Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 963

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 25 januari 2023

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over de brief van 29 augustus 2022 over Rijksbreed cloudbeleid 2022 (Kamerstuk 26 643, nr. 904).

De vragen en opmerkingen zijn op 3 november 2022 aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties voorgelegd. Bij brief van 24 januari 2023 zijn de vragen beantwoord.

De voorzitter van de commissie,
Kamminga

Adjunct-griffier van de commissie,
Van Tilburg

kst-26643-963
ISSN 0921 - 7371
's-Gravenhage 2023

Vragen en opmerkingen vanuit de fracties en reactie van de Staatssecretaris

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben kennisgenomen van het reeds aangekondigde Rijksbreed cloudbeleid 2022 van de Staatssecretaris voor Koninkrijksrelaties en Digitalisering. Deze leden constateren dat het streven naar het gebruik van publieke (commerciële) clouddiensten de nodige (veiligheids-) risico's met zich meebrengt voor overheidsdiensten die niet onbesproken mogen blijven. Deze leden achten het van belang om hier nader op in te gaan. Zij willen hierover dan ook nog enkele vragen stellen.
Allereerst willen de leden van de VVD-fractie erop wijzen dat het leeuwendeel van de publieke cloudmarkt gedomineerd wordt door aanbieders van Amerikaanse herkomst. In de praktijk betekent dit dat in de toekomst onze overheidsdiensten in de meeste gevallen zullen overstappen naar bekende Amerikaanse cloudpartijen. In dat licht willen deze leden wijzen op de implicaties van geldende Amerikaanse wetgeving en in het bijzonder de *Clarifying Lawful Overseas Use of Data Act* (Cloud Act). Conform de Cloud Act worden Amerikaanse aanbieders van elektronische communicatiediensten, dus ook cloudaanbieders, verplicht om gegevens die middels hun diensten worden verstuurd te bewaren en te verstrekken op verzoek van de Amerikaanse overheid. Deze vorderingen kunnen plaatsvinden ongeacht waar ter wereld de servers gelokaliseerd zijn. Dit komt erop neer dat, wanneer Nederlandse overheidsdiensten gebruik gaan maken van Amerikaanse cloudinfrastructuur, ook Nederlandse overheidsdata opgevraagd kunnen worden door de Amerikaanse overheid, zonder dat daarbij de betreffende overheidsdienst wordt geïnformeerd, zoals bleek uit de bevindingen van de Cloud Act memo opgesteld door advocatenkantoor Greenberg Traurig gericht aan het Nationaal Cyber Security Centrum (NCSC)[1]. Is de Staatssecretaris zich bewust van deze implicatie? Hoe beoordeelt zij dit?

De Cloud Act maakt het mogelijk dat de Amerikaanse overheid, waaronder opsporingsdiensten, toegang krijgen tot (persoons-)gegevens van Nederlandse burgers. Gelet op de extraterritoriale werking van de Cloud Act is toegang ook mogelijk als de data buiten de V.S. staat. Er zijn ook andere landen met dergelijke wetten en bijbehorende verplichtingen. Om eventuele risico's hieromtrent tegen te gaan, bevat het Rijksbreed cloudbeleid 2022 en het bijbehorende implementatiekader «risicoafweging cloudgebruik»[2] onder meer de plicht om een risicoafweging te maken. Ook bevat het specifieke eisen voor omgang met persoonsgegevens, en is het niet toegestaan staatsgeheim gerubriceerde gegevens in de cloud te plaatsen.
Een risicoafweging kan als uitkomst hebben dat dit risico acceptabel is. Ten aanzien van de Cloud Act geldt dat uit recent onderzoek van Greenberg Traurig blijkt dat: »[…]het risico dat de Amerikaanse overheid toegang krijgt tot Europese (persoons)gegevens, specifiek op basis van de CLOUD-act, weliswaar voorstelbaar, maar in de praktijk ook (heel) klein is».
Een adequate risicoafweging, waaronder het doen van een gedegen Data Protection Impact Assessment (DPIA) en een Data Transfer Impact Assessment (DTIA), blijft echter nodig om het risico in een concreet geval te beoordelen.

---

[1] NCSC, 16 augustus 2022, Cloud Act memo (https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-act-memo)
[2] Zie bijlage

Kan de Staatssecretaris hierbij specifiek ingaan op de bevindingen van Greenberg Traurig in de Cloud Act memo en de bestaande eisen die gelden voor ICT-dienstverlening van de overheid?

In het voorgaande antwoord is reeds ingegaan op de bevindingen van Greenberg Traurig. In hoeverre het gebruik van Amerikaanse clouddiensten, gelet op onder andere de Cloud Act, zich verhoudt tot de AVG kan het volgende worden gesteld. Een gedegen risicoafweging voorafgegaan door een risico-impactanalyse (Data Transfer Impact Assessment) is in dit verband nodig. Een uitkomst van een dergelijke risicoafweging kan zijn dat er aanvullende waarborgen moeten worden genomen zoals encryptie, om ervoor te zorgen dat het door het Unierecht vereiste beschermingsniveau wordt gewaarborgd. Het European Data Protection Board (EDPB) heeft daar aanbevelingen voor opgesteld [3]:«De bedoeling van de Aanbevelingen van het EDPB is om als richtsnoer te dienen voor exporteurs bij de rechtmatige doorgifte van persoonsgegevens naar derde landen, en tegelijkertijd om voor de doorgegeven gegevens een beschermingsniveau te waarborgen dat in wezen gelijkwaardig is aan het niveau dat binnen de EER wordt gewaarborgd», aldus Andrea Jelinek voorzitter van het EDPB.

De leden van de VVD-fractie vragen specifiek hoe het voornemen tot het gebruik van publieke (commerciële) clouddiensten, gelet op de implicaties van de Cloud Act, zich verhoudt tot de bestaande eisen krachtens de Algemene verordening gegevensbescherming (AVG), de Baseline Informatiebeveiliging Overheid (BIO) en het Voorschrift Informatiebeveiliging Rijksdienst (VIR). Kan de Staatssecretaris dit toelichten?

Ook het gebruik van public (commerciële) clouddiensten moet voldoen aan het VIR, het VIR-BI de BIO en de AVG.

In het verlengde hiervan, wordt gesteld dat bij de inkoop en aanbesteding van producten en diensten binnen de rijksoverheid eventuele risico's voor de nationale veiligheid worden meegewogen. Hierbij zou in het bijzonder gelet moeten worden 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. Gelet op de implicaties van de Cloud Act, hoe beoordeelt de Staatssecretaris specifiek de risico's voor de nationale veiligheid en de mogelijke verstoring van continuïteit van onze vitale processen indien Nederlandse overheidsdiensten gebruik maken van Amerikaanse cloudinfrastructuur, zo vragen deze leden.

Het Rijksbreed cloudbeleid 2022 benoemt een aantal risico's en verplicht daarom het uitvoeren van een risicoafweging. Het verplichte implementatiekader benoemt aan welke eisen een dergelijke risicoafweging moet voldoen. Als er uit de afweging blijkt dat uitbesteden aan cloud providers van ICT-dienstverlening een onacceptabel risico voor nationale veiligheid of continuïteit van vitale processen ontstaat, dan moeten hiervoor maatregelen getroffen worden of van uitbesteding worden afgezien. Sowieso is het niet toegestaan om staatsgeheime informatie in de cloud te plaatsen.

De leden van de VVD-fractie lezen daarnaast in de brief dat de BIO de inzet van publieke clouddiensten niet bij voorbaat uitsluit. Deze leden vragen de Staatssecretaris wat wordt bedoeld met «niet bij voorbaat uitsluit». Moet

[3] edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (europa.eu)

de BIO worden aangepast om gebruik te kunnen maken van publieke clouddiensten?

Nee, want zoals hiervoor aangegeven sluit de BIO het gebruik van publieke clouddiensten niet uit. Clouddiensten vallen in de huidige versie van de BIO onder leveranciersrelaties, hoofdstuk 15. Naleving van dit hoofdstuk draagt zorgt ervoor dat alle relevante informatiebeveiligingseisen een plaats krijgen in leveranciersovereenkomsten.

Is anderszins nog wijziging van wet- en regelgeving nodig? Zo ja, om welke wet- en regelgeving gaat het?

Nee, er zijn geen wijzigingen van wet- en regelgeving nodig om conform het Rijksbreed cloudbeleid 2022 gebruik te maken van de publieke cloud.

De leden van de VVD-fractie willen tevens wijzen op het lopende onderzoek van de Europese privacy toezichthouder European Data Protection Board (EDPB) naar cloudgebruik door de publieke sector waarvan de resultaten voor het eind van dit jaar verwacht worden. Gelet op de mogelijke uitkomsten van dit onderzoek, in het bijzonder op het vlak van de risicoanalyse gericht op het gebruik van non-EU cloudleveranciers, realiseert de Staatssecretaris zich dat met voorliggend voorstel vooruit wordt gelopen op dit onderzoek? Zo ja, kan de Staatssecretaris hierop reflecteren?

Ik ben bekend met dit onderzoek van EDPB en dit rapport wordt momenteel bestudeerd. Waar relevant zullen bevindingen uit dit rapport, en eventuele andere ontwikkelingen op EU-niveau, worden meegenomen in de voorziene evaluatie van het Rijksbreed cloudbeleid 2022 en/of de opvolging van die evaluatie.

Is het Adviescollege ICT-toetsing om advies gevraagd over het Rijksbreed cloudbeleid? Zo nee, waarom niet?

Nee. Het Adviescollege ICT-Toetsing (AcICT) adviseert over de verbetering van de beheersing van ICT-projecten en informatiesystemen. Het Rijksbreed cloudbeleid 2022 betreft géén ICT-project of informatiesysteem, maar biedt kaders waarin dit beleid uitgevoerd zou kunnen worden door organisaties binnen de rijksoverheid.

Voorts willen de leden van de VVD-fractie aandacht vragen voor het steeds groter wordende belang van het versterken van de Nederlandse en Europese digitale autonomie in het kader van onze strategische belangen. Dit belang is al eerder benadrukt in het Coalitieakkoord «Omzien naar elkaar, vooruitkijken naar de toekomst» (Bijlage bij Kamerstuk 35 788, nr. 77) met het expliciet benoemen van de noodzaak van strategische autonomie om onze veiligheid, rechtsstaat, democratie, mensen- en grondrechten en concurrentievermogen beter te beschermen. In het kader van deze uitgesproken politieke wens, hoe reflecteert de Staatssecretaris op haar besluit en voornemen om overheidsinstanties gebruik te laten maken van commerciële clouddiensten die grotendeels in Amerikaanse handen zijn? Kan de Staatssecretaris hierbij ingaan op haar beweegredenen voor haar besluit/voornemen?

Het nieuwe cloudbeleid maakt het voor de Rijksdienst ook mogelijk om gebruik te maken van Europese commerciële clouddiensten en initiatieven. Het Rijksbreed cloudbeleid 2022 stelt eisen aan veiligheid en privacy voor al het gebruik van publieke clouddiensten. Risico's omtrent marktconcentratie en politieke en geografische spreiding worden hierin

meegenomen, waarbij CIO Rijk departement-overstijgende risico's monitort.

De leden van de VVD-fractie stellen vast dat met het kiezen voor publieke clouddiensten, gezien de Amerikaanse dominantie, indirect wordt gekozen voor niet-EU cloudaanbieders en dat daarmee niet wordt ingezet op het verder ontwikkelen van de nationale of Europese cloudmarkt. Deelt de Staatssecretaris de mening dat juist omwille van het versterken van onze digitale autonomie, het een gemiste kans is om niet in te zetten op de ontwikkeling van Europese alternatieven?

