Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 904

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 augustus 2022

Met deze brief informeer ik u over het Rijksbrede cloudbeleid 2022; een uitwerking van de nieuwe visie op gebruik van *publieke* clouddiensten door de rijksoverheid. Dit beleid vervangt het eerdere beleid uit 2011, waarin nog gestreefd werd naar gebruik van *private* clouddiensten (Kamerstuk 26 643, nr. 179). Gebruik van publieke clouddiensten biedt potentiële voordelen, er zijn echter ook risico's die beheerst moeten worden. Op beide ga ik in deze brief in. In de bijlagen vindt u een duiding van hetgeen verstaan wordt onder (publieke) clouddiensten en de eerdere beleidsontwikkelingen op dat terrein.

Rijksbreed cloudbeleid 2022

Onder het nieuwe beleid mogen overheidsdiensten, met enkele uitzonderingen, onder voorwaarden publieke clouddiensten gebruiken. Deze uitzonderingen en voorwaarden worden hieronder uitgewerkt.

In de eerste plaats gelden voorwaarden voor de verwerking van persoonsgegevens in publieke clouddiensten. Dit vergt een goedgekeurde pre-scan gegevens-beschermingseffectbeoordeling (ook wel pre-scan DPIA genoemd). Bij hoog risico wordt een volledige data protection impact assessment (of formele DPIA) uitgevoerd, waarin zowel de verwerking zelf als de geldende grondslagen, de aard van de verwerking en de bijbehorende risico's en maatregelen zijn beschreven. Dit geldt ook bij verwerking van gegevens in een publieke cloud. Elk departement is zelf verantwoordelijk om de relevante risico's van het gebruik maken van een publieke cloud toepassing in beeld te hebben en tijdens het gebruik in beeld te houden. Op basis van deze risicoafweging kan de betreffende Minister voor tot en met departementaal vertrouwelijk gerubriceerde informatie besluiten tot gebruik van de publieke cloud. Voor die risicoafweging zal door de CIO Rijk met de departementale CIO's voor het einde van 2022 een «implementatierichtlijn risicoafweging cloudgebruik» worden opgesteld, mede op basis van de Baseline Informatiebeveiliging Overheid.

kst-26643-904
ISSN 0921 - 7371
's-Gravenhage 2022

Hiermee kan de departementale CIO-office bij gebruik van een clouddienst desgevraagd aan CIO Rijk een gegevensbeschermingseffectbeoordeling met daarin een samenhangende risicoanalyse overhandigen. Dit past binnen de bestaande coördinerende verantwoordelijkheid en het instrumentarium van CIO Rijk. Hetzelfde geldt voor interne en externe verantwoording aan de Auditdienst Rijk en de Algemene Rekenkamer.

Onderdelen van de overheid die niet tot de Rijksdienst behoren wordt geadviseerd om dit Rijksbeleid te volgen. Aan de departementen wordt gevraagd dit voor de onder hun Minister vallende ZBO's en eventueel andere organisaties te stimuleren.

Uitzonderingen

- Het gebruik van publieke clouddiensten is *niet toegestaan* voor staatsgeheim gerubriceerde informatie;
- Het Ministerie van Defensie valt buiten de scope van dit beleid.

Voorwaarden voor het gebruik van publieke cloud voor overheidsdiensten

Onder het Rijksbrede cloudbeleid 2022 gelden voor het gebruik van publieke cloud voorzieningen de volgende voorwaarden:

1. Departementaal beleid

Op basis van het Rijksbrede cloudbeleid 2022 formuleren alle departementen hun eigen cloudbeleid en cloudstrategie. Onderdelen van de overheid die niet tot de Rijksdienst behoren wordt geadviseerd om dit ook te doen. In overeenstemming met hun wettelijke taak houden Algemene Rekenkamer (ARK) en Auditdienst Rijk (ADR) hierop toezicht en monitort CIO Rijk de implementatie conform het Besluit CIO stelsel.

2. Risicoafweging

Publieke clouddiensten mogen worden gebruikt op basis van een in een gegevensbeschermingseffectbeoordeling opgenomen relevante risicoafweging, waartoe CIO Rijk een implementatierichtlijn ontwikkelt. Besluitvorming door de verantwoordelijke Minister moet toetsbaar en auditeerbaar zijn.

3. Gekend gebruik

Vanuit de verplichting tot het bijhouden van materieel publieke cloudgebruik en de risico's daarvan rapporteren departementen jaarlijks over verwerking van persoonsgegevens in een publieke cloud aan CIO Rijk. Een proces daarvoor zal worden geformuleerd in de implementatierichtlijn.

