Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2026–2027

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

168

Vragen van het lid **Kathmann** (PRO) aan de Staatssecretarissen van Economische Zaken en Klimaat en van Binnenlandse Zaken en Koninkrijksrelaties over *het herziene rijksbrede cloudbeleid 2026* (ingezonden 16 juli 2026).

Antwoord van Staatssecretaris **Aerdts** (Economische Zaken en Klimaat), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 29 september 2026). Zie ook Aanhangsel Handelingen, vergaderjaar 2025–2026, nr. 3029.

Vraag 1
Is het duidelijk voor alle relevante rijksorganisaties wat de gevolgen zijn van het herziene cloudbeleid? (Kamerstuk 26 643, nr. 1541) Kunt u aangeven of er organisaties zijn die bij voorbaat aangeven niet aan het herziene beleid te kunnen of zullen voldoen?

Antwoord 1
Ja, alle rijksorganisaties zijn tijdens het beleidstraject op verschillende momenten in diverse voorportalen meegenomen. De uitvoeringsorganisaties zijn via de betrokken koepelorganisaties geïnformeerd. Het herziene rijksbrede cloudbeleid is vastgesteld in de ministerraad. Op basis van de terugkoppeling vanuit het Netwerk van Publieke Dienstverleners (NPD) is het beleid op een aantal punten verduidelijkt en aangepast om overheidsorganisaties beter in staat te stellen om aan het beleid te kunnen voldoen. Op dit moment zijn geen organisaties bekend die niet aan het herziene beleid kunnen of zullen voldoen. Daarnaast is voor rijksorganisaties ook duidelijk dat in het coalitieakkoord geen extra middelen beschikbaar zijn voor het herziene cloudbeleid en het beleid ingepast moet worden binnen de bestaande departementale begrotingen. Hierdoor kan de implementatie langere tijd in beslag nemen, moeten scherpe keuzes gemaakt worden en moet waar nodig herprioritering plaatsvinden.

Vraag 2
Hebben rijksorganisaties voldoende beeld op hun eigen cloudgebruik om de herziene regels effectief na te leven? Op welke delen van het cloudlandschap van de overheid ontbreekt er nog overzicht?

ah-tk-20262027-168
ISSN 0921 - 7398
's-Gravenhage 2026

Antwoord 2
Rijksorganisaties zijn zelf verantwoordelijk voor hun eigen cloudgebruik en de naleving van de herziene regels. Naar aanleiding van het Rekenkamer-rapport «Het Rijk in de Cloud»[1] hebben de departementen een aanzienlijke inhaalslag gemaakt om hun cloudgebruik inzichtelijk te krijgen. De inzichten zijn in het CIO Beraad gedeeld.

Vraag 3
Welke rol krijgt de veelbelovende Nederlandse Digitale Dienst om zeker te stellen dat alle rijksorganisaties aan het herziene cloudbeleid kunnen en zullen voldoen? Bent u bereid de organisatie hiertoe de nodige capaciteit en instrumenten te geven?

Antwoord 3
Zoals nu voorzien gaat de Nederlandse Digitale Dienst (NDD) geen rol in de uitvoering van het herziene rijksbrede cloudbeleid spelen. De uitvoering van het beleid is primair de verantwoordelijkheid van de overheidsorganisaties waarbij CIO Rijk een monitorende taak heeft, zoals ook vastgelegd in het Besluit CIO-stelsel Rijksdienst 2026.[2]

Vraag 4
Kunt u een schematisch overzicht geven van maatregelen die ook overwogen zijn voor het herziene cloudbeleid, met een onderbouwing waarom deze uiteindelijk niet zijn opgenomen?