Binnen het Rijksbreed cloudbeleid 2022 is het voor de Rijksdienst mogelijk dat Rijksorganisaties gebruik maken van Europese publieke clouddiensten, inclusief duidelijke kaders waarbinnen dat mag.
Het kabinet zet op verschillende manieren in op de ontwikkeling van alternatieven, om zo de markt voor clouddiensten beter te laten functioneren en daarmee onze strategische autonomie te versterken. Onder andere via het GAIA-X initiatief draagt Nederland bij aan de ontwikkeling van innovatieve cloudoplossingen. Ook het Important Project of Common European Interest Cloud Infrastructure and Services (IPCEI CIS) draagt hieraan bij.

Zo ja, hoe verhoudt zich dit tot het besluit van de Staatssecretaris ten aanzien van het Rijksbreed cloudbeleid en hoe verhoudt zich dit tot de Important Project of Common European Interest (IPCEI)-investeringen gericht op cloud? Zo nee, waarom niet?

Er wordt binnen de IPCEI CIS door twaalf lidstaten, waaronder Nederland, geïnvesteerd in de ontwikkeling van alternatieve cloudoplossingen. Hierbij is er veel aandacht voor de veiligheid en duurzaamheid van deze oplossingen. Door openheid en interoperabiliteit te bevorderen dragen de ontwikkelde oplossingen bij aan een beter functionerende markt voor clouddiensten. Deze investeringen zijn noodzakelijk om geconstateerde marktfalen op de Europese interne markt te adresseren. Deze investeringen dragen bovendien bij aan het tegengaan van afhankelijkheden in de markt. De IPCEI CIS investeringen staan los van het Rijksbreed cloudbeleid maar dragen op termijn wel bij aan het beschikbaar komen van alternatieven op de markt voor clouddiensten.

De leden van de VVD-fractie willen, met het oog op het belang van het inzetten op Europese alternatieven, graag nader ingaan op de inspanningen die tot nu geleverd zijn in nationaal en Europees verband. Zo willen deze leden wijzen op de gezamenlijke verklaring van 25 lidstaten van de Europese Unie op 20 oktober 2020 om samen met de industrie te werken aan een volgende generatie van een Europese cloud. Welke concrete stappen zijn sinds deze verklaring gezet in Europees verband?

In de verklaring hebben de betrokken lidstaten gesteld dat innovatieve cloudoplossingen een belangrijke bijdrage kunnen leveren aan het verdienvermogen en de duurzaamheid van de EU. Om in dit kader de ontwikkeling van Europese innovatieve cloudoplossingen te bevorderen is in december 2020 de IPCEI-CIS geïnitieerd door Duitsland en Frankrijk, waarbij andere lidstaten zich hebben aangesloten. Naast Nederland doen ook België, Duitsland, Frankrijk, Hongarije, Italië, Letland, Luxemburg, Polen, Slovenië, Spanje en Tsjechië mee aan dit project. Om de betrokkenheid te onderstrepen is door deze landen hiervoor ook een manifest opgesteld en ondertekend. De Nederlandse investeringsvoorstellen voor IPCEI Cloud zijn samen met de voorstellen uit de andere lidstaten op 4 april jl. bij de Europese Commissie ingediend. Het verplichte goedkeuringsproces voor de voorstellen neemt door de omvang en complexiteit

van deze IPCEI meer tijd in beslag dan eerder aangenomen door alle betrokken partijen. De huidige verwachting is dat dit proces de eerste helft van 2023 zal worden afgerond.

Is de Staatssecretaris het met deze leden eens dat dit soort initiatieven, gelet op bovenstaande, juist gestimuleerd moeten worden? Zo ja, hoe beoordeelt zij de kansen en de meerwaarde van deze gezamenlijke inspanning in het licht van uw beslissing om overheidsdiensten publieke clouddiensten te VE Tlaten gebruiken?

Ja, dit is ook de reden dat dergelijke initiatieven worden ondersteund door het kabinet. Deze Europese initiatieven staan veelal nog in een beginstadium, maar worden door Nederland actief gesteund. Het Rijksbreed cloudbeleid 2022 maakt het ook mogelijk dat de rijksoverheid gebruik maakt van Europese publieke clouddiensten, met duidelijke kaders waarbinnen dat mag.

Daarnaast willen de leden van de VVD-fractie de Staatssecretaris attenderen op het recent verschenen rapport Marktstudie Clouddiensten van de Autoriteit Consument en Markt (ACM).[4] Naast dat dit rapport de Amerikaanse dominantie op de cloudmarkt aantoont, wordt gewaarschuwd voor «verborgen kosten» die gepaard gaan met overstappen en het risico op volledige afhankelijkheid. Hoe beoordeelt de Staatssecretaris deze waarschuwing?

Het kabinet heeft kennis genomen van het rapport en deelt de bevindingen van de ACM. Het kabinet is zich bewust van de risico's die voortkomen uit de marktmacht en afhankelijkheid van aanbieders van clouddiensten. De ACM noemt daarin onder andere de Digital Markets Act (DMA) en de aankomende Dataverordening (DA) als instrumenten die kunnen bijdragen aan het stimuleren van de concurrentie in de cloudmarkt, zodat deze risico's verminderd worden. Ook het kabinet ziet de DMA en DA als belangrijke instrumenten. Zo heeft het kabinet zich de afgelopen jaren sterk gemaakt voor het aanpakken van de macht van grote online platformen via de inzet voor de DMA. De DMA is in november 2022 in werking getreden. Daarnaast steunt het kabinet de in de DA voorgestelde maatregelen om aanbieders van clouddiensten te verplichten barrières voor overstappen tussen clouddiensten weg te nemen. In lijn met de aanbevelingen van de ACM in haar rapport zet het kabinet zich in voor extra maatregelen in de Dataverordening om de geconstateerde problemen in de cloudmarkt te adresseren, waaronder het bevorderen van de interoperabiliteit van clouddiensten, zodat clouddiensten van verschillende leveranciers makkelijker gecombineerd kunnen worden.
Voor deze problemen geldt dat dit door overheidsdiensten in de zakelijke afweging in combinatie met de risicoafweging meegenomen moet worden. Hiervoor is ook als verplichting in het Rijksbreed cloudbeleid opgenomen dat men over een exit-strategie dient te beschikken om deze afhankelijkheidsrisico's te mitigeren. Ook is opgenomen dat men vooraf moet nadenken over een eventuele overstap naar aan andere aanbieder.

In hoeverre zijn deze «verborgen kosten» zoals overstapheffingen en -toeslagen ingecalculeerd in het besluit en in hoeverre kan dit risico worden gemitigeerd door de opgenomen voorwaarde exit strategie?

Iedere Rijksorganisatie besluit zelf over de inzet van publieke clouddiensten binnen de kaders van het Rijksbreed cloudbeleid 2022. Hiermee

[4] ACM, 5 september 2022, Marktstudie Clouddiensten (https://www.acm.nl/system/files/documents/marktstudie-clouddiensten.pdf)

is iedere Rijksorganisatie zelf verantwoordelijk voor het beoordelen van de budgettaire impact. Eventuele overstapheffingen en -toeslagen zijn hier onderdeel van. Dit is tevens een verplicht onderdeel van de risicoafweging.

In hoeverre zijn de, vaak fikse, overstapkosten te rijmen met een strategie die tot en met 2025 duurt?

In de I-strategie Rijk 2021–2025 (Kamerstuk 26 643, nr. 779) is een van de speerpunten het opstellen van een Rijksbreed cloudbeleid. De uitwerking van dit speerpunt is het Rijksbreed cloudbeleid 2022. Het Rijksbreed cloudbeleid 2022 zal worden geëvalueerd in 2023 en zal indien nodig regulier worden aangepast. Ook na afloop van de I-strategie Rijk 2021–2025 blijft het Rijksbreed cloudbeleid 2022 geldig.

Is de Staatssecretaris het met deze leden eens dat bij het maken van keuzes die impact hebben op de strategische autonomie van Nederland verder gekeken moet worden dan slechts een paar jaar?

Ja, dit ben ik met u eens. Het Rijksbreed cloudbeleid 2022 wordt in 2023 geëvalueerd.

Ook het risico op volledige afhankelijkheid, ook wel de «vendor lock-in» genoemd, baart de leden van de VVD-fractie zorgen. Het ACMrapport waarschuwt voor de zuigwerking van big tech-clouddiensten. Door gebrekkige interoperabiliteit en dataportabiliteit zouden klanten effectief gevangen raken in het dienstenweb van big tech-cloudaanbieders wanneer eenmaal gebruik wordt gemaakt van de aangeboden cloudinfrastructuur van één bepaalde aanbieder. Het combineren van clouddiensten van verschillende aanbieders zou gepaard gaan met prijs- en kwaliteitsbeperkingen waardoor klanten het risico lopen om volledig afhankelijk te raken van één aanbieder. Hoe beoordeelt de Staatssecretaris dit geconstateerde risico op de onwenselijke «vendor lock-in»?

Om het risico op vendor lock-in te mitigeren, is de verplichting tot het hebben van een exit-strategie opgenomen.

In hoeverre mitigeren de opgenomen voorwaarden dit risico voor het gebruik van de publieke cloud voor overheidsdiensten?

Het is een onderwerp dat continu aandacht vraagt, maar het is de inschatting van het kabinet dat de opgenomen voorwaarden en werkwijzen dit risico mitigeren.

In hoeverre ziet de Staatssecretaris het ontbreken van afdwingbare open standaarden in de «European Data Act» als risico voor een toekomstige overstap naar een andere aanbieder?

Op basis van het huidige voorstel van de Dataverordening kan de Europese Commissie standaarden publiceren waar aanbieders van clouddiensten aan moeten voldoen. Deze standaarden moeten het overstappen tussen aanbieders mogelijk maken met behoud van zogeheten «functional equivalence». Wanneer de Dataverordening in werking treedt gelden deze standaarden ook voor de aanbieders van publieke clouddiensten waar de rijksoverheid gebruik van kan maken.

Welke mogelijkheden ziet de Staatssecretaris nog concreet om de technische en financiële overstapdrempels tussen clouddiensten weg te nemen?

Op dit moment ziet het kabinet de aanpak van financiële, contractuele en technische drempels zoals omschreven in het voorstel voor een Dataverordening als voldoende om deze drempels voor overstappen tussen clouddiensten weg te nemen. Ook de DMA zal bijdragen aan het verminderen van drempels om over te stappen naar andere aanbieders van clouddiensten. De DMA gaat gelden voor poortwachters, dit zijn platforms waar gebruikers niet of nauwelijks meer omheen kunnen. Op basis van de DMA mogen poortwachters de mogelijkheid voor gebruikers van clouddiensten om over te stappen naar een andere aanbieder niet belemmeren. Vanaf 2024 zullen de verplichtingen uit de DMA gaan gelden voor aangewezen poortwachters.

Is zij bereid om hier stappen in te zetten? Zo nee, waarom niet?

Voor wat betreft de maatregelen in de Dataverordening om barrières voor overstappen tussen clouddiensten weg te nemen zet het kabinet zich vooral in om het ambitieniveau uit het initiële voorstel te behouden en aan te scherpen. In de onderhandelingen over de Dataverordening wordt erop ingezet om de interoperabiliteit van clouddiensten te bevorderen. Hiermee zou ook de zogeheten multi-cloud, het gelijktijdig en verbonden gebruik van clouddiensten van meerdere aanbieders, beter mogelijk worden.

Op welke manier worden de verschillende departementen geholpen om de juiste risico-afwegingen te maken rondom de lock-in en om daar een uitvoerbare exit-strategie voor te maken?

Departementen worden geholpen bij het maken van de juiste risico-afwegingen en het opstellen van een exit-strategie middels het implementatiekader «risicoafweging cloudgebruik». Verder ontvangen departementen een handreiking met praktische voorbeelden om het werken met publieke clouddiensten zo verantwoord en simpel mogelijk te maken.