4. Exit strategie

Er dient altijd een «exit strategie» opgenomen te zijn in de overeenkomst met de cloudleverancier. Hierin staat hoe, bij beëindiging van de overeenkomst, data worden overgedragen en hoe wordt geregeld dat de verzameling data bij de leverancier vernietigd wordt.

5. Voldoen aan eisen voor ICT-dienstverlening

Alle typen clouddienstverlening, dus ook publieke, moeten allereerst voldoen aan de bestaande voorwaarden voor ICT-dienstverlening (zie hiervoor de bijlage). Risico's moeten bekend en voldoende gemitigeerd

zijn en blijven. De verantwoordelijk Minister moet zich hiervan verzekeren en dit kunnen aantonen. Dat gebruik wordt gemaakt van een publieke cloud toepassing en de bijbehorende risicoanalyse dienen onderdeel te zijn van een gegevensbeschermingseffectbeoordeling. Elk departement moet weten voor welke verwerkingen dit het geval is. 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 taak van een organisatie. Met andere woorden, voor de organisatie is die (cloud-)dienst van wezenlijk belang.

6. Toegespitste risicoanalyse

Bij verwerving of uitbesteding van activiteiten aan clouddienstverleners zijn specifieke risico's van toepassing vanwege marktconcentratie en politieke en geografische spreiding van gegevensverwerkingen. De risicoanalyse per inzet van materieel cloudgebruik voor overheidsdiensten betreft ten minste (dit zal verwerkt worden in de op te stellen implementatierichtlijn):

- De karakteristieken van gebruik van de clouddienst, zoals de (hoofd-) dienstverlener en eventuele onder-dienstverleners, het type dienstverlening (publieke/private/hybride/community cloud), de geografische regio van verwerking en opslag van gegevens.
- Hoe geregeld is dat de dienstverlener controle en verantwoordingsonderzoeken toelaat of daarover rapporteert; er bestaat een «right-to-audit» voor de opdrachtgevende organisatie of er is hierover contractueel voldoende zekerheid via Strategisch Leveranciers Management (SLM)

7. Cyberveiligheid

Cyberveiligheid verdient apart aandacht, mede omdat ook statelijke actoren zoals Rusland en China zijn geïnteresseerd in informatie die in Nederland te verkrijgen is. Bij gebruik van publieke cloud diensten ontstaat veelal gegevensverwerking in andere landen, waaronder soms ook in landen buiten de Europese Unie. Vanwege de wetgeving in die landen ontstaan vragen over de veiligheid van de informatie. We hanteren bij het cloudgebruik daarom ook de C2000 criteria[1], waardoor leveranciers of diensten uit landen met een actief cyberprogramma dat gericht is tegen Nederlandse belangen worden uitgesloten. Mocht er een risico zijn op dreiging van statelijke actoren, wordt voortijdig dreigings- en beveiligingsadvies ingewonnen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en/of Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Voor het overige sluiten we ons aan bij het Europese beleid op dit terrein dat waarborgen biedt tegen misbruik van de informatie die in een cloud is opgeslagen.

8. Openbaarheid

In het licht van de Wet Open Overheid (WOO)[2] wordt uitgegaan van openbaarmaking van de besluitvorming door de eigenaar, waaronder de besluitvorming over de gegevensbeschermingseffectbeoordelingen (DPIA's) en, indien van toepassing, adviezen van de Privacy Adviseur Rijk (PAR).

---

[1] Kamerstuk 25 124, nr. 96

[2] wetten.nl – Regeling – Wet open overheid – BWBR0045754

9. Opslag en verwerking van persoonsgegevens

Alle opslag en verwerking van persoonsgegevens vindt plaats conform geldende privacy-vereisten uit de AVG. Eén van de onderdelen van de AVG is het voldoen aan vereisten inzake doorgiften van persoonsgegevens (hoofdstuk V van de AVG), en daarbij wordt voldaan aan één van de onderstaande eisen:

a. opslag en verwerking binnen de Europese Economische Ruimte (EER), of
b. in landen waarvoor een adequaatheidsbesluit bestaat, of
c. op basis van een passend doorgiftemechanisme dat voldoet aan de vereisten (van art. 46, hoofdstuk V) van de AVG, zoals een modelcontract (standaard contractbepalingen of «standard contractual clauses»

Indien niet aantoonbaar aan één van die eisen (9.a 9.b of 9.c) is voldaan, dan wordt voor die verwerking en alle daarbij behorende subverwerkingen de uitgevoerde (pre-scan of formele) DPIA zo spoedig mogelijk na vaststelling aan CIO Rijk toegezonden. CIO Rijk gebruikt deze als aanvulling op de jaarlijkse rapportages in zijn monitorende verantwoordelijkheid en neemt de uitkomsten mee in de jaarlijkse cyclus van CIO gesprekken.