Antwoord 4
Zoals toegelicht in de beantwoording van vraag 1 is voor de herziening van het rijksbrede cloudbeleid een lang, interdepartementaal traject doorlopen. Het beleid is aangescherpt met het oog op geopolitieke en organisatorische ontwikkelingen, zodat de Rijksoverheid veilig gebruik kan maken van clouddiensten. Er zijn geen maatregelen overwogen die niet uiteindelijk in het cloudbeleid zijn opgenomen. In overleg met het NPD is de invoeringstermijn aangepast, omdat het stellen van een uniforme overgangstermijn bij een aantal organisaties een te grote impact op de bestaande planningen en het kostenniveau zou veroorzaken. In het beleid is nu voorzien dat in het geval dat een migratie of aanpassing aan het herziene cloudbeleid tot onoverkomelijke kosten of risico's zal leiden, deze migratie of aanpassing kan worden ingepland op een logisch (en eventueel later) moment in de levenscyclus van de betrokken systemen of applicaties.

Vraag 5 en 6
Welke concrete doelen heeft het kabinet om digitaal onafhankelijk te worden? Wordt het doel vastgesteld op 30% digitaal onafhankelijk per 2029, zoals gevraagd in de motie-Thijssen/Bruyning (Kamerstuk 36 574, nr. 5) en de initiatiefnota Wolken aan de Horizon (Kamerstuk 36 574, nr. 2)?
Hoeveel digitaal onafhankelijker wordt de Rijksoverheid door het herziene cloudbeleid in de komende jaren? Wordt het doel van 30% in 2029 gehaald?

Antwoord 5 en 6
De 30%-norm van de motie Thijssen (PRO)/Bruyning (NSC), evenals de initiatiefnota «Wolken aan de Horizon», is opgenomen als drijfveer van het herziene cloudbeleid en daarin expliciet opgenomen.
Het is niet vooraf vast te stellen wat de impact van één beleidsstuk is op de digitale afhankelijkheid van de Rijksoverheid. Om te zien wat het doel is van het kabinet t.a.v. digitale autonomie verwijs ik u graag naar de Visie Digitale Autonomie en Soevereiniteit van de Overheid.[3] Ook Europese ontwikkelingen, zoals het recent gepubliceerde wetsvoorstel voor de *Cloud & AI Development Act* (CADA), kunnen bijdragen aan grotere digitale onafhankelijkheid en het bereiken van de 30%-norm.

---

[1] Het Rijk in de cloud | Algemene Rekenkamer
[2] https://wetten.overheid.nl/BWBR0044613/2026-01-01
[3] Visie - Digitale autonomie en soevereiniteit van de overheid

Vraag 7
Kunt u heel concreet uitleggen welke rol u heeft, als coördinerend Staatssecretaris (EZK) en als Staatssecretaris verantwoordelijk voor uitvoeringsdiensten (BZK), om dit beleid te handhaven?

Antwoord 7
Conform de portefeuilleverdeling van het kabinet Jetten op dit onderwerp is de taakverdeling tussen de beide bewindspersonen als volgt:
Staatssecretaris van Economische Zaken – Digitale economie en soevereiniteit
– Coördinerend op digitalisering en soevereiniteit
– Normering en regulering van beleid t.a.v. digitalisering, technologie en soevereiniteit in samenleving en overheid
Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties – Koninkrijksrelaties en slagvaardige overheid
– CIO-Rijk
– Informatieveiligheid voor (Rijks)overheid
CIO-Rijk kan organisaties binnen de Rijksoverheid, die vallen onder het herziene rijksbrede cloudbeleid, aanspreken op het toepassen van het cloudbeleid.

Vraag 8
Welke instrumenten heeft u om het herziene cloudbeleid daadwerkelijk uit te voeren? Met hoeveel zekerheid kunt u zeggen dat dit beleid zal leiden tot een digitaal onafhankelijke Rijksoverheid?