De leden van de VVD-fractie hebben nog enkele laatste vragen. Wat is er in het kader van het Rijksbreed cloudbeleid 2022 geregeld voor de decentrale overheden?

Het Rijksbreed cloudbeleid 2022 is van toepassing op de Rijksdienst. Onderdelen van de overheid die niet tot de Rijksdienst behoren, waaronder decentrale overheden, wordt geadviseerd om dit Rijksbeleid te volgen. Het kabinet wil dit actief uitdragen.

Geldt voor deze overheden eenzelfde beleid als wordt voorgesteld in het Rijksbreed cloudbeleid 2022?

Nee, voor deze overheden geldt dit beleid niet. Het wordt hen wel geadviseerd om het Rijksbreed cloudbeleid 2022 te volgen.

Wordt dit nieuwe beleid al toegepast?

Ja. Voor verplicht beleid geldt dat een besluit van de Interdepartementale Commissie Bedrijfsvoering Rijksdienst (ICBR) voldoende is om het beleid van kracht te laten zijn. Het Rijksbreed cloudbeleid 2022 is ook in de ministerraad vastgesteld; het implementatiekader is op 20 december door de ICBR vastgesteld, en gelijktijdig met deze beantwoording aan uw Kamer aangeboden. De onderdelen van de Rijksdienst dienen sinds dat moment aan het Rijksbreed cloudbeleid 2022 te voldoen. Volgens het Rijksbreed cloudbeleid 2022 is de eerste stap nu dat de departementen een eigen departementaal cloudbeleid en -strategie op stellen. Hierin stellen zij zichzelf allereerst de vraag of ze gebruik gaan maken van de

publieke cloud. Indien ze hier positief op besluiten, zullen zij ook hierin toelichten waarmee zij dit willen gaan doen.

Is de Staatssecretaris het met deze leden eens dat het wenselijk is om in 2022 geen onomkeerbare stappen te zetten met betrekking tot afspraken met cloudaanbieders? Zo nee, waarom niet?

Ja, ik ben het hiermee eens. Hierom dient er een exit-strategie opgenomen te worden bij afspraken met cloudaanbieders, waar afdoende rekening gehouden wordt met data- en serviceportabiliteit.

Vragen en opmerkingen van de leden van de D66-fractie

De leden van de D66 fractie hebben met interesse kennisgenomen van het Rijksbreed cloudbeleid 2022. Deze leden hebben nog enkele vragen.
De leden van de D66-fractie lezen dat elke departement zelf verantwoordelijk is om de relevante risico's van het gebruik van een publieke cloud in beeld te hebben en te houden. Deze leden vragen waarom er niet van tevoren door het Rijk een risicokader is gemaakt zodat de departementen zich daar aan houden.

Een deel van de gesignaleerde risico's is in de voorwaarden van het Rijksbreed cloudbeleid 2022 opgenomen. In het implementatiekader «risicoafweging cloudgebruik» zijn deze verder uitgewerkt. Dit implementatiekader is op 20 december door de ICBR vastgesteld, en gelijktijdig met deze beantwoording aan uw Kamer verzonden. Aangezien departementen voor hun situatie specifieke risico's kunnen hebben, bevat het beleid en implementatiekader de minimale eisen waar een risicoafweging aan dient te voldoen, waarbij ook rekening gehouden moet worden met het specifieke cloudgebruik.

Kan de Staatssecretaris aangegeven in welke mate ieder departement individueel een data protection impact assessment (DPIA) moet doen als er gebruik wordt gemaakt van dezelfde publieke clouddienst?

De DPIA is afhankelijk van het risico dat de verwerking van (het type van) de persoonsgegevens oplevert. Indien departementen gebruik maken van dezelfde clouddienstverlener houdt dat niet automatisch in dat zij dezelfde soort gegevensverwerkingengegevensverwerkingen in die publieke cloud hebben. Ook kunnen de risico's van het gebruik van de publieke cloud per departement verschillen. Hierdoor dienen departementen individueel DPIA's uit te voeren, ook al maken zij gebruik van dezelfde publieke clouddienst.

Op basis van welk toetsingskader wordt bepaald of er sprake is van een hoog risico?

In het Rijksbreed cloudbeleid 2022 wordt een hoog risico specifiek genoemd bij privacyaspecten. Een hoog risico wordt daarbij bepaald op basis van een uitgevoerde pre-scan DPIA. Voorts zijn in art. 35(3) AVG criteria vermeld ter bepaling van een hoog privacyrisico. Als aanvulling hierop heeft de AP nog een definitieve lijst vastgesteld van verwerkingen van persoonsgegevens waarvoor een DPIA altijd nodig is.[5]

Wat als een departement de risico's te laag inschat, is hier sprake van toezicht?

[5] Besluit van de Autoriteit Persoonsgegevens van 27 november 2019 (Stcrt. 2019, nr. 64418).

Jaarlijks rapporteren de departementen over het materieel public cloudgebruik en onderliggende risico's aan CIO Rijk. De rapportages, DPIA's en risicoanalyses vormen de input voor de CIO-gesprekken die, in het kader van monitoring en advies, jaarlijks plaatsvinden. Naast deze periodieke rapportage voeren de departementen ook eigen audits en controles uit. De Audit Dienst Rijk (ADR) voert, als onafhankelijke internal auditor van de rijksoverheid, audits uit. Waarbij de Algemene Rekenkamer (ARK), als onafhankelijk instituut, vooral een controlerende rol heeft.

De leden van de D66-fractie lezen dat onderdelen die niet tot de Rijksdienst behoren ook geadviseerd worden dit Rijksbeleid te volgen. Deze leden vragen of hier gemeenten onder vallen.

Ja. Alle onderdelen van de overheid die niet tot de Rijksdienst behoren, waaronder gemeenten, wordt geadviseerd om dit Rijksbeleid te volgen.

Worden gemeenten door het Rijk begeleid of verder geadviseerd om hieraan te voldoen?

Het kabinet wil dit beleid actief uitdragen. Hoe gemeenten hierbij vanuit het Rijk of andere organisaties zoals de VNG zou kunnen worden begeleid of verder geadviseerd wordt op dit moment bekeken.

De leden van de D66-fractie stellen voorop dat, zoals de Marktstudie Clouddiensten van de ACM illustreert, het onwenselijk is dat de Amerikaanse techreuzen Microsoft, Google en Amazon vrijwel de gehele markt voor cloudaanbieders beheersen. In welke mate is het mogelijk om tussen cloudaanbieders te switchen als de huidige aanbieder niet voldoet aan de wensen?

De mate waarin het mogelijk is om over te stappen tussen cloudaanbieders verschilt per situatie, en is afhankelijk van factoren zoals het datavolume, het type dienstverlening, de betrokken aanbieders en de wensen van de eindgebruiker. In algemene zin kan op basis van het ACM rapport wel worden gesteld dat in de markt aanwezige financiële, technische en contractuele barrières belemmerend werken wanneer een gebruiker wil overstappen. Regelgeving kan eraan bijdragen dat het makkelijker wordt om over te stappen naar andere cloud aanbieders. Zo noemt de ACM de Dataverordening als een van de instrumenten die kan bijdragen aan het verminderen van afhankelijkheid en het stimuleren van concurrentie in de cloudmarkt. In de Dataverordening zijn bijvoorbeeld bepalingen opgenomen gericht op het wegnemen van financiële, contractuele en technische barrières die zullen bijdragen aan de verbeterde mogelijkheid om over te stappen. Ook de DMA draagt hieraan bij. In de DMA staat bijvoorbeeld de verplichting voor poortwachters dat zij de mogelijkheid voor gebruikers van clouddiensten om over te stappen naar een andere aanbieder niet mogen belemmeren.

Welk tijdspad en welke kosten komen bij een dergelijke switch kijken?

Dit zal per situatie verschillend zijn.

Zijn er aanwijzingen dat interoperabiliteit en dataportabiliteit zullen verbeteren de komende jaren bij deze aanbieders?

Het voorstel voor een Dataverordening bevat bepalingen gericht op het wegnemen van financiële, contractuele en technische overstapbarrières in de markt voor clouddiensten. Aanbieders van clouddiensten in de Europese interne markt moeten hieraan gaan voldoen wanneer de verordening in werking treedt. Het kabinet verwacht dat dit wetgevings-

voorstel interoperabiliteit en portabiliteit zal bevorderen. Verder zullen initiatieven zoals GAIA-X en IPCEI CIS gezien hun doelstellingen naar verwachting bijdragen aan beter functioneren van de markt in de komende jaren, waardoor de situatie op het gebied van interoperabiliteit en portabiliteit zal verbeteren.

Kan de Staatssecretaris toelichten wanneer het cloudbeleid aan evaluatie onderhevig is?

Het beleid wordt vanaf 2023, te starten één jaar na publicatie van het Rijksbreed cloudbeleid 2022, geëvalueerd.

De leden van de D66-fractie horen graag van de Staatssecretaris welke Europese lidstaten gelijkmatige wetten hebben zoals de Verenigde Staten op het gebied van datatoegang, zoals de Cloud Act en de Foreign Intelligence Surveillance Act.

Europese landen kunnen, net als andere landen, voorzieningen in hun nationale wetgeving hebben opgenomen die het voor inlichtingen-, veiligheids- en opsporingsdiensten mogelijk maakt rechtmatige toegang te krijgen tot data opgeslagen in datacentra. Net als in Nederland zijn Europese landen daarbij gebonden aan de eisen uit de EU-wetgeving en aan de eisen die het Europees Hof voor de Rechten van de Mens stelt aan toegang tot gegevens ten behoeve van de nationale veiligheid.

Is er altijd een plicht tot versleuteling van opgeslagen data bij het gebruik van clouddiensten? Zo nee, waarom wordt deze afweging per risico inschatting gemaakt?

Versleuteling is een beveiligingsmaatregel die afhankelijk van het type data en het bijbehorende risico toegepast moet worden, conform de aanpak van de BIO.

De Staatssecretaris geeft aan dat niet alle informatie geschikt is voor publieke clouddiensten, zoals staatsgeheim gerubriceerde informatie of informatie afkomstig van het Ministerie van Defensie. Is er nog een voornemen om aan de slag te gaan met een vorm van een eigen cloud voor zaken die niet in publieke clouddiensten mogen, mogelijk in Europees verband?

De veiligheid van gerubriceerde informatie heeft de aandacht van het kabinet. Zo wordt vanuit de routekaart digitale weerbaarheid uit de I-strategie Rijk ingezet op onder rijksbrede voorzieningen voor Hoog Gerubriceerde Informatie (HGI) en het realiseren en structureel borgen van de Nationale Cryptostrategie (NCS).

Vragen en opmerkingen van de leden van de CDA-fractie

De leden van de CDA-fractie hebben kennisgenomen van de brief van de Staatssecretaris over het Rijksbreed cloudbeleid 2022. Deze leden hebben hierover nog enkele vragen.

De leden van de CDA-fractie lezen dat het kabinet voornemens is om voorafgaand aan de keuze om publieke clouddiensten te gebruiken uitgebreide (pre-scan) DPIA's uit te voeren, om ervoor te zorgen dat de risico's in beeld zijn en goed afgedekt worden. Deze leden vragen of ook gedurende het gebruik van een publieke clouddienst wordt gemonitord en getoetst of het gebruik van de clouddienst nog aan de voorwaarden voldoet.

De toegespitste risicoafweging, exit-strategie en (pre-scan of formele) DPIA worden bij wezenlijke wijzigingen in de dienstverlening of wezenlijke verandering van de risico's geactualiseerd. Ten minste iedere drie jaar moet een actualisatie van de analyses plaatsvinden. De FG zal, als onderdeel van hun toezichthoudende rol (AVG, artikel 39), betrokken zijn bij het toezicht op de privacyrisico's binnen de organisaties.

De snelle technologische ontwikkelingen maken dit volgens deze leden noodzakelijk en zijvragen of de Staatssecretaris het hiermee eens is en hoe zij dit vormgeeft.

