Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1541

BRIEF VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 3 juli 2026

Met deze brief informeer ik u, mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, over de herziening van het rijksbreed cloudbeleid die in de ministerraad van 3 juli jl. is vastgesteld. Bijgevoegd vindt u ook het herziene document. In deze brief informeer ik u over de aanleiding van de herziening, de belangrijkste aanscherpingen en de vervolgstappen.

Het gebruik van verschillende vormen van cloud binnen de rijksoverheid neemt toe. Mede naar aanleiding van twee onderzoeken,[1] gewijzigde geopolitieke verhoudingen en ontwikkelingen in de cloudmarkt is de noodzaak ontstaan om tot een herziening van het rijksbreed cloudbeleid te komen.

Het herziene rijksbrede cloudbeleid gaat uit van het huidige gebruik van clouddiensten door de rijksoverheid, en geeft richting door middel van een aantal aanscherpingen. Die aanscherpingen hebben betrekking op de uitbreiding van het aantal overheidsorganisaties die onder het cloudbeleid gaan vallen, een scherpere formulering voor de exit-strategie, een verdere beperking ten aanzien van de landen waar data mag worden verwerkt en een aantal toepassingen die niet langer van publieke cloud gebruik kunnen maken. Het is te voorzien dat door de zwaardere eisen organisaties (nog) niet direct aan het cloudbeleid zullen voldoen. Daarom bevat het cloudbeleid een overgangstermijn.

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

[1] Betreffende «Bevindingen onderzoeksopdracht «Evaluatie public cloudbeleid Rijksoverheid»» door de Auditdienst Rijk en het rapport «Het Rijk in de cloud» van de Algemene Rekenkamer.

kst-26643-1541
ISSN 0921 - 7371
's-Gravenhage 2026

IV-mogelijkheden en de huidige kaders van de departementale begrotingen. Hierdoor kan de implementatie langere tijd in beslag nemen, moeten scherpe keuzes gemaakt worden en moet waar nodig herprioritering plaatsvinden. De overgangstermijn geeft ook de kans om, waar mogelijk, te profiteren van het groeiende aanbod van soevereine cloudoplossingen.

Ik geef u hieronder een overzicht van de belangrijkste aanscherpingen in het beleid, een verwijzing naar de paragraaf waar dit in het cloudbeleid terug te vinden is en de overwegingen om deze aanscherping te doen.

Aanscherpingen

(Sectie 1) De werking van het cloudbeleid wordt aangepast. Het aangescherpte beleid zal gelden voor de gehele rijksoverheid, met uitzondering van de Hoge Colleges van Staat en het Ministerie van Defensie. Hoge Colleges van Staat en andere overheidsorganisaties wordt geadviseerd om het beleid te volgen.

(Sectie 1) Voor bestaand cloudgebruik dat nu niet voldoet aan de eisen van het herziene rijkscloudbeleid, geldt een overgangstermijn van 4 jaar na vaststelling van dit beleid. Bestaande overeenkomsten met een langere looptijd mogen gerespecteerd worden. In de gevallen waar migratie of aanpassing hoge kosten of risico's met zich meebrengen, mag de aanpassing of migratie worden ingepast op een logisch moment in de levenscyclus van de betrokken toepassing.

Deze overgangstermijn is ingevoerd om organisaties de gelegenheid te geven de aanpassingen en eventuele migraties goed in te passen in de bestaande meerjarenplannen. De overgangsperiode geeft ruimte aan de overheid en de markt om meer soevereine cloudvoorzieningen te realiseren. Op deze wijze worden desinvesteringen en verdringingseffecten op reeds geplande aanpassingen voorkomen.

(Sectie 3.1) Bij het maken van een integrale risicoafweging wanneer sprake is van materieel cloudgebruik wordt extra aandacht gevraagd voor de mogelijke risico's van een te grote leveranciersafhankelijkheid en die van andere jurisdicties. Dat laatste komt voor wanneer leveranciers (deels) onder een andere jurisdictie dan de Nederlandse of één van de EU of Europese Economische Ruimte (EER)-lidstaten valt.

(Sectie 3.2) De huidige exit-strategieën hebben vaak vooral betrekking op de eis dat een cloudleverancier bij een exit de data overhandigt en, na vertrek, deze zal vernietigen. In het herziene beleid wordt nu ook het opstellen van een meer gedetailleerd exitplan verplicht. Dit plan moet zowel betrekking hebben op een reguliere en geplande exit alsook op een situatie waarbij de clouddienst op korte termijn niet meer beschikbaar is of al uitgevallen is. Het gevraagde exitplan zorgt voor meer inzage in de benodigde doorlooptijd en kritische randvoorwaarden bij een exit. Het noodplan geeft inzage in de mate waarin een overheidsorganisatie in staat is bij verstoringen in de digitale keten toch te functioneren. Deze aanscherping past ook goed binnen de aanbevelingen van het rapport «Van kwetsbaar naar weerbaar».[2]

(Sectie 3.3) Materieel cloudgebruik en de bijbehorende risicoanalyse en exitplannen moet gemeld worden bij CIO Rijk. Deze centrale melding stelt CIO Rijk in staat haar monitorende rol ten aanzien van cloudgebruik en de daaruit voortkomende risico's uit te voeren. De uiteindelijke besluit-

[2] Rapport «Van Kwetsbaar naar Weerbaar»

vorming en acceptatie van risico's blijft de verantwoordelijkheid van de betrokken bewindspersoon of bestuurder van de overheidsorganisatie.