Antwoord 8
Ter ondersteuning van de uitvoering van het herziene cloudbeleid zal ook het bijbehorende implementatiekader worden herzien. Deze herziening zal in samenwerking met een aantal grote uitvoeringsorganisaties plaatsvinden en is erop gericht om een aantal praktische werkwijzen aan te geven waarmee risicoanalyses, exitstrategieën en plannen kunnen worden uitgevoerd. Opgedane ervaring met migreren naar passende voorzieningen zal worden gedeeld met organisaties die onder het herziene cloudbeleid vallen.
Een digitaal soevereine Rijksoverheid gaat overigens verder dan alleen cloudgebruik. Dat neemt echter niet weg dat het herziene cloudbeleid hier wel een belangrijke rol in speelt. Autonomie is in brede zin één van de primaire drijvers geweest in de herziening van het beleid. Zoals toegelicht in het cloudbeleid, indien organisaties besluiten af te wijken van dit beleid dan wordt, in overleg met het kerndepartement, vooraf melding gedaan aan CIO Rijk. Meldingen aan CIO Rijk kunnen, na inhoudelijke afstemming en beoordeling, leiden tot aanwijzingen van de CISO Rijk om aanvullende maatregelen te nemen.

Vraag 9
Heeft u overwogen om het coördinatiebesluit, waarin de bevoegdheden van bewindspersonen zijn vastgelegd, uit te breiden zodat u dwingender kan optreden om het herziene cloudbeleid uit te voeren? Waarom heeft u dit niet gedaan, cf. de motie-Six Dijkstra (Kamerstuk 26 643, nr. 1294)?

Antwoord 9
Om de departementale autonomie te behouden is hier niet voor gekozen. Departementen zijn en blijven zelf verantwoordelijk voor hun eigen bedrijfsvoering, waaronder ICT. Conform het Besluit CIO-stelsel Rijksdienst 2026 heeft ieder departement een eigen CIO en CISO. Hierbij is CIO Rijk en CISO Rijk kaderstellend en coördinerend. Dit doet verder niet af aan voorgenoemde departementale autonomie.

Vraag 10
Waarom is er, ondanks de hoge ambities in het coalitieakkoord, geen budget beschikbaar gesteld voor de herziening van het cloudbeleid?

Antwoord 10
Voor de herziening van het cloudbeleid zijn in het coalitieakkoord geen extra middelen beschikbaar gesteld. Dit betekent dat het beleid ingepast moet worden binnen bestaande IV-mogelijkheden en de huidige kaders van de departementale begroting.

Vraag 11
Wat bedoelt u met de «scherpe keuzes» en «herprioritering» die nodig zijn omdat het kabinet geen middelen reserveert voor haar eigen digitale ambities?

Antwoord 11
Voor rijksorganisaties die aan het herziene cloudbeleid moeten voldoen zullen er inderdaad keuzes gemaakt moeten worden t.a.v. wat er wanneer plaats kan vinden qua activiteiten rondom bijvoorbeeld het migreren van ICT-diensten. Dit betreft naast financiële middelen ook de beschikbaarheid van personeel om dergelijke trajecten te verzorgen, evenals bestaande overeenkomsten met al-dan-niet langere looptijden. Het herziene cloudbeleid komt hieraan tegemoet door hier rekening in te houden met de overgangstermijn.

Vraag 12
Met welke investeringen zou het herziene cloudbeleid sneller en effectiever toegepast kunnen worden? Hoe kan voorkomen worden dat door «scherpe keuzes» en «herprioritering» geen vaart wordt gemaakt met de nodige maatregelen om digitaal onafhankelijk te worden?

Antwoord 12
Er is geen investeringsoverzicht opgesteld. Departementen en uitvoeringsorganisaties zullen hier zelf keuzes in moeten maken binnen de in het herziene cloudbeleid genoemde overgangstermijnen. Als er aanvullende middelen beschikbaar kunnen worden gesteld, of bestaande middelen kunnen worden vrijgemaakt voor de implementatie van de soevereine overheidscloud, kan dit een platform bieden om systemen daarop te laten landen en daarmee te laten voldoen aan het herziene rijksbrede cloudbeleid.

Vraag 13
Kunt u de overgangstermijn van vier jaar onderbouwen? In welke gevallen wordt hier van afgeweken? Hoe voorkomt u dat migraties van bestaand cloudgebruik allemaal vertraagd worden wegens «hoge kosten of risico's»?