Het kabinet onderschrijft dit. Daarom is in het implementatiekader opgenomen dat de toegespitste risicoafweging, exit-strategie en (pre-scan of formele) DPIA bij wezenlijke wijzigingen in de dienstverlening of wezenlijke verandering van de risico's worden geactualiseerd, inclusief de te nemen passende acties. Dit vindt ten minste iedere drie jaar plaats of vaker als daar aanleiding toe is. CIO Rijk monitort hierop.

De leden van de CDA-fractie vragen of in het beleid ook is opgenomen dat rijksbreed bijgehouden wordt waar, hoeveel en voor hoelang gebruik gemaakt wordt van welke clouddiensten, inclusief de gronden voor het gebruik van de betreffende clouddienst.

De departementen rapporteren jaarlijks aan CIO Rijk over het materieel public cloudgebruik en de risico's daarvan. Dit gebeurt als onderdeel van het rapportageproces voor het IB-beeld, conform de departementale taken en volgens het besluit CIO-stelsel.

Deze leden vragen voorts hoe ervoor wordt gezorgd dat zoveel mogelijk centraal gestandaardiseerde contractuele voorwaarden worden opgesteld, om het cloudgebruik zoveel mogelijk te uniformeren.

Centraal gestandaardiseerde contractuele voorwaarden worden voor deelnemende organisaties geregeld vanuit de Strategisch Leveranciers Management-functie (SLM).

De leden van de CDA-fractie vragen aan de Staatssecretaris of en zo ja, welke adviezen de Staatssecretaris heeft ingewonnen over de vraag of het gebruik van publieke clouddiensten, en of bijvoorbeeld ook advies is gevraagd aan het Adviescollege ICT-toetsing.

Het Rijksbreed cloudbeleid 2022 is interdepartementaal tot stand gekomen, met adviezen vanuit de CIO's, CTO's en CISO's van alle ministeries en diverse grote uitvoeringsorganisaties.
Het Adviescollege ICT-Toetsing (AcICT) adviseert over de verbetering van de beheersing van ICT-projecten en informatiesystemen. Het Rijksbreed cloudbeleid 2022 betreft géén ICT-project of informatiesysteem, doch biedt kaders waarbinnen deze uitgevoerd zouden kunnen worden. Er is daarom geen advies gevraagd aan het Adviescollege ICT-toetsing.

De leden van de CDA-fractie lezen in de beslisnota van 7 juli 2022 over de mediaberichten dat de Ierse privacy toezichthouder DPC mogelijk Meta gaat verbieden data van Europese gebruikers naar clouddiensten in de Verenigde Staten te sturen, omdat zij niet aan de juridische voorwaarden voldoet. Deze leden vragen of hierover bij de Staatssecretaris inmiddels al meer over bekend is geworden en of deze berichten ook zijn meegewogen in de definitieve afweging om publieke clouddiensten, met enkele uitzonderingen, onder voorwaarden mogelijk te maken.

Op 25 november 2022 heeft de Ierse toezichthouder (DPC) een besluit genomen waarbij Meta een boete van € 265 miljoen werd opgelegd voor een datalek in 2019 waarbij persoonsgegevens van ongeveer 533 miljoen Facebook-gebruikers wereldwijd betrokken waren.
Bij totstandkoming van het Rijksbreed cloudbeleid 2022 zijn ontwikkelingen op Europees niveau meegewogen. Ook voor de evaluatie die zal starten in 2023 zullen Europese ontwikkelingen gemonitord worden.
Zoals gezegd dient de verwerking van persoonsgegevens ook bij het gebruik van Clouddiensten rechtmatig plaats te vinden. Wanneer sprake is van doorgifte van persoonsgegevens naar landen buiten de EER, dan moet voldaan zijn aan de voorwaarden van hoofdstuk V van de AVG. Daarbij is het van belang dat de richtsnoeren die op 18 juni 2021 zijn vastgesteld door het Europees Comité voor Gegevensbescherming (EDPB) worden gevolgd. Deze richtsnoeren bieden handvatten bij de beoordeling welke aanvullende maatregelen kunnen worden getroffen bij de verwerking van persoonsgegevens door derden. Aanvullend hierop heeft de Europese Commissie haar concept-adequaatheidsbesluit met de VS ter advisering voorgelegd aan de EDPB. Naar verwachting zullen de lidstaten in het eerste kwartaal van 2023 zich kunnen buigen over het concept-adequaatheidsbesluit in het artikel 93 comité. De Minister voor Rechtsbescherming zal uw Kamer daar te zijner tijd over informeren.

De leden van de CDA-fractie signaleren dat op Europees niveau veel aandacht is voor de ontwikkelingen rondom cloudgebruik. Deze leden vragen of de Staatssecretaris nader kan ingaan op de samenloop met de Europese ontwikkelingen op het gebied van de IPCEI Cloud.

In een verklaring uit 2020 hebben 27 Europese lidstaten gesteld dat innovatieve cloudoplossingen een belangrijke bijdrage kunnen leveren aan het verdienvermogen en de duurzaamheid van de EU. Hierbij spelen de Europese ontwikkelingen rondom cloudgebruik door private en publieke partijen een rol. Om in dit kader de ontwikkeling van Europese innovatieve cloudoplossingen te bevorderen is in december 2020 de IPCEI-CIS geïnitieerd door Duitsland en Frankrijk, waarbij andere lidstaten zich hebben aangesloten. Naast Nederland doen ook België, Duitsland, Frankrijk, Hongarije, Italië, Letland, Luxemburg, Polen, Slovenië, Spanje en Tsjechië mee aan dit project. Om de betrokkenheid te onderstrepen is door deze landen hiervoor ook een manifest opgesteld en ondertekend.
De Nederlandse investeringsvoorstellen voor IPCEI Cloud zijn op 4 april jl. bij de Europese Commissie ingediend. Het verplichte goedkeuringsproces voor de voorstellen neemt door de omvang en complexiteit van deze IPCEI meer tijd in beslag dan eerder aangenomen door alle betrokken partijen. De huidige verwachting is dat dit proces in de eerste helft van 2023 zal worden afgerond.
Verder wordt momenteel in het kader van de Cyberbeveiligingsverordening (Cyber Security Act) een vrijwillig Europees certificatieschema ontwikkeld voor de clouddiensten. De cyberbeveiligingsverordening is een Europese verordening, die een Europees kader introduceert op het gebied van cyberbeveiligingscertificering. De cyberbeveiligingsverordening maakt het mogelijk om op Europees niveau cyberbeveiligingscertificeringsregelingen (in de praktijk ook wel aangeduid als «certificatieschema's») vast te stellen voor categorieën van ICT-producten, -diensten en -processen. In opdracht van de Europese Commissie wordt thans een cyberbeveiligingscertificeringsregeling voor de cloud diensten (de zgn. Europese Cloud certificering schema) met cyberbeveiligingsvoorschriften ontwikkeld. Naar verwachting zal dit schema medio 2023 worden opgeleverd. Na de implementatie hiervan zullen de cloudaanbieders binnen twee jaar moeten voldoen aan de vereiste securitymaatregelen.

Deze leden vragen of de Staatssecretaris voornemens is om op lange termijn gebruik te willen gaan maken van betrouwbare Europese cloudaanbieders, die mogelijkerwijs voortkomen uit de initiatieven rondom IPCEI Cloud.

Alle departementen zijn vanuit het nieuwe cloudbeleid verplicht een eigen cloudstrategie op te stellen. Daarin maken zij als eerste de keuze of en waarmee ze de publieke cloud in gaan. Indien ze hiertoe besluiten, bepalen zij zelf welke clouddiensten zij gaan gebruiken. Voorgaande antwoorden geven weer hoe wij vanuit het kabinet wordt bijdragen aan Europese initiatieven zoals IPCEI-CIS.

Deze leden vragen de Staatssecretaris of zij kan toelichten of het voorgenomen Rijksbreed Cloudbeleid in overeenstemming is met de Europese Data Act.

Het Rijksbreed Cloudbeleid staat niet direct in relatie tot de Dataverordening. Het Rijksbreed cloudbeleid is gericht op de Rijksdienst als afnemer van clouddiensten, terwijl de Dataverordening zich richt op de aanbieders van clouddiensten. Leveranciers van publieke clouddiensten waar de rijksoverheid in lijn met het Rijksbreed cloudbeleid diensten van kunnen afnemen, zullen op het moment van inwerkingtreding aan alle eisen van de Dataverordening moeten voldoen.

Vragen en opmerkingen van de leden van de SP-fractie

De leden van de SP-fractie hebben kennisgenomen van de uitwerking van de nieuwe visie op het gebruik van publieke clouddiensten van de rijksoverheid. Deze leden vinden de verschuiving van gebruik van private clouddiensten naar publieke een goede stap, deze leden maken zich nog wel zorgen over de invulling van wat «publiek» precies betekent en de waarborgen die ontbreken voor veilig gebruik en opslag.

Bij publieke clouddiensten wordt de cloudinfrastructuur gedeeld door meerdere partijen en aangeboden door een (commerciële) partij. De kaders voor veilig gebruik en opslag zijn in de uitsluitingen en voorwaarden van het Rijksbreed cloudbeleid 2022 meegenomen. Deze worden verder toegelicht en uitgewerkt in het implementatiekader, zoals dat op 20 december door de ICBR is vastgesteld, en gelijktijdig met deze antwoorden met uw Kamer is gedeeld.

De grootste vraag die de leden van de SP-fractie hebben, is waarom gezegd wordt dat er publieke clouddiensten zijn, terwijl de opslag ingekocht wordt bij grote(re) tech- en/of ICT-bedrijven van uit de Verenigde Staten, China of andere internationale spelers.

In het Rijksbreed Cloudbeleid 2022 wordt de in de sector gangbare terminologie gehanteerd uit de NIST Definition of Cloud Computing. De NIST is de National Institute for Standards and Technology uit de Verenigde Staten.
In dit technologie domein heeft «publiek» een andere betekenis dan bijvoorbeeld «publiek» en «privaat» (bijvoorbeeld over instellingen) in Nederlands recht.
Een «public» cloud is een clouddienst bij een dienstverlener waar zowel de hardware als de software met andere organisaties wordt gedeeld, en waarin je (afhankelijk van behoefte) een stukje capaciteit en verwerking krijgt toebedeeld door de dienstverlener. De verwerkingen worden van elkaar gescheiden door logische beveiligingsmaatregelen.

Waarom is bij het vormgeven niet nagedacht over geopolitieke belangen die mee kunnen spelen bij bepalen wie een clouddienst mag aanbieden? Als dit wel is meegewogen, dan vragen deze leden, welke afwegingen zijn gemaakt?

Er is hierover nagedacht en in het Rijksbreed Cloudbeleid 2022 is richting meegegeven voor geopolitieke afwegingen. Bij de beoordeling van risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere partijen bij digitale producten hanteert het kabinet de overwegingen die zijn vermeld in de brief aan de Tweede Kamer over C2000, van 26 april 2019 (Kamerstuk 25 124, nr. 96). Hierbij wordt o.a. meegewogen of een partij afkomstig is uit een land met een offensief cyberprogramma. De overwegingen worden in samenhang met elkaar bezien en alleen wanneer alle overwegingen van toepassing zijn, en blijkt dat nationale veiligheidsrisico's niet voldoende kunnen worden beheerst, worden waar mogelijk partijen uitgesloten.
Mocht er een risico zijn op dreiging van statelijke actoren, moet men voortijdig dreigings- en beveiligingsadvies inwinnen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en/of Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Het risico van spionage door andere landen is meegewogen in onder meer de uitsluiting van gebruik van publieke clouddiensten voor informatie die als staatsgeheim is gerubriceerd.

