Cloudbeleid - Ministerie van Financiën (CB-MinFin)

Datum 4 december 2023

Colofon

Versienummer	1.0
Contactpersoon	E. Baardman Enterprise Architect M 06 52 50 25 09 Concerndirectie Informatievoorziening en Databeheersing | Architectuur e.baardman@belastingdienst.nl

Inhoud

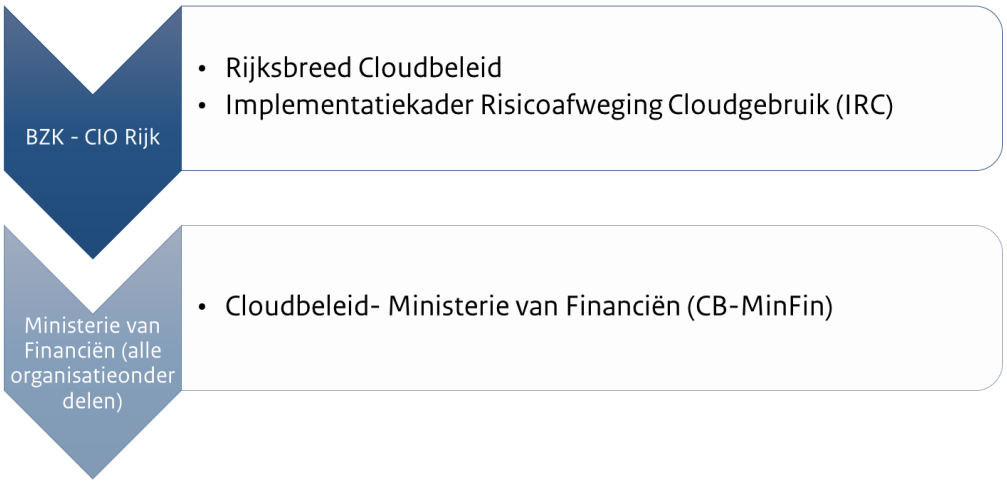
1 Inleiding

1.1 Achtergrond

Op 19 augustus 2022 is het Rijksbreed Cloudbeleid 2022 goedgekeurd door de ministerraad. Dit beleid stelt dat alle departementen, uitvoerings- en andere overheidsorganisaties hun eigen cloudbeleid en cloudstrategie formuleren op basis van het Rijksbreed Cloudbeleid 2022. Het Ministerie van Defensie valt buiten de scope van het Rijksbreed Cloudbeleid. In het Rijksbreed Cloudbeleid 2022 is aangekondigd dat er nog een "implementatierichtlijn risicoafweging cloudgebruik" in 2022 zou worden opgesteld. Deze is 20 december 2022 opgeleverd onder de noemer "Implementatiekader risicoafweging cloudgebruik" en goedgekeurd door het ICBR.

Het Rijksbreed Cloudbeleid 2022 en het Implementatiekader Risicoafweging Cloudgebruik (**IRC)** vormen het beleid waar alle onderdelen van het Ministerie van Financiën aan moeten voldoen. Het Cloudbeleid – Ministerie van Financiën (**CB-MinFin**) is een aanvulling en verdieping/concretisering op genoemde stukken en vervangt het Afwegingskader Cloud Financiën uit 2021. Het CB-MinFin vervangt ook het Beleid voor Publieke Clouddiensten uit 2019 voor de DG's Belastingen, Douane en Toeslagen.

In het CB-MinFin is het kaderstellende deel van het Rijksbreed Cloudbeleid 2022 en het IRC overgenomen, zodat alles bij elkaar staat in 1 document (zie Figuur *1*).



Figuur 1: Samenhang cloudbeleidsstukken

1.2 Doelstelling

Het CB-MinFin geeft aan binnen welke beleidskaders een clouddienst gebruikt mag worden door een directie/keten voor een gedefinieerd bedrijfsproces en gedefinieerde gegevensset waar de directie/keten verantwoordelijk voor is.

1.3 Scope

Het Cloudbeleid – Ministerie van Financiën (CB-MinFin):

- is van toepassing op het gehele Ministerie van Financiën met onderliggende organisatieonderdelen. Hierna wordt dit samengevat als: **de organisatieonderdelen**;
- schrijft voor binnen welke beleidskaders een clouddienst gebruikt mag worden. Het bevat niet de cloudstrategie dat aangeeft wanneer het gebruik van clouddiensten gewenst is binnen een organisatieonderdeel;
- schrijft voor aan welke verplichtingen bij verwerving en gebruik van clouddiensten voldaan moet worden;
- is van toepassing op het gebruik van clouddiensten die, rechtstreeks of via een samenwerkingspartner of via een overheidsdienst, aangeboden worden door een commerciële partij;
- is van toepassing op het bestaand gebruik van clouddiensten en bij het voornemen tot gebruik van clouddiensten.

1.4 Leeswijzer

Hoofdstuk 2 beschrijft de definities van een aantal relevante begrippen.

Hoofdstuk 3 beschrijft in beknopte vorm het beleidskader.