Antwoord 13
De termijn van vier jaar is gekozen omdat deze termijn redelijk lijkt te ziin voor cloumigraties. Daarbij is ruimte om de bestaande meerjaren implementatie-planning niet te ingrijpend te hoeven aan te passen en een dergelijke termijn voorkomt voor rijksorganisaties ook grote desinvesteringen. Uit het overleg met het NPD is echter gebleken dat in sommige gevallen deze termijn toch een forse impact kan hebben op continuïteit en kosten. Om daarmee rekening te houden, is de optie toegevoegd dat, in die gevallen, de aanpassingen op een later moment in de levenscyclus van een applicatie of omgeving kan worden ingepast. Op dit moment zijn nog geen eventuele uitzonderingen bekend.

Vraag 14
Wat bedoelt u ermee dat het «afgeraden» wordt om e-mail- en documentbeheer in de publieke cloud te zetten? Betekent dit dat binnen vier jaar alle mailservers en documentbeheer daadwerkelijk uit de publieke cloud worden gehaald?

Antwoord 14
E-mail en documentenbeheer worden in het nieuwe rijksbrede cloudbeleid aangemerkt als een nationaal belang, en *bij voorkeur* niet in de publieke cloud ondergebracht. Dit wordt nader gepreciseerd in het beleid met de uitleg dat e-mail en documenten niet in de publieke cloud mogen worden verwerkt, tenzij rijksorganisaties voldoen aan de volgende drie voorwaarden: onafhankelijk is vastgesteld dat de continuïteit van de dienstverlening anders in gevaar komt, een risicoanalyse en exit plan volgens dit beleid zijn gemaakt en getoetst, en het besluit is geaccordeerd door de betrokken Minister in overeenstemming met de bewindspersoon voor digitalisering.

Vraag 15
Welke aanpassingen in het IT-inkoopbeleid zijn nodig om het herziene cloudbeleid verder te ondersteunen? Heeft u plannen om het inkoopbeleid aan te scherpen, en zo ja, welke?[4]

Antwoord 15
Dit najaar ontvangt uw Kamer door de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties de visie op rijksinkoop. Deze visie neemt verdere stappen, zoals ook het herziene cloudbeleid, op digitale soevereiniteit. Richtlijnen voor het ontwerpen, ontwikkelen en inkopen van ICT-systemen vinden onder meer hun weg naar de inkooppraktijk via het categoriemanagement ICT, waarmee de Rijksoverheid de vraag naar ICT bundelt en de ICT gezamenlijk inkoopt en aanbesteedt. De noodzaak om mede via het herziene cloudbeleid versneld digitaal soeverein te worden heeft daarnaast gevolgen voor het strategisch leveranciersmanagement (SLM). Aan uw Kamer is toegezegd dat SLM zich meer gaat richten op de marktsectoren waarvan de digitale voorzieningen nodig zijn (zoals bijvoorbeeld clouddiensten) en er daar vanuit keuzes worden gemaakt voor de meest passende leverancier, contractvormen en exit-constructies.[5]

Vraag 16
Waarom wordt een generiek cloud-tenzij beleid enkel «afgeraden»? Waarom formuleert u dit niet dwingender?

Antwoord 16
Het kabinet vertrouwt erop dat het herziene rijksbrede cloudbeleid en gekozen woordkeuze een duidelijk kader is voor alle rijksorganisaties.

Vraag 17
Hoe wordt er op toegezien dat rijksorganisaties binnen 12 maanden een exitplan opstellen voor bestaand cloudgebruik?[6] Bent u van plan dit per organisatie te monitoren en met de Kamer te delen? Welke gevolgen zijn er als een organisatie niet op tijd een exitplan aanlevert?

Antwoord 17
Het opstellen en beoordelen van exitplannen is een verantwoordelijkheid van het departement of organisatie zelf. Daarnaast wordt beoogd materieel cloudgebruik gemeld bij CISO Rijk, waar ook een deling van de exitplannen integraal onderdeel van is. Dit zal niet met de Kamer gedeeld worden, aangezien dit operationele bedrijfsvoering betreft. Zie verder de beantwoording van vraag 21.