Deze leden zijn er van geschrokken dat bij de technische briefing naar voren kwam dat lessen vanuit de aankoop van camera's door gemeenten of software door de politie niet zijn betrokken. De Kamer heeft meermaals aangegeven dat bij dit soort cruciale inzet van ICT/digitale technieken de naïviteit over spionage moet wordt afgeschud. Kan de Staatssecretaris aangeven hoe verschillende ministeries in de inkoop van hun cloud hierop selecteren en afwegen?

Alle departementen zijn vanuit het nieuwe cloudbeleid verplicht een eigen cloudstrategie op te stellen. Hierin kan de keuze gemaakt worden om gebruik te maken van Europese cloudaanbieders, of aan andere cloudaanbieders als daar aan wetten (zoals de AVG) en voorschriften en verplichtingen (zoals de BIO en het Rijksbreed Cloudbeleid 2022) wordt voldaan. Bij de beoordeling van risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere partijen bij digitale producten hanteert het kabinet de overwegingen die zijn vermeld in de brief aan de Tweede Kamer over C2000, van 26 april 2019 (Kamerstuk 25 124, nr. 96). Hierbij wordt o.a. meegewogen of een partij afkomstig is uit een land met een offensief cyberprogramma. De overwegingen worden in samenhang met elkaar bezien en alleen wanneer alle overwegingen van toepassing zijn, en blijkt dat nationale veiligheidsrisico's niet voldoende kunnen worden beheerst, worden waar mogelijk partijen uitgesloten.

De leden van de SP-fractie maken zich zorgen over dat iedere overheidsdienst of ministerie zelf zijn inkoop verzorgt en eigen strategie bepaalt. Deze leden vinden dat niet wenselijk. Kan de Staatssecretaris aangeven of en zo ja hoe zij de coördinatie – dan wel regie – kan versterken en het beleid minder vrijblijvend kan maken?

Het Rijksbreed Cloudbeleid 2022 is een verplicht beleid voor de Rijksdienst. Dit beleid is nader uitgewerkt in het eveneens verplichte implementatiekader, dat gelijktijdig met deze antwoorden aan uw Kamer is gestuurd.

Herkent de Staatssecretaris zich in de uitspraak «outsourcing is standaard» bij de inkoop van ICT-systemen en -producten? Wat vindt zij van die uitspraak?

Bij het gebruik van ICT-middelen en diensten maakt de rijksoverheid veel gebruik van wat er in de markt beschikbaar is. Zo worden telefoons en computers ingekocht en worden in veel gevallen ontwikkeling en beheer van middelen uitbesteed. Dit geldt zowel voor traditionele IT-infrastructuur in de Overheids Datacenters (ODC) als voor clouddiensten.

De leden van de SP-fractie vragen of de Staatssecretaris overweegt om eigen cloud of Europese clouddiensten te ontwikkelen ten einde niet afhankelijk te zijn van intercontinentale spelers.

Het kabinet steunt op verschillende manieren de ontwikkeling van Europese clouddiensten, onder andere via de IPCEI CIS en GAIA-X. Beide projecten dragen bij aan de ontwikkeling van een nieuwe generatie cloudoplossingen door marktpartijen, op basis van Europese waarden en regels. Samen met beleidsinitiatieven gericht op het beter laten functioneren van de markt, zoals de Dataverordening en DMA, draagt dit in de ogen van het kabinet voldoende bij aan het voorkomen van afhankelijkheid van spelers op de markt.

De leden van de SP-fractie hebben de indruk dat het cloudbeleid een rijdende trein is en dat bijsturing of aanpassing vanuit de Kamer nauwelijks mogelijk is. Kan de Staatssecretaris daarop reageren? Hoe ziet zij haar brief van 29 augustus 2022, als een voorstel of als uitleg van beleid?

De brief van 29 augustus 2022 bevat het interdepartementaal afgestemde en door de MR vastgestelde Rijksbreed Cloudbeleid 2022. Dit is daarmee het beleid zoals dat nu geldt voor de rijksoverheid. Dit beleid is nader uitgewerkt in het verplichte implementatiekader, dat is vastgesteld op 20 december in het ICBR en gelijktijdig met deze antwoorden aan uw Kamer is gestuurd. De departementen gaan met het implementatiekader en de nog komende handreiking voor implementatie aan de slag. Dit zal worden geëvalueerd, waarna het beleid eventueel zal worden bijgesteld. Ik blijf over het Rijksbreed cloudbeleid graag in gesprek met uw Kamer.

Deze leden hebben sterk de indruk dat de beleidskeuzes voldongen feiten zijn en daarom vragen zij aan de Staatssecretaris hoe dit beleid tot stand is gekomen. Welke beleidsmakers hebben dit opgesteld, wie hadden daarbij inspraak, en wanneer is dit beleid vastgesteld en door wie? Deze leden willen nadrukkelijk aangeven dat het niet om de personen gaat, maar om de functies en disciplines. Graag willen deze leden weten hoe er om is gegaan met advies en wie dat heeft gegeven. Kan de Staatssecretaris een helder overzicht maken van wie geadviseerd heeft of geconsulteerd is?

Het Rijksbreed cloudbeleid 2022 is interdepartementaal tot stand gekomen, nadat eerst een Verkenning Cloudbeleid voor de Rijksdienst heeft plaatsgevonden Deze verkenning heeft laten zien dat binnen de bestaande kaders meer mogelijk is met betrekking tot gebruik van publieke clouddiensten. CIO Rijk heeft het voortouw genomen om dit te concretiseren in een beleidskader, met als oogpunt de versterking van de ICT-infrastructuur voor de Nederlandse Rijksdienst. In de totstandkoming zijn in diverse afstemmingsrondes adviezen vanuit de CIO's, CTO's en CISO's van alle ministeries, diverse grote uitvoeringsorganisaties, het NCSC en hun medewerkers meegenomen. Het standpunt van de AIVD over publiek cloudgebruik is overgenomen. De departementen hebben in de Interdepartementale Commissie Bedrijfsvoering Rijk (ICBR) met het voorgestelde Rijksbreed cloudbeleid ingestemd. Het beleid is daarna vastgesteld in de ministerraad van 19 augustus 2022.

De leden van de SP-fractie stellen vast dat de beleidsbrief van de Staatssecretaris door wetenschappers niet positief is ontvangen, sterker: «hoogleraren maken gehakt van nieuwe cloudkoers van het kabinet» kopte Agconnect.nl op 22 september 2022[6]. Kan de Staatssecretaris helder ingaan op de bezwaren van de hoogleraren Van Dijck en Jacobs in de Volkskrant[7] van dezelfde datum? Kan zij de zorgen die de hoogleraren hebben wegnemen? Deze leden dagen haar daartoe uit.

Ja. De zorgen van de hoogleraren Van Dijck en Jacobs zaten in het Volkskrant artikel primair op het gebied van privacy en strategische autonomie.
Het Rijksbreed cloudbeleid 2022 staat binnen de regels van de AVG en bevat ook richtlijnen voor hoe om te gaan met landen van buiten de Europese Economische Ruimte. Alle opslag en verwerking van persoonsgegevens vindt plaats conform geldende privacy-vereisten uit de AVG. Wanneer een overheidsorganisatie besluit om van een public cloud dienst gebruik te maken, moet in de overeenkomst met cloudleveranciers een exit-strategie opgenomen zijn. Hierin staat onder andere hoe data overgedragen kan worden bij de beëindiging van de overeenkomst. De kosten van de uitvoering van een overeenkomst, ook die van de exit-strategie, moeten worden opgebracht door de organisatie die de overeenkomst aangaat. Via de rapportages die door de organisaties worden aangeleverd, monitort CIO Rijk of er voor de rijksoverheid in bredere zin geen ongewenste afhankelijkheden van één aanbieder ontstaan. Wanneer dit risico ontstaat kan CIO Rijk hierop acteren.
Het Rijksbreed Cloudbeleid 2022 geeft aan onder welke voorwaarden van public clouddiensten gebruik gemaakt kan worden en geeft kaders mee waarbinnen rijksoverheidsorganisaties verantwoord gebruik kunnen maken van public cloud diensten. Dit om ervoor te zorgen dat onze gevoelige gegevens veilig zijn.
Er is een gesprek geweest tussen de hoogleraren Van Dijck en Jacobs en de Staatssecretaris van Koninkrijksrelaties en Digitalisering, waarbij met hen is gesproken langs de lijnen zoals geschetst in de vorige vraag.

De leden van de SP-fractie zien dat in documenten een duidelijk onderscheid wordt gemaakt wat er wel en wat er niet in de cloud kan worden opgeslagen. Zo worden staatsgeheime en vertrouwelijke stukken alleen opgeslagen als het veilig kan.
Welke richtlijnen zijn er precies voor het vaststellen van welke documenten geclassificeerd zijn en de vraag wanneer het wel veilig kan?

Het rubriceren (classificeren) van documenten is voor de Rijksdienst in het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI) gedefinieerd. Het Nationaal Bureau Verbindingsbeveiliging (NBV), onderdeel van de AIVD, heeft aangegeven dat staatsgeheim gerubriceerde informatie niet veilig in de cloud kan, ongeacht de situatie.

De leden van de SP-fractie willen tot slot weten hoe er omgegaan wordt met de legacy van oude clouddiensten en de documenten die daar nu in staan?

Het Rijksbreed Cloudbeleid 2022 schept de mogelijkheid om van publieke clouddiensten gebruik te maken na afweging, maar stelt daartoe géén verplichting. Informatie en data gegenereerd voordat dit cloudbeleid is

---

[6] Agconnect, 22 september 2022, Hoogleraren maken gehakt van nieuwe cloudkoers kabinet (https://www.agconnect.nl/artikel/hoogleraren-maken-gehakt-van-nieuwe-cloudkoers-kabinet).
[7] Volkskrant, 21 september 2022, Opinie: Onze overheid moet haar kostbare data niet klakkeloos uitleveren aan Google en Amazon (https://www.volkskrant.nl/columns-opinie/opinie-onze-overheid-moet-haar-kostbare-data-niet-klakkeloos-uitleveren-aan-google-en-amazon/).

vastgesteld, kan, mits wordt voldaan aan de gestelde voorwaarden, dus naar de cloud worden gemigreerd, maar dit hoeft niet. Oude private clouddiensten kunnen nog steeds worden gebruikt, evenals informatie in systemen op eigen locaties en in eigen datacentra.

Zijn die documenten allemaal terug te vinden in systemen als digidoc als de stukken worden opgevraagd of als ze nodig zijn voor beleidsanalyse?

Alle organisaties maken eigen keuzes waar zij stukken opslaan voor beleidsanalyse, en hebben daar ook eigen systemen voor. Voor enkele departementen betreft dit DigiDoc.

Is gewaarborgd dat overheidsdiensten en ministeries kunnen overstappen naar een publieke clouddienst? Of later een overstap kunnen maken als zij een andere of een écht publieke clouddienst willen gebruiken?

Ja, met het Rijksbreed Cloudbeleid 2022 kunnen onderdelen van de Rijksdienst onder voorwaarden overstappen naar een publieke clouddienst. Om een overstap te faciliteren is in het Rijksbreed Cloudbeleid 2022 de voorwaarde opgenomen dat men een exit-strategie moet hebben.

Vragen en opmerkingen van de leden van de GroenLinks-fractie

De leden van de Groenlinks-fractie hebben met belangstelling kennisgenomen van de brief van de Staatssecretaris over het Rijksbreed cloudbeleid. Deze leden hebben naar aanleiding van de brief een aantal vragen en opmerkingen.
De leden van de GroenLinks-fractie constateren dat de cloudmarkt niet optimaal functioneert en dat er geïnvesteerd moet worden in (Europese) alternatieven. Deze leden vragen de Staatssecretaris hoe Nederland kan proberen hier grip op te houden om te voorkomen dat hier miljoenen worden ingepompt maar de overstap naar Europese diensten nooit wordt gemaakt.