10. Bijzondere persoonsgegevens

Bijzondere persoonsgegevens hebben extra bescherming nodig, en daarom geldt daarvoor een zwaardere beleidsverplichting. Voor deze gegevens wordt **in principe géén** gebruik gemaakt van publieke cloudvoorzieningen, tenzij aantoonbaar aan eisen (9.a. of 9.b) is voldaan. Uitzonderingen hierop die voldoen aan 9.c zijn mogelijk op basis van «pas-toe-of-leg-uit» (comply or explain).
Indien aan eis 9.c wordt voldaan of in alle andere situaties, dan wordt de explain die minimaal de uitgevoerde (pre-scan of formele) DPIA bevat, zo spoedig mogelijk na vaststelling aan CIO Rijk toegezonden. CIO Rijk gebruikt deze als aanvulling op de jaarlijkse rapportages in zijn monitorende verantwoordelijkheid en neemt de uitkomsten mee in de jaarlijkse cyclus van CIO gesprekken.

11. Basisregistraties

In geval van de opslag en verwerking van een *basisregistratie* [3], of een bron van een basisregistratie wordt, **in principe géén** gebruik gemaakt van publieke cloudvoorzieningen. Uitzonderingen hierop zijn mogelijk op basis van «pas-toe-of-leg-uit» (comply or explain).
Indien (bronnen van) basisregistraties in de publieke cloud worden verwerkt of opgeslagen, dan wordt de explain die een risicoanalyse bevat of die bij persoonsgegevens minimaal de uitgevoerde (pre-scan of formele) DPIA bevat, *door de eigenaar van de bronregistratie* vooraf aan CIO Rijk toegezonden zodat zijn advies kan worden meegenomen in de besluitvorming.
Het advies van de CIO rijk betreft een professionele inschatting en neemt geen verantwoordelijkheid weg van de beslisser.
Voor de afnemers van basisregistraties gelden de reguliere eisen voor verwerking in publieke cloudvoorzieningen zoals opgenomen in dit document. Voor zover het daarbij gaat om (bijzondere) persoonsgegevens uit een basisregistratie gelden ook de voorwaarden zoals bij 9. en 10. geformuleerd.

Samengevat in een tabel zegt het voorgaande:

---

[3] Stelsel van basisregistraties – Digitale Overheid

Soort Gegevens	Verantwoordelijke[1]	Advies CIO rijk	In Publieke cloud?	Besluit door	Toezicht
Staatsgeheime informatie	Eigenaar	geen advies	Nee	–	Diverse toezichthouders, waaronder departementale Beveiligingsautoriteit[2] (BVA)
Persoonsgegevens	Eigenaar	advies, indien nodig[3]	Ja, mits voldaan aan eis 9.a, 9.b of 9.c	Departementale Bestuursraad of gedelegeerde	Functionaris Gegevens bescherming en departementale CIO
Bijzondere Persoonsgegevens	Eigenaar	advies, indien nodig[3]	Nee, tenzij voldaan aan eis 9.a of 9.b of aan eis 9.c met explain	Departementale Bestuursraad of gedelegeerde	Functionaris Gegevens bescherming en departementale CIO
Basis registratie	Eigenaar, of eigenaar in het departement in geval van een Zelfstandig Bestuursorgaan (ZBO)	advies vooraf	Nee, tenzij met explain	Departementale bestuursraad	Departementale CIO

[1] Dit betreft de procesverantwoordelijke, niet de verwerkingsverantwoordelijke
[2] Stcrt. 2020, nr. 62845 Besluit BVA-stelsel Rijksdienst 2021
[3] Vanuit de monitorende rol

Naast deze bovengenoemde verantwoordelijkheden hebben de Autoriteit Persoonsgegevens (AP), de ADR en de ARK wettelijke toezichtsverantwoordelijkheden.

Tot slot

Ik ben voornemens om extra aandacht te vragen van de departementen voor verantwoording over de risicoanalyses en bescherming van persoonsgegevens, via vraaggestuurd onderzoek van de ADR. Daarnaast zeg ik toe, als onderdeel van de controle op het beleid, om vanaf 2023 (te starten één jaar na publicatie van) het Rijksbreed Cloudbeleid 2022 te evalueren en over de voortgang van de implementatie te rapporteren om daarmee uw Kamer de gelegenheid te geven om nadere vragen te stellen.