Vraag 18
Worden organisaties verplicht om opvolging te geven aan de «aanwijzingen» van de Chief Information Security Officer (CISO) Rijk, als blijkt dat aangeleverde cloudplannen, de risicoanalyse en/of het exitplan niet in lijn zijn met het beleid?

Antwoord 18
Een aanwijzing dient te allen tijde te worden opgevolgd door organisaties die onder het coördinatiebesluit vallen. Voor andere organisaties zal dat via, bijvoorbeeld politiek/bestuurlijke, gesprekken dienen plaats te vinden.

Vraag 19
Waarom is er niet voor gekozen om de CISO Rijk of de Staatssecretaris belast met Digitale Zaken de bevoegdheid te geven om cloudplannen, de risicoanalyse en/of het exitplan als geheel af te wijzen, als deze niet voldoen aan het herziene cloudbeleid?

---

[4] In voetnoot 5 van de Herziening rijksbreed cloudbeleid: «Leveranciersafhankelijkheid is een risico dat niet alleen bij cloud voorkomt maar bij elke technologie keuze een rol speelt. [...] Dit zal in het inkoopbeleid verder uitgewerkt moeten worden.» (p.5)

[5] Kamerstuk 26 643, nr. 1450

[6] Dit wordt gesteld in voetnoot 12 van de Herziening rijksbreed cloudbeleid.

Antwoord 19
Het is een politieke keuze geweest om de ministeriële verantwoordelijkheden in deze ongewijzigd te laten. Het herziene rijksbrede cloudbeleid bevat voldoende aangrijpingspunten om bij geconstateerde tekortkomingen, in goed overleg tot een gepaste oplossing te komen.

Vraag 20
Hoe verwacht u dat rijksorganisaties de «geopolitieke risico's» van cloudgebruik in hun risicoanalyse in kaart brengen? Welke criteria worden hiervoor gebruikt?

Antwoord 20
In de komende maanden zal het *Implementatiekader risicoafweging cloudgebruik* aangepast worden aan het herziene rijksbrede cloudbeleid. Hierin zal ook voor dit punt aandacht zijn.

Vraag 21
Hoe bent u van plan aan de Kamer te rapporteren over de opgestelde risicoanalyses en exitplannen van rijksorganisaties?

Antwoord 21
Het kabinet is niet van plan om aan de Kamer te rapporteren over de opgestelde risicoanalyses en exitplannen van rijksorganisaties, Dit omdat het opstellen en beoordelen van de opgestelde risicoanalyses en exitplannen operationele bedrijfsvoering binnen de overheid betreft, en tevens omdat de uitkomsten van de risicoanalyses vertrouwelijk worden behandeld om geen informatie te delen waarmee wij de risico's voor die rijksorganisaties zouden vergroten.

Vraag 22
Wat bedoelt u met het gegeven dat overheidsdocumenten en mailberichten «bij voorkeur» niet in de publieke cloud worden ondergebracht? Waarom bent u hier niet dwingender in, gezien de gevoeligheid van deze gegevens en de erkende risico's van de publieke cloud?

Antwoord 22
Zie antwoord op vraag 14.

Vraag 23
Kunt u concreet maken wanneer aan de drie uitzonderingsgronden is voldaan om tóch mailverkeer en documenten in de publieke cloud te mogen houden? Na hoeveel tijd wordt bezien of deze uitzonderingsgronden nog steeds gelden?

Antwoord 23
Zie antwoord op vraag 14. Daarnaast blijft elke organisatie zelf verantwoordelijk voor haar eigen risicobeleid en -acceptatie van risico's en worden uitzonderingen geaccordeerd door de betrokken Minister in overeenstemming met de bewindspersoon voor digitalisering.

