



> Retouradres Postbus 20011 2500 EA Den Haag

Algemene Rekenkamer
t.a.v. president drs. P.J. Duisenberg
Postbus 20015
2500 AE Den Haag

Turfmarkt 147
2511 DP Den Haag

Onze referentie
2024-0000917309

Uw referentie

Datum 9 december 2024
Betreft Onderzoek AR – Het Rijk in de cloud

Geachte heer Duisenberg,

Allereerst wil ik u danken voor het voorliggende rapport van de Algemene Rekenkamer (AR) naar aanleiding van het onderzoek 'Het Rijk in de cloud' naar het public cloudgebruik bij de Rijksoverheid. Het rapport levert mij belangrijke inzichten in de wijze waarop de Rijksoverheid de public cloud inzet en wat daarin verbeterd kan worden.

U beoordeelt het public cloudgebruik door de rijksoverheid als zorgelijk. Ik deel uw zorgen: burgers en bedrijven moeten erop kunnen vertrouwen dat de overheid zorgvuldig omgaat met hun gegevens en betrouwbaar haar taken uitvoert. Het inzetten van public cloud is daarbij, met de juiste afwegingen, van belang voor het functioneren van de overheid. Dit heeft hiermee ook mijn volle aandacht. Met dit rapport kan ik beter sturen op het benutten van kansen en met name op het beheersen van risico's rondom public cloudgebruik zoals betrouwbaarheid van verwerkingen of digitale autonomie. Hieronder geef ik aan op welke wijze ik actie ga nemen naar aanleiding van uw rapport.

Strekking van het onderzoek

Uw onderzoek geeft inzicht in het cloudgebruik door het Rijk en of het Rijk de voorwaarden die zijn opgenomen in het 'Rijksbreed cloudbeleid 2022' en het 'Implementatiekader risicoafweging cloudgebruik' in voldoende mate heeft geïmplementeerd. Daarbij heeft u ook meegewogen in hoeverre de soevereiniteit, continuïteit van de dienstverlening en gegevensbescherming gewaarborgd zijn.

Het onderzoek is in twee fases uitgevoerd. In de eerste fase is een inventarisatie binnen de hele rijksoverheid uitgevoerd, met twee meetmomenten, over het gekende cloudgebruik. In de tweede fase zijn drie grote cloudcontracten nader onderzocht.

Het rapport laat zien dat de rijksoverheid veelvuldig gebruik maakt van public clouddiensten, en tegelijkertijd dat op alle onderzochte gebieden nog stappen gezet moeten worden: het inzicht in het cloudgebruik is niet volledig, risicobeheersing (analyse en maatregelen) is nog onvoldoende, sturing en toezicht zijn nog niet toereikend en ook het beleid kent verbeterpunten. Dit alles leidt tot risico's met betrekking tot (digitale) autonomie, continuïteit van de dienstverlening

en gegevensbescherming¹. Uw overall conclusie is dat het cloudgebruik door de rijksoverheid zorgelijk is.

Algemeen beeld

Ik deel het inzicht dat de beheersing van het cloudgebruik verbetering nodig heeft. Het cloudbeleid van de rijksoverheid is met twee jaar relatief jong. Ik constateer dat overheidsorganisaties de mogelijkheid om public clouddiensten in te zetten toegepast hebben, maar dat dit nog niet altijd (volledig) conform het beleid plaatsvindt. U constateert dat het tweede meetmoment al een verbetering heeft getoond. Hoewel er ook sprake is van clouddiensten die reeds in gebruik waren voordat het beleid vastgesteld werd, is de achterstand te groot.

Zoals u ook in het rapport schrijft kan de cloud voordelen bieden zoals efficiëntie, flexibiliteit, schaalbaarheid en veiligheid. Dit kan dienstverlening verbeteren of bedrijfsvoering efficiënter maken.

Uw bevindingen, conclusies en adviezen sluiten nauw aan op mijn eigen evaluatie, met daarin meegenomen het onderzoek van de Auditdienst Rijk (ADR). Deze evaluatie heb ik op 16 oktober 2024 met de Tweede Kamer gedeeld².

Ik neem uw adviezen mee in de verbeteringen in en herzieningen van het Cloudbeleid en het implementatiekader, de besturing en de dagelijkse praktijk. Dit is een traject waarop ik centraal acties uitzet. Daarnaast moeten ook alle departementen en hun onderdelen met deze acties aan de slag gaan, onder aansturing van de eigen politieke en ambtelijke leiding.

Alle departementen en hun onderdelen: Verbetering operatie: meer inzicht en betere risicobeheersing

U constateert dat het inzicht in en de risicobeheersing van het cloudgebruik nog onvoldoende zijn. De inventarisaties door de departementen en hun onderdelen zijn nog niet volledig waardoor belangrijke inzichten ontbreken. Evenmin delen de onderdelen in alle gevallen deze inventarisaties met hun departement en inventarisaties van materieel public cloudgebruik met CIO rijk. Daarnaast ontbreken in veel gevallen vastgestelde risicoanalyses. Mede daardoor blijven de getroffen maatregelen achter.

De operationele beheersing valt onder de ministeriële verantwoordelijkheid van de desbetreffende departementen. U constateert dat tussen de twee meetmomenten al verbetering was opgetreden. Ik zal met mijn collega's actie nemen om de ingezette inhaalslag te versterken en zo het departementaal inzicht in het cloudgebruik te verbeteren en te komen tot betere departementale risicobeheersing. Ik zal dit centraal ondersteunen. Meer zicht op individuele risico's geeft ons vervolgens ook de mogelijkheid te sturen op departement-overstijgende

¹ De ARK verstaat dit onder gegevensbescherming: *'Voldoende bescherming van de gegevens. Bij de public cloud ligt het eigenaarschap van software en hardware en soms ook gegevens meestal niet bij de overheidsorganisatie zelf. Beschikbaarheid, vertrouwelijkheid en integriteit van de gegevens zijn dan belangrijk.'* Dit is anders dan gegevensbescherming zoals in de AVG gehanteerd wordt.