Ik zal de uitwerking van het cloudbeleid opvolgen via de rapportages over de I-strategie Rijk, zowel vanuit het perspectief van versterken van de digitale weerbaarheid alsook het bestendigen van het ICT-landschap, respectievelijk thema 2 en 3 uit de I-strategie Rijk 2021–2025. Tevens kan ik u desgewenst over dit thema in een technische briefing nader laten informeren.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen

Bijlage

Uw Kamer vroeg het Kabinet in de motie Van der Burg[4] c.s. op 20 mei 2010 om een cloudstrategie. Doel hiervan was om, in navolging van diverse andere landen een strategie voor de hele Nederlandse overheid te ontwikkelen voor cloud computing. Onderdeel hiervan was ook een «cloud first» strategie, waarin mogelijkheden voor de inrichting van een overheidscloud duidelijk waren omschreven. Met bijbehorende voor- en nadelen. Daarbij moesten ook de veiligheidsrisico's en afhankelijkheidsrisico's in beschouwing worden genomen.

Het kabinet koos destijds voor een strategie op basis van een «gesloten» (=»private») Rijkscloud».[5] Reden hiervoor was dat – op dat moment – de argumenten tegen het toepassen van «publieke[6]» cloud computing zwaarder wogen dan de voordelen. Deze Rijkscloud zou gerealiseerd worden als onderdeel van het Uitvoeringsprogramma Compacte Rijksdienst.
In de kabinetsreactie op het Eindrapport van de Tijdelijke commissie ICT-projecten[7] (Commissie Elias) vulde het kabinet de cloudstrategie van het Rijk verder in. Een citaat uit deze brief luidt als volgt:

«Ik kies er daarom voor, op basis van de cloudstrategie, om een Rijkscloud in te richten als een voorziening die ICT-diensten, gebaseerd op cloudtechnologie, levert voor de ondersteuning van de primaire en secundaire processen binnen de Rijksdienst. Deze voorziening wordt ingericht binnen een exclusief voor het Rijk beschikbaar beveiligd netwerk.»

De private Rijkscloud is uiteindelijk niet gerealiseerd, omdat geen gemeenschappelijke behoeftestelling heeft plaatsgevonden. Wel zijn er bij verschillende ministeries en uitvoeringsorganisaties zelfstandige private cloudoplossingen in gebruik genomen. De markt voor publieke clouddiensten heeft het afgelopen decennium echter een grote ontwikkeling doorgemaakt, versneld door de Covid-pandemie. Diensten zijn betrouwbaarder geworden en worden op zeer grote schaal door burgers en bedrijven gebruikt. Ook zijn de veiligheidsmogelijkheden uitgebreid en geeft de grootschalige uitrol van updates en patches de mogelijkheid veel sneller te reageren op fouten in software dan in het verleden.
Daarom is het hoog tijd om het Rijksbrede cloudbeleid uit 2011 te herzien.

In deze toelichting wordt u meegenomen in de brede context: er wordt uitgelegd wat clouddiensten zijn, wat het verschil is tussen breed gebruikte begrippen publieke (publieke) en private cloud en wat de ontwikkelingen binnen de rijksoverheid zijn geweest sinds 2011. Vervolgens worden beleidsontwikkelingen in het buitenland aangegeven. Voordelen en risico's worden besproken voordat het beleid wordt geformuleerd.

Wat is de cloud? Wat zijn clouddiensten?

Er zijn meerdere manieren om diensten van ICT-voorzieningen (bijv. netwerken, servers, opslag, applicaties) af te nemen. De term cloud is een verzamelnaam voor een aantal variaties daarvan. Wat de cloud in belangrijke mate onderscheidt van andere manieren, is dat een afnemer

---

[4] Kamerstuk 26 643, nr. 157
[5] Kamerstuk 26 643, nr. 179
[6] In de brief werd gesproken over «open» en «gesloten» cloud, die thans algemeen bekend staan als «publieke» en «private» cloud oplossingen.
[7] Kamerstuk 33 326, nr. 13

zelf (zonder menselijke interactie met de leverancier) de voorzieningen kan afnemen[8].

De cloud komt in verschillende modellen. De twee uitersten zijn de publieke cloud en de private cloud. Bij de publieke cloud worden de computermiddelen aangeboden door een commerciële partij. Zowel de rijksoverheid als andere bedrijven en particulieren kunnen een deel van die middelen op hetzelfde platform afnemen.

Als één overheidsorganisatie toegang heeft tot computermiddelen, dan spreken we van een private cloud. Een private cloud kan in beheer zijn van de rijksoverheid zelf of exclusief door een marktpartij worden aangeboden.