Vraag 24
Wat bedoelt u met het gegeven dat het sleutelbeheer van versleutelde vertrouwelijke gegevens «bij voorkeur» niet bij de cloudleverancier wordt neergelegd? Waarom belegt u het niet per definitie in eigen beheer?

Antwoord 24
Er is een overgangstermijn van vier jaar in het herziene cloudbeleid opgenomen om de organisaties zowel richting te geven als ruimte om hun systemen en processen daaraan te laten voldoen. De inrichting van cryptografisch sleutelbeheer is een technisch complexe zaak die niet op korte termijn door iedere organisatie zelfstandig zal kunnen worden ingeregeld. Het is raadzaam om eerst praktisch uitvoerbare oplossingen voor de juiste omvang beschikbaar te hebben, voordat er juridisch of beleidsmatige situaties worden verboden of verhinderd. Als de data risico's voor de nationale veiligheid raken, zal de inkoop onder de ABRO worden uitgevoerd voor o.a. de departementen en agentschappen.

Vraag 25
Onder welke voorwaarden is het volgens u acceptabel om bijzondere persoonsgegevens alsnog in de publieke cloud te verwerken? Hoe wordt vastgesteld dat de mitigerende maatregelen afdoende zijn?

Antwoord 25
Verwerking van bijzondere persoonsgegevens vindt bij voorkeur niet in de publieke cloud plaats. In het geval dat er bijzondere persoonsgegevens in een publieke cloud worden verwerkt, moeten aanvullende maatregelen, zoals «Privacy Enhancing Technologies» worden toegepast. Dit kan bijvoorbeeld het pseudonimiseren van de gegevens zijn, of het toepassen van encryptie. Dit zal in de Data Protection Impact Assesment (DPIA) en risicoanalyse moeten worden beschreven.
Het ligt in de lijn der verwachting dat de specifieke maatregelen in samenwerking met de relevante toezichthouders, zoals de RDI, zullen worden ontwikkeld.

Vraag 26
Wat bedoelt u ermee dat het rijksbrede cloudbeleid «waar mogelijk» toegepast zal worden bij uitgezonderde organisaties? Worden de uitgezonderde organisaties wel geacht om hun eigen cloudbeleid aan te scherpen?

Antwoord 26
Artikel 5.1 gaat vooral over systemen die verband houden met internationale samenwerking. Daarbij is het gebruik van een soevereine, Europese oplossing niet altijd praktisch of heeft de Nederlandse overheidsorganisatie geen of weinig invloed op gemaakte technologische keuzes. Bij een dergelijke uitzondering geldt dat, waar mogelijk, het beleid zoveel als mogelijk wordt toegepast. Bijvoorbeeld door het maken van een risico analyse en het maken van een exitplan. Voor de overige systemen en cloudgebruik van een dergelijke geldt het herziene cloudbeleid onverkort, inclusief de noodzaak om een eigen cloudbeleid te hebben.

Vraag 27
Kunt u «kleinschalige doelen» noemen waarvoor het rijksbrede cloudbeleid een uitzondering zou maken? Hoe en door wie wordt bepaald of iets wel of niet uitgezonderd wordt?

Antwoord 27
In het herziene rijksbrede cloudbeleid, Art 5.3, is een uitzondering voor «kleinschalige of tijdelijke email verwerking» opgenomen. Hiervoor geldt dat voor specifieke, kleinschalige doelen, waarbij bijvoorbeeld online samenwerking van belang is, een uitzondering kan worden gemaakt. Hierbij moet vooraf een risicoanalyse gemaakt zijn en in geval van gerubriceerde documenten, encryptie worden toegepast. Uiteindelijk is elke organisatie zelf verantwoordelijk voor de continuïteit van de onder haar verantwoordelijkheid vallende vitale en essentiële processen en de afweging welke onderdelen voor welke tijd kunnen worden gemist.

Vraag 28
Kunt u deze vragen afzonderlijk en vooraf aan het commissiedebat «Digitaliserende overheid en toezicht» van 30 september 2026 beantwoorden?

Antwoord 28
Ja.