(Sectie 4) Bij gebruik van publieke cloud is opslag en verwerking beperkt tot de landen van de EER en worden data versleuteld (behalve wanneer het openbare data betreft). Daarmee beschouw ik de motie Rajkowski (VVD) als afgedaan.[3]

(Sectie 4.3) Voor kritieke en essentiële entiteiten, in het kader van respectievelijk de Wet weerbaarheid kritieke entiteiten en de Cyberbeveiligingswet, wordt afgeraden om voor de ondersteuning van de kerntaken afhankelijk te zijn van een leverancier die deels onder een andere jurisdictie dan de Nederlandse of een van de EU of EER-lidstaten valt. Daarmee wordt ook invulling gegeven aan de motie van de leden Thijssen (PRO) en Bruyning (NSC).[4]

(Sectie 4.5) Voor e-mail- en documentbeheer wordt afgeraden deze in de publieke cloud te verwerken. Bestaande publieke cloudoplossingen zullen, met een overgangstermijn, worden gemigreerd. E-mail en documenten bevatten een grote hoeveelheid overheidsinformatie die, zelfs wanneer individuele e-mails of documenten niet hoog gerubriceerd zijn, door de combinatie van hun inhoud en grote hoeveelheid toch een risico kunnen vormen. Daarnaast is de bedrijfsvoering vaak in grote mate afhankelijk van dit e-mail en documentbeheer. Met deze aanpassing beschouw ik de motie van de leden Kathmann (PRO) en Six Dijkstra (NSC) als afgedaan.[5]

(Sectie 4.6) Gebruik van publieke cloud voor verwerking van bijzondere persoonsgegevens wordt afgeraden en wanneer dit toch noodzakelijk is, moeten Privacy Enhancing Technologies worden toegepast.

(Sectie 5.2) Het gebruik van publieke clouddiensten blijft niet toegestaan voor staatsgeheime gerubriceerde informatie en voor te beschermen belangen (TBB) niveau 1 tot en met 3. Bij gebruik van externe leveranciers moeten deze voldoen aan de eisen van de Algemene Beveiligingseisen Rijksoverheid (ABRO 2026[6]).

(Sectie 5.4) Basisregistraties van de rijksoverheid mogen publieke cloud toepassen voor redenen van performance en schaalbaarheid. De brondata mogen niet in de publieke cloud worden beheerd. Daarmee blijft de beschikbaarheid van deze registraties in eigen hand.

Vooruitblik

De herziening van het rijksbreed cloudbeleid valt samen met meerdere trajecten in andere overheidslagen. Als verdere uitwerking van het herziene cloudbeleid zal het implementatiekader risicoafweging cloudgebruik van een update worden voorzien. Daarnaast is het de ambitie om te komen tot een integraal afwegingskader risicobeoordeling voor digitale diensten. De uitvoeringsorganisaties zullen betrokken worden bij de herziening van het implementatiekader om hun perspectief voldoende mee te wegen.

Daarnaast wil ik op korte termijn met de medeoverheden aan de slag om te komen tot een overkoepelend overheidsbreed cloudbeleid. De problematiek en uitdagingen op het niveau van gemeenten, provincies en

---

[3] Kamerstukken II 2022/23, 26 643, nr. 975.
[4] Kamerstukken II 2024/25, 36 574, nr. 13.
[5] Kamerstukken II 2024/25, 36 740 VII, nr. 20.
[6] https://open.overheid.nl/details/a13699d9-fcf4-43ef-b282-ece9519e9b81/

waterschappen is immers niet anders. Een overkoepelend overheidsbreed cloudbeleid draagt bij aan verdere standaardisatie binnen de overheid, wat weer bevorderlijk is voor een gelijk beschermingsniveau, mogelijkheden tot bundeling van inkoopkracht en de rol van de overheid als «launching customer».

Daarnaast zal de impact van EU-regelgeving, zoals voorgesteld in de Cloud and AI Development Act (CADA) ook een impact hebben op het toekomstige beleid. Voor wat betreft het CADA is 26 juni jl. een BNC-fiche gepubliceerd.[7]

De Staatssecretaris van Economische Zaken en Klimaat,
W.J.M. Aerdts

[7] Kamsterstukken 2025/26, 22 112, nr. 4395