dienstverlening anders in gevaar komt.
b. Risicoanalyse en exit plan volgens dit beleid zijn gemaakt en getoetst.
c. Het besluit is geaccordeerd door de betrokken minister in overeenstemming met de bewindspersoon voor digitalisering.

Waar werkplekdiensten nu al in de publieke cloud zijn ondergebracht, geldt een overgangstermijn van 4 jaar, of de resterende looptijd van een bestaande overeenkomst als deze langer is. In gevallen waar de benodigde aanpassingen en migraties onoverkomelijke risico's of kosten met zich meebrengen, kan de migratie worden ingepast in de geplande levenscyclus van een applicatie. De daarmee ontstane risico's moeten worden geaccepteerd. Dit wordt gemeld bij CIO Rijk.

4.6 Opslag en verwerking van belangrijke gegevens

Voor alle informatie geldt dat opslag en verwerking plaatsvindt binnen de EER[20] en Zwitserland[21]. Voor informatie en processen die nationale veiligheid of digitale autonomie raken, zullen aanvullende eisen worden gesteld conform de daarvoor geldende kaders.

Data worden bij opslag, verzending en mogelijk ook bij verwerking versleuteld. Enige uitzondering hierop zijn bestanden met openbare data. Bij vertrouwelijke gegevens wordt bij voorkeur het sleutelbeheer niet ondergebracht bij de cloud leverancier maar dit in eigen beheer, of bij een andere, op dat gebied gecertificeerde partij belegd.

Verwerking van bijzondere persoonsgegevens vindt bij voorkeur niet in de publieke cloud plaats. Als er toch een noodzaak is om dit te doen, dan moeten, naast de maatregelen uit dit beleid, zoals onder andere een DPIA, ook aanvullende maatregelen, zoals Privacy Enhancing Technologies toegepast worden.

[18] Voor specifieke of tijdelijke email of document faciliteiten kan een uitzondering worden gemaakt (bijvoorbeeld voor een project of om over een noodvoorziening uit continuïteits-overwegingen te kunnen beschikken.

[19] Hiermee wordt ook een invulling gegeven aan Kamerstukken II, 2024/25, 26 643, nr. 1315 en Kamerstukken II, 2024/25, 36 740 VII, nr. 20

[20] Deze richtlijn geldt niet voor Caribisch Nederland.

[21] Op basis van het adequaatsheidsbesluit van de Europese Commissie.

5. Uitzonderingen

5.1 Organisaties

Systemen die verband houden met internationale samenwerkingen, zoals bijvoorbeeld in EU verband, of systemen waar de inzet van ICT verband houdt met het wereldwijde karakter van werkzaamheden, zoals bijvoorbeeld bij het Ministerie van Buitenlandse Zaken, zijn van dit beleid uitgezonderd. Ditzelfde geldt voor systemen van het NCSC, die onder omstandigheden moeten werken als dat voor de rest van de overheid moeilijk is.

Voor deze uitzonderingen geldt dat dit beleid waar mogelijk toegepast wordt. Er zal in ieder geval voldaan worden aan de eisen rond risicoanalyse en exit-plannen en rapportage daarvan aan CISO Rijk.

5.2 Gerubriceerde data

Het gebruik van publieke clouddiensten is niet toegestaan voor staatsgeheim gerubriceerde informatie of voor Te Beschermen Belangen niveau 1, 2 en 3.[22]

5.3 Kleinschalige of tijdelijke email verwerking

Voor specifieke, kleinschalige doelen, waarbij bijvoorbeeld online samenwerking van belang is, kan een uitzondering worden gemaakt. Hierbij moet vooraf een risico analyse gemaakt zijn en in geval van gerubriceerde documenten, encryptie worden toegepast.

5.4 Basisregistraties

Basisregistraties worden niet (alleen) in een publieke cloud binnen of buiten de EER worden ondergebracht. Gebruik van publieke cloud voor capaciteit of performance eisen is mogelijk met inachtneming van de richtlijnen voorkomend uit dit beleid. De brondata worden niet in een publieke cloud beheerd.

Hiervoor geldt een overgangstermijn van 4 jaar, of de resterende looptijd van een bestaande overeenkomst als deze langer is. In gevallen waar de benodigde aanpassingen en migraties onoverkomelijke risico’s of kosten met zich meebrengen, kan de migratie worden ingepast in de geplande levenscyclus van een applicatie. De daarmee ontstane risico’s moeten worden geaccepteerd.

5.5 Internationale samenwerking

Bij internationale samenwerking (zoals onder andere door rijkskennisinstellingen en planbureaus) kan het voor deelname aan onderzoeken en bij uitwisseling van gegevens, noodzakelijk zijn, af te wijken van dit beleid voor wat betreft gebruik van publieke cloud en verwerking buiten de EER en Zwitserland. Indien dit om materieel cloudgebruik gaat, wordt dit, in overleg met het kerndepartement, voorzien van risicoanalyse en exitplan, gemeld aan CIO Rijk (cisorijk@minbzk.nl).

[22] Hier vallen ook (onderdelen van) basisregistraties onder.

6. Definities

Voor definities van de gebruikte cloud-terminologie wordt verwezen naar de Cloud definities en begrippenlijst, zoals vastgesteld door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO).

https://pgdi.nl/files/view/091e1d60-71d0-4617-aaba-1b4d88b45a91/cloud_definities_en_begrippenlijst_v1.0.pdf