Een mengvorm van de private en publieke cloud heet een hybride cloud. Een hybride cloud is opgebouwd uit meerdere delen, waarvan sommige in een publieke en sommige in een private cloud zijn ondergebracht. Om goed overzicht te houden op de informatie in dat samenspel van diensten wordt een informatiearchitectuur gebruikt.

Ontwikkelingen binnen de overheid sinds 2011

In de Kamerbrief uit april 2011[9] stelde het kabinet vast dat dat de argumenten tegen het toepassen van publieke cloud computing op dat moment globaal zwaarder wogen dan de voordelen. Deze argumenten hadden te maken met de toenmalige onvolwassenheid van de markt en de gestelde eisen aan informatiebeveiliging.

Het aanbod van publieke cloud computing (met voor de overheid toepasbare ICT-oplossingen) was toen nog beperkt. Het aantal leveranciers en clouddiensten was vrij groot, maar slechts een klein deel daarvan was bedrijfsmatig volwassen genoeg om ingezet te kunnen worden voor de Nederlandse overheid.
De publieke cloud toepassingen kwamen nog niet tegemoet aan de specifieke wensen en verantwoordelijkheden van de Nederlandse overheid. Dit was ook de ervaring van andere landen.

Qua informatiebeveiliging bleek dat de risico's van publieke clouddienstverlening nog niet voldoende konden worden afgedekt. Zo was privacybescherming nog geen integraal onderdeel van publieke cloudtoepassingen. Het kabinet richtte zich daarom destijds voornamelijk op een gesloten Rijkscloud in eigen beheer.

Intussen heeft de markt voor de publieke cloud zich verder ontwikkeld en wordt het breed toegepast. Volgens het Centraal Bureau voor de Statistiek (CBS) maakte in 2020 53% van de Nederlandse bedrijven gebruik van de

---

[8] De breed gedragen definitie van het National Institute of Science and Technology (NIST) luidt: Cloud computing is een model om op afroep op een gemakkelijke manier via een netwerk toegang te krijgen tot een gedeelde verzameling van configureerbare computer resources (bijvoorbeeld netwerken, servers, opslag, applicaties en diensten) die snel kunnen worden geleverd en vrijgegeven met minimale inspanning of interactie met leveranciers.
Cloud computing heeft vijf essentiële karakteristieken:
- On-demand selfservice: naar behoefte verkrijgbaar zonder menselijke interactie met de leverancier
- Breed beschikbare netwerktoegang: te gebruiken via een gestandaardiseerde netwerkverbinding
- Gedeelde resources: computermiddelen worden gedeeld door verschillende afnemers
- Snelle elasticiteit: gebruik is snel op en af te schalen. Beschikbare computermiddelen lijken onbeperkt
- Afgemeten dienstverlening: het verbruik is meetbaar, transparant en eenduidig

[9] Kamerstuk 26 643, nr. 179

cloud en 39% van gedeelde servers (publieke cloud)[10]. Ook bedrijven die hoge eisen stellen aan beveiliging en privacy gebruiken de cloud. In de financiële sector heeft DNB een pioniersrol gespeeld in de beheersing van risico's van cloudoplossingen. Inmiddels maakt 49% van de banken gebruik van de cloud en 38% van de publieke cloud. In de gezondheidszorg maakt 59% van de bedrijven gebruik van de private cloud en 43% van de publieke cloud.

Extern onderzoek stelde in 2019 vast[11] dat meer dan 50% van de overheidsorganisaties wereldwijd gebruik maakt van office pakketten uit de cloud. Beleidsmatig lijken landen wereldwijd steeds meer open te staan voor publieke cloudtoepassingen.
Al deze ontwikkelingen in de markt zien we ook terug in het rijksbeleid.

In 2016[12] werd in de Strategische I-Agenda Rijksdienst aangegeven dat de inzet van clouddienstverlening bij externe leveranciers tot de opties behoort. Er is echter niet ingegaan op het onderscheid tussen de publieke en private cloud. Daarnaast werd het oude standpunt niet expliciet herzien. Dit blijkt in de praktijk onduidelijkheid te creëren, die met het nieuwe beleid wordt weggenomen.

Ook rond privacy van publieke clouddienstverlening zijn belangrijke stappen gezet. Met de invoering van de AVG moeten ook internationale publieke clouddienstverleners zich houden aan dezelfde privacyregels als ze hun diensten in Europa aanbieden. Dankzij de inzet van het Strategisch Leveranciers Management Rijk in 2019[13], 2020[14] en 2021[15] wijzigt Microsoft haar productaanbod en wordt langzaam duidelijk dat de inzet van publieke clouddiensten vanuit AVG-perspectief geen onoverkomelijke problemen hoeft op te leveren

Het Strategisch Leveranciers Management Rijk is voornemens om ook het gebruik van oplossingen van andere leveranciers (zoals Amazon Web Services – AWS en Google Cloud) binnen de rijksoverheid, in overeenstemming met de AVG mogelijk te maken[16]. Hieruit concluderen we dat de beleidslijn van het Rijk de inzet van publieke clouddiensten niet bij voorbaat uitsluit vanuit het oogpunt van privacy. In lijn hiermee bent u recent geïnformeerd over de overeenkomst met Google om in overeenstemming met privacy vereisten, van Google Workspace in de Google cloud gebruik te maken[17].