Om de ontwikkeling van Europese innovatieve cloudoplossingen te bevorderen is de IPCEI-CIS geïnitieerd door Duitsland en Frankrijk, waarbij andere lidstaten zich hebben aangesloten. Naast Nederland doen ook België, Duitsland, Frankrijk, Hongarije, Italië, Letland, Luxemburg, Polen, Slovenië, Spanje en Tsjechië mee aan dit project. De Nederlandse investeringsvoorstellen voor IPCEI Cloud zijn op 4 april jl. bij de Europese Commissie ingediend. Bij de Europese Commissie vindt strenge toetsing van de voorstellen plaats, om te zorgen dat deze verenigbaar zijn met de Europese staatssteunregels. Ook wordt getoetst of de voorstellen bijdragen aan technische innovatie. Het verplichte goedkeuringsproces voor de voorstellen neemt door de omvang en complexiteit van deze IPCEI meer tijd in beslag dan eerder aangenomen door alle betrokken partijen. De huidige verwachting is dat dit proces in de eerste helft van 2023 zal worden afgerond. De in de IPCEI CIS ontwikkelde oplossingen zijn niet specifiek gericht op de rijksoverheid als afnemer. Ook als de rijksoverheid zelf de stap niet zet naar clouddiensten kan de IPCEI CIS nieuwe oplossingen opleveren.

Ook vragen de leden van de GroenLinks-fractie hoe de Staatssecretaris ervoor gaat zorgen dat we kunnen waarborgen dat veiligheid van informatie ook daadwerkelijk gewaarborgd wordt.

Jaarlijks rapporteren de departementen over het materieel public cloudgebruik en onderliggende risico's aan CIO Rijk. De rapportages, DPIA's en risicoanalyses vormen de input voor de CIO-gesprekken die, in het kader van monitoring en advies, jaarlijks plaatsvinden. Naast deze

periodieke rapportage voeren de departementen ook eigen audits en controles uit. De ADR voert, als onafhankelijke internal auditor van de rijksoverheid, audits uit. Waarbij de ARK, als onafhankelijk instituut, vooral een controlerende rol heeft.
Bij de beoordeling van risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere partijen bij digitale producten hanteert het kabinet de overwegingen die zijn vermeld in de brief aan de Tweede Kamer over C2000, van 26 april 2019 (Kamerstuk 25 124, nr. 96). Hierbij wordt o.a. meegewogen of een partij afkomstig is uit een land met een offensief cyberprogramma. De overwegingen worden in samenhang met elkaar bezien en alleen wanneer alle overwegingen van toepassing zijn, en blijkt dat nationale veiligheidsrisico's niet voldoende kunnen worden beheerst, worden waar mogelijk partijen uitgesloten. Mocht er een risico zijn op dreiging van statelijke actoren wordt voortijdig dreigings- en beveiligingsadvies ingewonnen van de AIVD en/of MIVD.

Is er bij overheden voldoende interne kennis van clouddiensten? Zo nee, hoe gaat dit alsnog georganiseerd worden?

In de Rijksbrede I-Strategie 2021–2025 wordt aandacht besteed aan het vergroten van de kennis en kunde bij rijksambtenaren op het gebied van digitalisering. Dat gebeurt bijvoorbeeld via de Rijks Academie voor Digitalisering en Informatisering Overheid (RADIO). Cloud computing is één van de onderwerpen waar leeractiviteiten op zijn en worden ontwikkeld, zodat bij het Rijk kennis wordt ontwikkeld en geborgd.

De leden van de GroenLinks-fractie hebben eerder al zorgen geuit over de sturing vanuit de Autoriteit Persoonsgegevens (AP). In zowel de technische briefing als de kabinetsbrief is niet duidelijk gemaakt hoe de zorgen nu weggenomen worden, buiten de opmerking dat er vergelijkbare risico's zouden zitten aan diensten afnemen van andere Europese landen. De AP noemde echter specifiek de wetgeving uit de VS als risico voor Europese privacy en daaruit volgend de soevereiniteit van lidstaten, waaronder Nederland. Hoe zijn de bezwaren van het AP precies weggenomen?

De AP heeft een brief gestuurd met zijn adviezen omtrent het Rijksbreed cloudbeleid 2022. Tevens heeft er een gesprek met de AP plaatsgevonden omtrent hun aandachtspunten. In de beleidsreactie op de brief van de AP wordt nader ingegaan hoe hun adviezen ter harte genomen worden.

En op basis waarvan wordt de inschatting gemaakt dat andere Europese landen een vergelijkbare bedreiging zijn voor Nederlandse dataveiligheid?

Europese landen kunnen, net als andere landen, voorzieningen in hun nationale wetgeving hebben opgenomen die het voor inlichtingen-, veiligheids- en opsporingsdiensten mogelijk maakt rechtmatige toegang te krijgen tot data opgeslagen in datacentra. Net als in Nederland zijn Europese landen daarbij gebonden aan de eisen uit de EU wetgeving en aan de eisen die het Europees Hof voor de Rechten van de Mens stelt aan toegang tot gegevens ten behoeve van de nationale veiligheid.

De leden van de GroenLinks-fractie constateren dat gefocust wordt op het risico van data breaches of toegang tot data door cloudproviders. Deze leden constateren dat dit slechts een aspect is van het soort van risico's bij het afnemen van cloudservices. Er moet ook aandacht zijn voor wat cloudproviders leren of allerhande aspecten van het functioneren van de Nederlandse overheid middels het soort van services en software dat verschillende instanties afnemen bij een cloudprovider. Deelt de Staatssecretaris dit standpunt?

We delen de mening dat het gebruik van publieke clouddiensten risico's met zich meebrengt. Voor de Rijksdienst is daarom in het Rijksbreed cloudbeleid 2022 opgenomen dat er voordat er gebruik mag worden gemaakt van een public clouddienst, een risicoafweging uitgevoerd moet worden. Dergelijke risicoafwegingen moeten integraal de risico's afdekken.

Hierover hebben deze leden ook nog enkele specifieke vragen. Is er een goede security assessment gemaakt van wat voor inzichten cloudproviders kunnen ontwaren op basis van de services die aan de overheid verleend worden?

Het Nationaal Bureau Verbindingsbeveiliging van de AIVD heeft in januari 2021 geadviseerd over public clouddiensten en gerubriceerde gegevens. Het Rijksbreed cloudbeleid 2022 zelf geeft ook inzicht in de gesignaleerde risico's.

Wat voor security risico's leveren die inzichten op?

Het is voorstelbaar dat de cloudprovider zaken kan waarnemen als: a) welke diensten worden gebruikt, b) door wie zij worden gebruikt, c) tijdstip van gebruik, d) periodiciteit van het gebruik, e) geografische verspreiding van gebruik, f) frequentie en volume van gebruik.
In theorie kan hier bepaalde informatie uit worden afgeleid. Een aantal (geheel fictieve) voorbeelden ter illustratie zijn: a) onverwachte pieken in het gebruik kunnen wijzen op opschaling in crisissituaties, of b) het inschakelen van aanvullende beveiligingsfuncties kan wijzen op verhoogde dreiging. Deze wijze van informatie achterhalen wordt vaak als «traffic analysis» aangeduid.

Hoe is dit meegewogen in de risicoanalyse?

Het Rijksbreed cloudbeleid 2022 en het bijbehorende implementatiekader adresseren deze risico's Zo mag staatsgeheim gerubriceerde informatie niet in de public cloud worden gezet. Ook is het mogelijk om aanbieders uit landen met een offensief cyberprogramma tegen Nederland te weren. Verder gelden voor bepaalde gegevens en diensten meer en stringentere voorwaarden.
De risico's die uit «traffic analysis» voortvloeien zullen naar verwachting minder schadelijk zijn dan de algemene cloud risico's die ook door de GroenLinks fractie expliciet worden genoemd, namelijk: a) het risico van «data breaches» met daarbij toegang tot leesbare overheidsdata of b) het risico van toegang tot leesbare overheidsdata door cloudproviders.
In de eerdergenoemde Implementatiekader zijn deze algemene cloud risico's in meer detail beschreven.
In gevallen dat overheidsdata niet leesbaar is voor de dader van een «data breach» of voor de cloudprovider, bijvoorbeeld omdat data versleuteld is, kan toch nog enige informatie worden achterhaald via «traffic analysis». Maar de hoeveelheid achterhaalde informatie zal kleiner zijn en de achterhaalde informatie zal globaler zijn.

In het verlengde hiervan hebben de leden vragen over de afhankelijkheid van Silicon Valley black box technologie. Wat voor afhankelijkheden van black box software solutions ontstaan er op het moment dat de overheid in zee gaat met externe cloudproviders, en wat betekent dit voor onze capaciteit om fundamentele rechten te waarborgen?

In het cloudbeleid is de exit-strategie als voorwaarde opgenomen om vendor lock-in te voorkomen. De departementen houden hun materieel public cloudgebruik en de risico's daarvan bij. Jaarlijks rapporteren de

departementen over het materieel public cloudgebruik en onderliggende risico's aan CIO Rijk. De rapportages, DPIA's en risicoanalyses vormen de input voor de CIO-gesprekken die, in het kader van monitoring en advies, jaarlijks plaatsvinden. CIO Rijk beoordeelt deze op uitzonderlijke risico's, zoals departement overstijgende risico's waaronder stapelingsrisico's.

Blijft er genoeg technische kennis binnen de overheid, wetende dat cloudcomputing black box technologie is?

Met de toenemende digitalisering en aanhoudende schaarste op de arbeidsmarkt wordt het steeds belangrijker om voldoende en de juiste kennis op I in huis te hebben. De Staatssecretaris van Koninkrijksrelaties en Digitalisering zet daar vanuit de I-strategie Rijk in op het thema «I-vakmanschap». Daarbij gaat het niet alleen om het ontwikkelen van rijksbreed beleid om zowel jong talent als de oudere jongere te verleiden bij de overheid te komen en blijven werken (nieuwe mensen binnen halen en houden) maar ook om de kennisontwikkeling bij niet I-personeel te stimuleren (en zittende collega's waar nodig te voorzien van een «I-injectie»). In de Rijksbrede I-Strategie 2021–2025 wordt aandacht besteed aan het vergroten van de kennis en kunde bij ambtenaren op het gebied van digitalisering. Dat gebeurt bijvoorbeeld via de Rijks Academie voor Digitalisering en Informatisering Overheid (RADIO). Cloud computing is één van de onderwerpen waar leeractiviteiten op zijn en worden ontwikkeld.

Beperkt dit onze mogelijkheden om technologie te auditen en te snappen hoe het werkt en leidt dit tot technologische afhankelijkheid van tech bedrijven?

Nee, dit beperkt ons niet zolang er maar contractuele afspraken gemaakt worden waaronder het zogeheten auditrecht. Het is daarnaast ook verplicht een exit strategie te hebben, voordat men naar de cloud gaat, juist om afhankelijkheid te voorkomen.

Is er inzicht in de manier waarop het gebruik van de cloud de manier van werken van de overheid gaat veranderen en zich gaat scharen naar de waarden en behoeftes van de cloudprovider?

De Minister van JenV heeft eerder aangegeven dat de overheid een multi-cloud strategie nastreeft om niet afhankelijk te zijn van één cloudprovider.[8] Er is dus geen sprake van dat we ons gaan scharen naar de waarden en behoeftes van cloudproviders. Daarnaast houdt CIO Rijk vanuit zijn monitorende rol een overzicht bij van materieel public cloudgebruik waarmee dergelijke strategische afhankelijkheden tijdig geïdentificeerd kunnen worden.