² [Kamerbrief evaluatie Rijksbreed cloudbeleid | Kamerstuk | Rijksoverheid.nl](#)

risico's en dit bijvoorbeeld mee te nemen in het onderzoek naar digitale autonomie.

Uw bevindingen en aanbevelingen nemen we ook mee voor cloudgebruik dat in voorbereiding is. Dit geldt bijvoorbeeld voor de door u onderzochte werkplekdiensten van SSC-ICT: die zijn nu nog nagenoeg volledig on-premises. SSC-ICT vernieuwt haar werkplekdiensten. Hierbij zullen geen onomkeerbare stappen worden gezet conform de afspraken met Kamer hierover. Voor al het gepland cloudgebruik geldt steeds dat vooraf passende en formele risico-mitigatie plaatsvindt.

Invoering van de Algemene Beveiligingseisen Rijksoverheid Opdrachten (ABRO)³ zal ook bijdragen aan het beter mitigeren van risico's van cloudgebruik. Dit stelt standaard meer eisen aan de dienstverlening en de leverancier zelf en ook wordt standaard onderzocht of de dienstverlening en leverancier hieraan voldoen.

MinBZK en de departementen: Verbetering besturing en toezicht

Omdat de operationele beheersing achterblijft, adviseert u om minder vrijblijvend te sturen en beter toezicht te houden.

Ik onderschrijf dat de operationele verbetering ook meer besturing en toezicht vereisen. Om te sturen op de voortgang van de operationele verbetering heb ik maatregelen genomen om mij periodiek te laten informeren over de stand van zaken door CIO Rijk. Waar nodig zal ik samen met mijn collega's bijsturen. Tevens zal ik inzetten op meer samenhang tussen onderdelen van de overheid waar dit nationale belangen of veiligheid raakt. CIO Rijk zal hierin een coördinerende en faciliterende rol vervullen zodat de CIO's binnen de rijksoverheid kunnen sturen op te nemen verbeterstappen.

MinBZK: Verbetering beleid en uitbreiding scope

Hoewel veel van voorgaande bevindingen opgelost worden door het volledig volgen van het cloudbeleid en implementatiekader, ziet u ook verbeteringsmogelijkheden in het beleid door het beleid uniformer en concreter te maken. De hoofdlijn daarin is om minder verschillen te laten ontstaan tussen de departementale cloudbeleidsstukken, de scope uit te breiden naar de gehele overheid, waaronder de medeoverheden en zbo's, en om bepaalde overheidsdiensten specifiek uit te sluiten van cloudgebruik.

Ik sta voor de één overheidsgedachte en ik wil de medeoverheden en zbo's betrekken in de vernieuwing van het cloudbeleid, en te komen tot één cloudbeleid voor de gehele overheid. Deze gedachte wordt ook meegenomen in de Nederlandse Digitaliseringsstrategie (NDS), welke momenteel uitgewerkt wordt.

Ik sta in beginsel positief tegenover het concreter en uniformer maken van het beleid. Dit sluit ook aan op mijn eigen evaluatie. In de komende herziening van het rijksbrede public cloudbeleid zal ik deze punten meenemen. Het beperken van verschillen tussen de departementale beleidstukken en het uitsluiten van specifieke diensten zijn waardevolle adviezen. Op strategisch beleidsniveau is veel

³ Zie kamerstukken 36471-96, pag. 98 en 26 643; 30 821 Nr. 1215

uniformiteit mogelijk. Tegelijkertijd zijn er duidelijke operationele verschillen tussen de rijksorganisaties die leiden tot verschillende functionele behoeften in het cloudgebruik. Daarnaast zijn er meerdere manieren om operationeel goede risicobeheersing uit te voeren. Daar moet ruimte voor blijven. Een one-size-fits-all benadering kan passen op strategische niveau maar niet altijd op operationeel niveau. Het vinden van de juiste balans tussen blijft dus van belang.

MinBZK en departementen: Verbeteren samenwerking inkoop en contractbeheer

U constateert dat Strategisch Leveranciersmanagement (SLM) onvoldoende geraadpleegd wordt en dat de contractuele afspraken complex zijn. U adviseert om meer gezamenlijk in te kopen met daarbij een centrale rol voor SLM en hierbij ook samenwerking in EU-verband op te zoeken.

Ik onderschrijf het belang om meer samen te werken bij inkoop en daarbij de rol en positie van SLM te versterken met bijvoorbeeld een gedeeld expertisecentrum en (externe) specialistische dienstverlening. Dit leidt ook tot een set met formele afspraken, een logische opbouw en hiërarchie, minder contracten en dus minder complexiteit. Een gebalanceerde en dekkende maatregelenset (technisch, interne procedures, afspraken met toeleverancier etc.) draagt bij aan het beter borgen van de autonomie, continuïteit en gegevensbescherming. Samenwerken maakt het mogelijk om hierin effectiever in op te treden.

Met de EU is contact over samenwerking en die zullen we ook hiervoor inzetten. We werken op diverse gebieden samen, waaronder cloud en onderzoeken naar Europese cloudinitiatieven.

Ik nodig u graag uit om over de aanpak en opvolging van uw bevindingen in gesprek te gaan.

Hoogachtend,
De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
Digitalisering en Koninkrijksrelaties

Zsolt Szabó