Sinds 1 januari 2019 vervangt de Baseline Informatiebeveiliging Overheid (BIO) de specifieke baselines voor Rijk Gemeenten, Waterschappen en Provincies. Met de BIO hanteert de overheid een uniform kader voor informatiebeveiliging. We constateren dat de BIO de inzet van publieke clouddiensten niet bij voorbaat uitsluit. Wel is het mogelijk dat met behulp van de BIO eisen aan de beschikbaarheid of vertrouwelijkheid van informatie worden gesteld, waar de beveiliging van een publieke clouddienst niet aan kan voldoen. Daarom moet de inzet van publieke clouddiensten per situatie worden beoordeeld.

---

[10] https://opendata.cbs.nl/statline/#/CBS/nl/dataset/84832NED/table?ts=1621458057248
[11] https://www.gartner.com/en/newsroom/press-releases/2019-08-28-gartner-2019-hype-cycle-shows-cloud-office-has-hit-ma
[12] Kamerstuk 31 490, nr. 221
[13] Kamerstuk 32 761, nr. 622
[14] memo «Stand van Zaken Microsoft augustus 2020»
[15] memo «Audit op Microsoft»
[16] Zie memo «Stand van zaken Google»
[17] Kamerstuk 26 643, nr. 859

Beleidsontwikkeling in het buitenland

Landen gaan verschillend om met publieke cloudtoepassingen. Er lijkt een trend zichtbaar waarbij landen beginnen met een focus op de private cloud en in de loop van de tijd steeds meer overstappen op de hybride of publieke cloud. Die overstap kent meerdere variaties. Sommige overheden zien de publieke cloud als één van de opties (bijv. Frankrijk, lerland, Zwitserland). Andere overheden zien de publieke cloud (al dan niet hybride) als de voorkeursoptie (Australië, Canada, Italië, Malta, Vlaanderen, lJsland, Singapore, Verenigd Koninkrijk). Vooral het Verenigd Koninkrijk is al jarenlang koploper in de inzet van publieke cloudtoepassingen bij overheidsorganisaties. Zij werken er al sinds 2012 mee. Hun aanpak diende als blauwdruk voor landen als Australië en Canada.

Ook op EU-niveau zien we aandacht voor de voordelen van cloudtechnologie. De Europese Commissie erkent de voordelen die cloudtechnologie heeft rond kostenreductie, snelheid en flexibiliteit[18]. Ook speelt volgens de EC cloud computing een rol bij de introductie van kunstmatige intelligentie, «Internet-of- Things» en blockchain. De Europese Commissie wil dit stimuleren door te investeren in innoverende cloudprojecten, onder meer via de IPCEI-CIS waar ook Nederland aan deelneemt. Anderzijds wil de EC beleid en regels ontwikkelen die cloudgebruikers beschermen, de clouddienstverlening veiliger maakt en zorgt voor eerlijke concurrentie en optimale voorwaarden voor een succesvolle Europese cloudindustrie. Zo zorgt bijvoorbeeld de verordening (EU) 2018/1807 van het Europees Parlement voor een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie. Samen met de AVG zorgt dit voor een ongelimiteerd verkeer van data binnen de EU. Ook de aankomende dataverordening, die zich richt op het verbeteren van de mogelijkheden tot het overstappen tussen aanbieders van clouddiensten is in dit kader relevant, met name ten aanzien van de noodzaak tot een exit-strategie.

Op 20 oktober 2020 hebben 25 EU lidstaten gezamenlijk verklaard om samen met de industrie te werken aan een volgende generatie van een Europese cloud. Die zou de hoogste normen moeten nastreven op het gebied van gegevensbescherming, cyberbeveiliging, dataportabiliteit/ omkeerbaarheid, interoperabiliteit, transparantie, openheid, energie efficiëntie, prestaties en betrouwbaarheid.

Wet en Regelgeving en overige voorwaarden bij dienstverlening

Wet- en regelgeving stelt, expliciet of impliciet, eisen aan de informatievoorziening binnen de rijksoverheid. Hier moeten alle informatiesystemen aan voldoen. Of dat in de praktijk kan, wordt per geval bekeken en besloten, en dit geldt ook voor zowel publieke als private clouddienstverlening.