De leden van de GroenLinks-fractie hebben vragen over het economisch model van de cloudindustrie. In de brief van de Staatssecretaris wordt zeer beperkt ingegaan op het economische model van de cloudindustrie en hoe deze leert en profiteert van de data die de overheid beschikbaar stelt. Academici zoals Seda Gurses en Cecilia Rikap tonen aan dat de algoritmes, die onderdeel zijn van de cloudservices van grote tech bedrijven, slimmer worden door middel van de data die overheden beschikbaar stellen voor verwerking en analyse. Dit betekent dus dat deze bedrijven direct profiteren van de unieke toegang die ze hebben tot overheidsdata. Hoe kijkt de Staatssecretaris hiernaar?

---

[8] Kamerstuk 26 643 en 32 761, nr. 859

Uitgangspunt is dat contractueel wordt overeengekomen dat een wederpartij de door opdrachtgever (in dit geval een rijksoverheidsorganisatie) verstrekte, en de op basis daarvan in opdracht van opdrachtgever gegenereerde, gegevens en data uitsluitend gebruikt voor het verrichten van de afgesproken prestatie en voor zover dit gebruik noodzakelijk en proportioneel is voor deze prestatie, en er afspraken worden gemaakt over de data, over toegankelijkheid van de gegevens en of die wel/niet voor analyse van de cloudprovider beschikbaar mag komen of niet. Tevens wordt afgesproken, op welke manier aangetoond wordt dat aan die afspraken wordt voldaan (assurance en assurance audit reports). In zijn algemeenheid geldt dat de technische inrichting voor clouddiensten zo opgezet moet worden dat er grote scheiding van rechten is, en toegang tot data op strikte manier wordt gecontroleerd, (voor controle achteraf) wordt vastgelegd, ook voor de cloudprovider zelf.

De voordelen die deze tech bedrijven halen uit het hebben van toegang tot overheidsdata voor het trainen van hun algoritmes roept bij deze leden de vraag op of deze algoritmes niet publiek gemaakt moeten worden. Graag ontvangen deze leden de visie van de Staatssecretaris hierop.

Het kabinet vindt niet dat bedrijven die vrij beschikbare data van de overheid gebruiken om hun algoritmen te trainen, vervolgens ook hun algoritmen dienen te publiceren. Het publiceren van algoritmen kan een deel van het concurrentievoordeel van een bedrijf prijsgeven. Wel dient het gebruik van algoritmen plaats te vinden binnen de reguliere wettelijke kaders.

De leden van de GroenLinks-fractie hebben voorts een vraag over de toegang van buitenlandse inlichtingendiensten. Op welke manier kunnen buitenlandse inlichtingendiensten toegang krijgen tot gegevens wanneer clouddiensten in andere landen gevestigd zijn en onder de wetgeving van het betreffende land vallen?

Wanneer data van Nederlandse gebruikers aanwezig is in datacentra in een derde land, dan is de data onderwerp van de nationale regelgeving van dit derde land. Er zijn landen die in de nationale wetgeving een voorziening hebben opgenomen die rechtmatige toegang tot data verschaft voor inlichtingen- en veiligheidsdiensten. Dat betekent dat de data host kan worden verplicht de data in reactie op een rechtmatig verzoek aan de relevante overheid te overhandigen. Ook kunnen medewerkers op basis van hun nationaliteit onder dergelijke wetgeving en verplichtingen vallen.
In voorkomend geval is in de nationale wetgeving ook een voorziening opgenomen voor toegang tot data indien de clouddienstverlener gevestigd is in een derde land, zoals bijvoorbeeld het geval is bij Verenigde Staten onder de Cloud Act.

Hoe kan Nederland deze gegevens zo goed mogelijk beschermen tegen ongewenste interesse van buitenlandse diensten?

Het is van belang dat een risicoafweging vooraf gaat aan het plaatsen van data in een publieke cloudoplossing. Het gebruik van publieke clouddiensten is daarbij onder geen enkele voorwaarde toegestaan voor staatsgeheim gerubriceerde informatie. Daaruit moet ook volgen welke risico's er bestaan ten aanzien van ongewenste toegang door buitenlandse inlichtingen- en veiligheidsdiensten. Om het risico te beperken kan bijvoorbeeld worden gekozen voor publieke cloudoplossingen waarbij de data in Nederland of een ander Europees land blijft, of voor bijvoorbeeld private cloudoplossingen. De AVG stelt eisen aan gegevensverkeer naar derde landen: Het derde land moet over een «adequaat beschermings-

niveau» beschikken, en als dat niet zo is moet de organisatie die gegevens exporteert waarborgen stellen die ervoor moeten zorgen dat de persoonsgegevens van EU-burgers voldoende beschermd zijn. Een factor die daarbij wordt meegenomen is in welke mate buitenlandse veiligheidsdiensten toegang tot die gegevens hebben.

Tot slot hebben de leden van de GroenLinks-fractie nog enkele losse vragen aan de Staatssecretaris. Voor hoe lang zal een risicoanalyse en een DPIA als geldig beschouwd worden? Heeft de Staatssecretaris de intentie om een nieuwe analyse te doen als servicevoorwaarden veranderen?

De toegespitste risicoafweging, exit-strategie en (pre-scan of formele) DPIA worden bij wezenlijke wijzigingen in de dienstverlening of wezenlijke verandering van de risico's geactualiseerd. Ten minste iedere drie jaar moet een actualisatie van de analyses plaatsvinden, conform de aanbeveling van de AP.[9]

Een andere vraag die bij deze leden nog speelt is de vraag binnen welke termijn naar een alternatieve cloudleverancier overgestapt kan worden wanneer een leverancier nieuwe voorwaarden krijgt waardoor de service niet meer wenselijk of niet meer geschikt is?

Dit is afhankelijk van de leverancier en de gemaakte afspraken en de complexiteit van de af te nemen clouddienst(en).

Indien de overheid gebruik gaat maken van cloudservices zal wat de leden van de GroenLinks-fractie betreft een belangrijke eis moeten zijn dat van de meest energiezuinige state-of-the-art servers gebruik gemaakt wordt en het datacenter restwarmte zal hergebruiken. Deelt de Staatssecretaris dit standpunt?

De Staatssecretaris deelt het standpunt dat energie efficiëntie één van de belangrijke eisen is bij de toekomstige inkoop van public cloud services, conform het beleid Inkopen met impact. Aanbieders dienen duidelijk te maken hoe ze daar inhoud aangeven, daarbij kunnen restwarmte en energie efficiënte van servers van de ingezette datacenters aspecten zijn die meetellen. Naast de in te kopen public cloud service dient ook de leverancier te voldoen aan eisen als het Global Reporting Initiative om geschikt te zijn als aanbieder van public cloud diensten.

Vragen en opmerkingen van de leden van de Volt-fractie

De leden van de Volt-fractie hebben kennisgenomen van het Rijksbreed cloudbeleid 2022. Daarover hebben deze leden nog enkele vragen.
De leden van de Volt-fractie merken op dat de Staatssecretaris in het Rijksbreed cloudbeleid schrijft dat één van de voordelen van het gebruiken van publieke cloudleveranciers is dat zij veel grotere investeringen in informatiebeveiliging doen dan de rijksoverheid zelf wil of kan doen. Om hoeveel investeringen gaat het hier?

Waar het gaat om grote cloudaanbieders is er sprake van enkele van de grootste bedrijven ter wereld, met een jaaromzet van vele miljarden. Het leveren van cyberveilige producten en (cloud)diensten is hun «core business». In augustus 2021 hebben een aantal grote bedrijven gezamenlijk aangekondigd om aanvullende investeringen te doen in

[9] Data Protection Impact Assessment, Autoriteit Persoonsgegevens. Opgehaald van: Data protection impact assessment (DPIA) | Autoriteit Persoonsgegevens

cybersecurity, in overleg met de Amerikaanse overheid.[10] Het is daarbij belangrijk om te realiseren dat dergelijke aanbieders hun investeringen in cybersecurity (deels) doorberekenen aan hun klanten.
Kan de Staatssecretaris uitleggen waarom de rijksoverheid dergelijke investeringen niet wil doen?
Het verkopen van cyberveilige producten, zoals clouddiensten, is voor tech-giganten als Amazon, Microsoft Google, IBM en Apple «core business». Voor de Nederlandse overheid is dat niet het geval. De Nederlandse overheid moet haar budgetten, gebaseerd op politieke keuzes, verdelen over een veelvoud van onderwerpen ook binnen cybersecurity zelf. Het kabinet hecht echter veel waarde aan cybersecurity, en heeft daarom evenals het vorige kabinet structurele middelen vrijgemaakt die specifiek zijn gelabeld voor het verhogen van de digitale weerbaarheid. Het vorige kabinet heeft 95 miljoen structureel geïnvesteerd in de versterking van digitale weerbaarheid.
Daar bovenop investeert dit kabinet een extra 111 miljoen euro structureel in cybersecurity. Deze middelen maken deel uit van een bredere structurele investering van 300 miljoen waarmee onder andere de AIVD en MIVD worden versterkt en investeringen worden gedaan op het gebied van economische veiligheid en de vitale infrastructuur. De genoemde structurele investering van 111 miljoen draagt bij aan het uitvoeren van de verschillende acties die de departementen ondernemen ten behoeve van de realisatie van de doelen uit de Nationale Cybersecurity Strategie.

Welke andere belangen, naast investeringen in beveiliging worden afgewogen bij de keuze om voor publieke cloudleveranciers te kiezen?

Omdat de departementen onderling aanzienlijk verschillen, hangt dit af van de departementale cloudstrategie en -beleid. In de implementatiekader staat dat in de risicoafweging de kosten, baten en risico's verder afgewogen moeten worden.

Uit de beantwoording op schriftelijke vragen van het lid Van Ginneken[11] volgt dat de European Data Protection Board (EDPB) onderzoek doet naar de voor- en nadelen van het gebruik van niet-Europese clouddiensten bij overheidssystemen. De uitkomsten daarvan kunnen volgens de Staatssecretaris worden gebruikt om meer inzicht te geven in de risico's. Welke risico's heeft de Staatssecretaris zelf al in kaart gebracht?

In het Rijksbreed cloudbeleid 2022 zijn de risico's voor staatsgeheime informatie zo hoog ingeschat dat deze niet in de publieke cloud verwerkt mogen worden. Bij de inkoop en aanbesteding van producten en diensten binnen de rijksoverheid worden (eventuele) risico's voor de nationale veiligheid namelijk meegewogen.
Hierbij wordt in het bijzonder gelet op mogelijke risico's voor de continuïteit van vitale processen, spionage, de integriteit en exclusiviteit van kennis en informatie en de ongewenste opbouw van strategische afhankelijkheden. Ook wordt 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. Met het oog op eventuele risico's voor privacy wordt er in het cloudbeleid onderscheid gemaakt tussen gewone persoonsgegevens en bijzondere persoonsgegevens en basisregistratie.

---

[10] https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/
[11] Aanhangsel Handelingen II 2021/22, nr. 3420

Hoe heeft zij die verschillende risico's afgewogen bij het vaststellen van het Rijksbreed cloudbeleid?

Deze risico's zijn afgewogen bij de totstandkoming van het Rijksbreed cloudbeleid 2022 in de interdepartementale samenwerking met CIO's, CISO's en CTO's, inclusief betrokkenheid van Nationaal Bureau Verbindingsbeveiliging (NBV) dat onderdeel is van de AIVD, en het NCSC.

De leden van de Volt-fractie merken op dat de Staatssecretaris in het Rijksbreed cloudbeleid schrijft dat rijksdiensten vrij zijn om aanbieders van clouddiensten te kiezen op basis van hun eigen risicoafweging. Zijn er volgens de Staatssecretaris risico's denkbaar waartegen simpelweg geen enkel voordeel opweegt?

Het risico op spionage voor staatsgeheime informatie is dusdanig groot dat daar geen enkel voordeel tegen opweegt. Daarom is staatsgeheime informatie uitgesloten van de publieke cloud.

Zoals bijvoorbeeld het onderbrengen van persoonsgegevens bij een dienst die (deels) eigendom is van de Chinese staat?

Bij de beoordeling van risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere partijen bij digitale producten hanteert het kabinet de overwegingen die zijn vermeld in de brief aan de Tweede Kamer over C2000, van 26 april 2019 (Kamerstuk 25 124, nr. 96). Hierbij wordt o.a. meegewogen of een partij afkomstig is uit een land met een offensief cyberprogramma. De overwegingen worden in samenhang met elkaar bezien en alleen wanneer alle overwegingen van toepassing zijn, en blijkt dat nationale veiligheidsrisico's niet voldoende kunnen worden beheerst, worden waar mogelijk partijen uitgesloten.

Welke middelen en bevoegdheden heeft de Staatssecretaris om in te grijpen als een Rijksdienst desondanks van plan is hiervoor te kiezen?

Het Rijksbreed cloudbeleid 2022 is interdepartementaal tot stand gekomen via de ICBR en goedgekeurd door de ministerraad. De departementen rapporteren jaarlijks aan CIO Rijk over het materieel public cloudgebruik en de risico's daarvan. De ontvangen rapportages, DPIA's en risicoafwegingen gebruikt CIO Rijk conform het cloudbeleid en het CIO-stelsel in de jaarlijkse cyclus van de CIO-gesprekken als onderdeel van diens monitorings- en adviesfunctie. De departementen voeren daarnaast jaarlijks hun eigen controles uit. Naast het aanleveren van informatie over materieel public cloudgebruik, is er ook de jaarlijkse rapportagesystematiek voor departementen, waarbij zij hun eigen audit uitvoeren. De ADR voert, als onafhankelijke internal auditor van de rijksoverheid, audits uit. Waarbij de ARK, als onafhankelijk instituut, vooral een controlerende rol heeft. Voor wat betreft persoonsgegevens is de Autoriteit Persoonsgegevens (AP) de toezichthouder.

Is het voor de departementen daadwerkelijk mogelijk om regie te houden over de persoonsgegevens waarvoor zij verwerkingsverantwoordelijke zijn?

Ja, zolang voldaan wordt aan bestaande wet- en regelgeving, waaronder de AVG en het Rijksbreed cloudbeleid 2022. De FG zal, als onderdeel van hun toezichthoudende rol (AVG, artikel 39), betrokken zijn bij het toezicht op de privacyrisico's binnen de organisaties.

Op welke manier is de Staatssecretaris voornemens om dit te coördineren en daar toezicht op te houden?

Jaarlijks rapporteren de departementen over het materieel public cloudgebruik en onderliggende risico's aan CIO Rijk. De rapportages, DPIA's en risicoanalyses vormen de input voor de CIO-gesprekken die, in het kader van monitoring en advies, jaarlijks plaatsvinden. Naast deze periodieke rapportage voeren de departementen ook eigen audits en controles uit. De ADR voert, als onafhankelijke internal auditor van de rijksoverheid, audits uit. Waarbij de ARK, als onafhankelijk instituut, vooral een controlerende rol heeft.

De leden van de Volt-fractie vragen hoe de Staatssecretaris oordeelt over de spanning tussen de Europese AVG en de Amerikaanse Cloud Act. Op basis van de AVG moeten immers afspraken gemaakt worden over de verwerking van persoonsgegevens met derdelanden en tussen verantwoordelijken en verwerkers, maar die contractuele afspraken houden in principe geen stand tegenover de verplichting in de Cloud Act om gegevens te delen met de Amerikaanse overheid. Is het wel mogelijk om aan de Europese wettelijke verplichtingen te voldoen en tegelijkertijd gegevens bij de Amerikaanse partij op te slaan?

De Cloud Act maakt het inderdaad mogelijk dat, ondanks contractuele afspraken, de Amerikaanse overheid toegang kan krijgen tot (persoons-)gegevens van Nederlandse burgers als dat in het belang is van de nationale veiligheid. Volgens recent onderzoek van Greenberg Traurig is dit risico weliswaar voorstelbaar maar in de praktijk (heel) klein. Om eventuele risico's hieromtrent tegen te gaan en in lijn met de Aanbevelingen van de EDPB inzake internationale gegevensdoorgifte, bevatten internationale contracten, veelal gebaseerd op de Standard Contractual Clauses van de Europese Commissie[12], de verplichting om een adequate risicoafweging te maken aan de hand van een Data Transfer Impact Assessment (DTIA). In deze DTIAs wordt onder meer rekening gehouden met de Cloud Act en de eventuele gevolgen daarvan voor betrokkenen. Een uitkomst van een dergelijke risicoafweging kan zijn dat er aanvullende waarborgen moeten worden genomen om de juiste toepassing van de SCC's te garanderen en ervoor te zorgen dat het door de AVG vereiste beschermingsniveau wordt gewaarborgd.
De Autoriteit Persoonsgegevens (AP) onderschrijft deze werkwijze in haar brief d.d. 11 november 2022 inzake het Rijksbrede Cloudbeleid[13]; «De AP adviseert dan ook nadrukkelijk om, voorafgaand aan het inzetten van een clouddienst, een Transfer Impact Assessment (TIA) uit te (laten) voeren. Hierdoor kunnen risico's tijdig worden geïdentificeerd zodat er, indien mogelijk, aanvullende maatregelen kunnen worden getroffen om ervoor te zorgen dat het fundamentele recht op bescherming van persoonsgegevens wordt gewaarborgd bij de inzet van een clouddienst en tevens de continuïteit van essentiële dienstverlening kan worden gewaarborgd.« Een positieve ontwikkeling in dit verband is voorts dat de VS op 7 oktober jongstleden nieuwe regelgeving heeft aangenomen waarin concrete wijzigingen op het gebied van gegevensbescherming worden doorgevoerd, onder andere wat betreft de toegang tot Europese persoonsgegevens door Amerikaanse overheidsinstanties, in het bijzonder inlichtingen- en veiligheidsdiensten. De Europese Commissie is positief over deze nieuwe regelgeving en gaat ervan uit dat dit als basis kan fungeren voor een nieuw adequaatheidsbesluit.
Met het antwoord op deze vraag wordt tevens tegemoetgekomen aan de toezegging uit het debat Digitaliserende overheid met de Staatssecretaris van Koninkrijksrelaties en Digitalisering van 5 oktober 2022 om een brief te sturen rondom het Trans-Atlantic Privacy Data Framework.

---

[12] SCC's zijn een van de doorgiftemechanismen genoemd in artikel 46 AVG en het meest gebruikt instrument voor internationale doorgiften.
[13] brief_over_rijksbreed_cloudbeleid_2022.pdf (autoriteitpersoonsgegevens.nl) p. 3–4.

Hoe kan worden gegarandeerd dat gegevens de EU niet verlaten, althans niet bij buitenlandse overheden terecht komen?

Het Rijksbreed cloudbeleid schrijft niet voor dat gegevens altijd binnen de EU moeten blijven. Staatsgeheime informatie mag sowieso niet in de public cloud worden geplaatst, vanwege de mogelijke risico's. Voor persoonsgegevens bevat het cloudbeleid kaders die voorschrijven op welke wijze met persoonsgegevens moet worden omgegaan. Ook omschrijft het onder welke voorwaarden eventuele doorgifte wel of niet is toegestaan. Om eventuele risico's tegen te gaan is er, en in lijn met de Aanbevelingen van de European Data Protection Board inzake internationale gegevensdoorgifte, de verplichting om een adequate risicoafweging te maken aan de hand van een Data Transfer Impact Assessment (DTIA). In deze DTIAs wordt onder meer rekening gehouden met buitenlandse wet- en regelgeving en de eventuele gevolgen daarvan voor betrokkenen. Een uitkomst van een dergelijke risicoafweging kan zijn dat er aanvullende waarborgen moeten worden genomen om ervoor te zorgen dat het door de AVG vereiste beschermingsniveau wordt gewaarborgd.

In aanvulling op het voorgaande. Heeft de Staatssecretaris de mogelijkheid om de Europese waarden te borgen

Kaders en regels gesteld op Europees niveau zijn altijd van toepassing, zo ook op dit Rijksbreed cloudbeleid 2022. Dit geldt hier onder meer voor de waarde die wij in Europa hechten aan privacy, zoals geborgd in de AVG.

Kan de Staatssecretaris toelichten welke waarden zij precies bedoelt als zij het heeft over Europese waarden?

In de aanbiedingsbrief bij de werkagenda «Waardengedreven Digitaliseren» heb ik veiligheid, democratie, zelfbeschikking, privacy en transparantie als publieke waarden geïdentificeerd, die het uitgangspunt zijn vanuit waar we naar digitalisering kijken. Vanuit deze waarden zet ik mij in Europa in om het voortouw te nemen in een sterkere samenwerking tussen EU-lidstaten rond digitalisering.

Tijdens de technische briefing inzake Rijksbreed cloudbeleid d.d. 20 oktober 2022 is eveneens gevraagd naar Europese alternatieven, waaronder Gaia-X. Heeft de Staatssecretaris er vertrouwen in dat dit project als alternatief voor Amerikaanse cloudleveranciers kan werken?

Het kabinet steunt op verschillende manieren de ontwikkeling van Europese clouddiensten, onder andere via de IPCEI CIS en GAIA-X. Beide projecten dragen bij aan de ontwikkeling van een nieuwe generatie cloudoplossingen door marktpartijen, op basis van Europese waarden en regels. Samen met beleidsinitiatieven gericht op het beter laten functioneren van de markt, zoals de Dataverordening en DMA, draagt dit in de ogen van het kabinet bij aan het ontwikkelen van alternatieven voor Amerikaanse cloudleveranciers met als ambitie om tot een volwaardig Europees aanbod te komen.

Zijn er *best-practices* in andere lidstaten binnen de EU, die we kunnen gebruiken voor het vaststellen van ons Rijksbreed cloudbeleid? Bijvoorbeeld landen waarin expliciet een andere afweging is gemaakt ten aanzien van de verwerking van staatsgeheime gegevens of bijzondere en gevoelige persoonsgegevens? Zijn die geconsulteerd?

Het Rijksbreed cloudbeleid 2022 is reeds vastgesteld en op 29 augustus 2022 aan de Kamer gestuurd. Een onderdeel daarvan is de evaluatie die in

2023 gestart zal worden, en waarna er een eventuele update van het beleid zal volgen. Bij totstandkoming van het Rijksbreed cloudbeleid 2022 zijn ontwikkelingen op Europees niveau meegewogen. Er zijn in de totstandkoming van het Rijksbreed cloudbeleid 2022 geen consultaties met specifieke landen geweest. In de evaluatie die zal starten in 2023 zullen Europese ontwikkelingen gemonitord worden.

In 2020 hebben de EU-lidstaten gezamenlijk verklaard toe te werken naar een Europese cloud en daarbij onder andere te streven naar hoge standaarden op het gebied van energie-efficiëntie. Toch komt deze overweging niet terug in de lijst met voorwaarden voor het gebruik van de publieke cloud voor de rijksdiensten. Waarom is ervoor gekozen om energie-efficiëntie hierin niet op te nemen?

Rijksdiensten dienen in te kopen volgens het Rijksinkoopbeleid: «Inkopen met impact». Energie-efficiëntie is onderdeel van de doelstellingen.

Zijn er andere manieren waarop rijksdiensten worden aangemoedigd om dit in de overweging mee te nemen?

Duurzaam, sociaal en innovatief inkopen is de standaard van de rijksoverheid. Dit staat beschreven in de strategie Inkopen met Impact van de rijksoverheid. Elk departement en/of organisatieonderdeel vertaalt de rijksdoelen naar eigen, specifieke doelen en legt die vast in Maatschappelijk Verantwoord Inkopen (MVI)-actieplannen, categorieplannen en routekaarten.