Algemeen geldt voor uitbestedingen dat o.a. moet worden voldaan aan eisen uit het Voorschrift Informatiebeveiliging Rijksdienst (VIR)[19], Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie

[18] https://digital-strategy.ec.europa.eu/en/library/cloud-and-edge-computing-different-way-using-it-brochure

[19] https://wetten.overheid.nl/BWBR0022141/2007-07-01

(VIRBI)[20], de BIO[21], de regels omtrent archiveren[22], de AVG[23], de Wet Open Overheid (WOO)[24] en Wet Politiegegevens (WPG)[25];

Bij de opslag en verwerking van persoonsgegevens moet aan alle wettelijke vereisten, zoals die uit de Algemene Verordening Gegevensbescherming, worden voldaan. Bij gebruik van een publieke cloudplatform is dat een bijzonder punt van aandacht omdat een nieuwe sub-verwerker mogelijk op een andere plaats in de wereld, immers enkele muisklikken verwijderd is.

Op basis van Hoofdstuk V van de AVG gelden er aanvullende wettelijke vereisten wanneer er gegevens vanuit landen buiten de Europese Economische Ruimte (EER of «derde landen») toegankelijk zijn om ervoor te zorgen dat het niveau van gegevensbescherming wordt geborgd. Echter, wanneer de Europese Commissie voor een derde land een adequaatheids-besluit heeft genomen geldt dat dit derde land een adequaat niveau van gegevensbescherming borgt en hoeven er geen extra maatregelen te worden genomen.

Bij de inkoop en aanbesteding van producten en diensten binnen de rijksoverheid, worden (eventuele) risico's voor de nationale veiligheid meegewogen. Hierbij wordt in het bijzonder gelet op mogelijke risico's voor de continuïteit van vitale processen, de integriteit en exclusiviteit van kennis en informatie en de ongewenste opbouw van strategische afhankelijkheden.
Hierbij wordt ook rekening gehouden met systemen en componenten die komen uit een land met een actief cyberprogramma dat gericht is tegen belangen van Nederland en haar bondgenoten[26]. Het lijnmanagement is verantwoordelijk voor het naleven van alle regels, binnen het (departementale) CIO-stelsel.

Beleidsontwikkeling voor verwerving of uitbesteding van ICT-diensten (waar clouddiensten deel van zijn) en het organiseren van Rijksbrede afwegingen raken ook het verantwoordelijkheidsgebied van de Chief Procurement Office van de Rijksdienst (CPO-Rijk).

Voordelen gebruik publieke clouddiensten

Publieke clouddiensten bieden een aantrekkelijk perspectief voor de ontwikkeling naar een meer innovatieve, transparante, flexibele en efficiënte digitale rijksoverheid. De lage instapkosten, gekoppeld aan het feit dat men betaalt naar gebruik, maakt de financiering van ICT-gebruik in de publieke cloud transparant.

Tevens zijn risico's vaak beter te beheersen dan voorheen. Dat wordt mede veroorzaakt doordat de publieke cloudleveranciers grote bedragen investeren en veel expertise inzetten bij het beveiligen van hun diensten. Deze investeringen zijn vele malen hoger dan wat de rijksoverheid zelf wil of kan investeren in informatiebeveiliging. Bij de ontwikkeling van informatievoorziening binnen de rijksoverheid heeft gebruik van cloudvoorzieningen daarom vaak de voorkeur, met uitzondering waar het

[20] Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) – BWBR0033507 (overheid.nl)
[21] Baseline informatiebeveiliging Overheid Informatieveiligheid
[22] Regels voor archieven overheid | Archieven | Rijksoverheid.nl
[23] Algemene verordening gegevensbescherming EUR-Lex – 32016R0679
[24] wetten.nl – Regeling – Wet open overheid – BWBR0045754
[25] Wet Politiegegevens – BWBR 0022463
[26] Quickscan Nationale Veiligheid bij Inkoop en Aanbesteden

belang of de vertrouwelijkheid van de informatie of dienst zo hoog is dat de risico's te groot zijn.

Cloudleveranciers hebben laten zien dat ze in staat zijn om zeer snel innovatieve technologieën beschikbaar te stellen (zoals bij «data science»). De introductie van dergelijke technieken gaat sneller en goedkoper dan normaal gesproken binnen de rijksoverheid. Daarnaast vereist de inzet van de publieke cloud een hoge mate van standaardisatie. Dit kan in potentie kostenbesparend werken en de kwaliteit en implementatiesnelheid van ICT-projecten binnen het Rijk verhogen. Publieke clouddiensten zijn ook goed schaalbaar en in een «multi-cloud» omgeving zelfs te combineren. Hierdoor wordt het voor het Rijk makkelijker om ICT-dienstverlening op te schalen of te reduceren, te wisselen van leverancier en met onderdelen van verschillende leveranciers de beste dienstverlening voor burgers en bedrijven te creëren.

Risicobeheersing

Wel zijn er diverse risico's en technologie- en leveranciersafhankelijkheden verbonden aan het afnemen van publieke cloud diensten, waarvoor terecht wordt gewaarschuwd.
De huidige markt voor cloudtechnologie wordt in belangrijke mate gedomineerd door buitenlandse technologiebedrijven. De Autoriteit Consumenten en Markt is in mei 2021 begonnen met een marktstudie, die gaat inventariseren of sprake is van marktimperfecties zoals marktmacht, lock-in effecten en informatie-asymmetrie.

Ook de Cybersecurity Raad waarschuwt voor marktdominantie door, en afhankelijkheid van, buitenlandse partijen. Zij vraagt de Nederlandse overheid om nationaal en in EU-verband een rol te spelen op de markt voor clouddienstverlening, zowel beleidsmatig als met investeringen en een stimulerend inkoopbeleid. Het cloudbeleid maakt dat mogelijk.

Op 11 mei hebben de Raad en het parlement van de EU een voorlopig politiek akkoord bereikt over de wet digitale markten (Digital Markets Act – DMA).
Dit wordt als essentieel gezien om de digitale markten te stimuleren en beter te ontsluiten, de consument en organisaties meer keuzevrijheid te bieden en om innovatie te bevorderen.

Om zicht op stapeling en daaraan verbonden risico's te houden, is in het beleid opgenomen dat beleidsdepartementen geïnformeerd gehouden worden bij clouduitbestedingen en CIO Rijk hierover uitvragen kan doen. Om administratieve druk te vermijden is dit beperkt tot «materieel cloudgebruik» dus bij processen en voorzieningen van enige omvang die relevant zijn voor de werking van elk departement en daarmee van de staat. Tevens geldt een verplichting voor het opnemen van een «exit strategie» in de overeenkomst met de leverancier.

Politiek is er veel aandacht geweest voor de mogelijke toegang tot gegevensverzamelingen van zowel privacy als spionage gevoelige data door juridisch afgedwongen, en geheim te houden, medewerking aan veiligheidsdiensten. Dit geldt met name voor de VS, met de Cloud Act en de Foreign Intelligence Surveillance Act, waar tevens de grootste cloudaanbieders vandaan komen. Minder aandacht is geweest voor andere landen, ook binnen de EU, waar vergelijkbare verplichtingen bestaan. Om dergelijke risico's te vermijden is het opslaan of verwerken van staatsgeheimen in publieke cloud omgevingen niet toegestaan en zullen in andere gevallen maatregelen genomen moeten worden die dit risico tot een te accepteren niveau verminderen, zoals bijvoorbeeld sterke

versleuteling. Extra aandacht is gegeven en waarborgen zijn opgenomen voor privacy gevoelige informatie en de basisregistraties van de overheid.

Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) sluit de inzet van Publieke clouddiensten voor informatiesystemen op Departementaal Vertrouwelijk niveau niet meer bij voorbaat uit. Het NBV adviseert wel om dit nauwkeurig op case-by-case basis te beoordelen[27]. Hierbij rekening te houden met de volgende afwegingen:

- Er worden nooit clouddiensten afgenomen van dienstverleners uit landen met een offensief cyberprogramma tegen Nederlandse belangen.
- Waar sprake is van een risico van statelijke actoren wordt tijdig dreigings-en beveiligingsadvies ingewonnen van AIVD en/of MIVD.
- Bij verwerving of uitbesteding van IT-diensten naar de publieke cloud wordt de cloud oplossing met de on-premise situatie vergeleken. Hierbij worden niet alleen de beveiligingsrisico's en -onzekerheden maar ook de mogelijke beveiligingsvoordelen vergeleken.

Om de privacy risico's voor alle uitbestedingen, dus ook voor het gebruik maken van zowel private als publieke cloudoplossingen, is het maken van een risicoanalyse verplicht.
CIO Rijk komt een handreiking met voorbeelden, waarmee zo'n analyse te maken is. In de risicoanalyse wordt speciale aandacht gegeven aan (de bescherming van) bijzondere persoonsgegevens.

[27] Zie nota «NBV standpunt publieke-clouddiensten en gerubriceerde gegevens (januari 2021)»