Hoofdstuk 4 beschrijft een nadere uitwerking van het beleidskader en de daaraan gekoppelde taken en verantwoordelijkheden voor verschillende rollen.

Hoofdstuk 3 en 4 bevatten de beleidsregels uit het Rijksbreed Cloudbeleid en het IRC en de aanvullende MinFin beleidsregels. De beleidsregels uit het Rijksbreed Cloudbeleid en van het IRC zijn waar mogelijk specifiek geduid.

Er is een analysemodel (opvraagbaar) waarin precies te zien is welke regels vanuit het Rijksbreed Cloudbeleid en het IRC waar zijn overgenomen en/of nader uitgewerkt.

Hoofdstuk 5 gaat specifiek in op de rollen Cloud Broker en Cloud Auditor, omdat dit nieuwe rollen zijn.

In de Bijlage – Verantwoording is een toelichting te vinden over hoe bepaalde beleidsregels uit het Rijksbreed Cloudbeleid en het IRC zijn geduid en verwerkt.

2 Begrippen

Dit hoofdstuk beschrijft de definities van een aantal relevante begrippen die in dit beleidsdocument gehanteerd worden.

2.1 Cloud computing

Cloud computing[1] 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:

1. On-demand selfservice: naar behoefte verkrijgbaar zonder menselijke interactie met de leverancier
2. Breed beschikbare netwerktoegang: te gebruiken via een gestandaardiseerde netwerkverbinding
3. Gedeelde resources: computermiddelen worden gedeeld door verschillende afnemers
4. Snelle elasticiteit: gebruik is snel op en af te schalen. Beschikbare computermiddelen lijken onbeperkt
5. Afgemeten dienstverlening: het verbruik is meetbaar, transparant en eenduidig

2.2 Cloud implementatiemodellen

De veel gehanteerde definities van de NIST[1] voor de cloud implementatiemodellen zijn:

Publieke clouddienst (*public cloud*): een *cloud computing* dienst die aangeboden wordt voor open gebruik door het grote publiek. Het kan eigendom zijn van, worden beheerd door en worden geëxploiteerd door een commerciële, academische of overheidsorganisatie, of een combinatie ervan. Het wordt aangeboden vanuit de datacenters van de clouddienst leverancier.
In de Rijksoverheidscontext is veelal sprake van het eigendomsrecht van een commerciële partij. De beheer- en exploitatieverantwoordelijkheid wordt mede bepaald door de soort clouddienst (zie paragraaf 2.3) die wordt afgenomen.

Private clouddienst (*private cloud)*: een *cloud computing dienst* die aangeboden wordt aan één organisatie bestaande uit meerdere consumenten (bijvoorbeeld bedrijfsonderdelen). Het kan eigendom zijn van en beheerd door de organisatie, een derde partij of een combinatie daarvan. Het wordt aangeboden vanuit eigen datacenters (*on premise*) of vanuit datacenters van een derde partij (*off premise*).

Hybride clouddienst (*hybrid cloud*): een *cloud computing* dienst die is samengesteld uit twee of meerdere implementatiemodellen (public, private or community) die elk als zelfstandige entiteit gekoppeld zijn met elkaar door technologie die overdraagbaarheid (portabiliteit) van gegevens en applicaties ondersteund.

[1] NIST 800-145: The NIST Definition of Cloud Computing

Community clouddienst (*community cloud*): een *cloud computing* dienst die aangeboden wordt voor exclusief gebruik door een specifieke groep gebruikers van organisaties die gemeenschappelijke belangen hebben. Het eigenaarschap, beheer en exploitatie kan liggen bij één van de deelnemende organisatie, een derde partij of een combinatie. Het wordt aangeboden vanuit eigen datacenters (*on premise*) of vanuit datacenters van een derde partij (*off premise*).

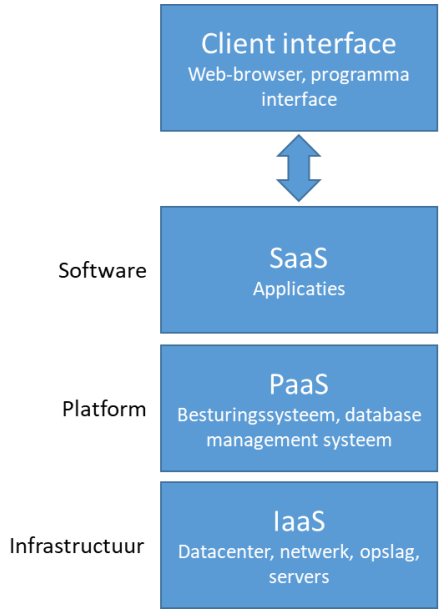
2.3 Soorten clouddiensten

Het aantal soorten clouddiensten neemt door de jaren heen toe. De belangrijkste worden hieronder beschreven.

Business Process as a Service (BPaaS)[2]: een *cloud computing* dienst voor de levering van business process outsourcing (BPO)-services. Dit soort diensten zijn vaak geautomatiseerd en waar menselijke procesactoren nodig zijn, is er geen specifieke toegewezen groep medewerkers voor een klant.

Software as a Service (SaaS)[1]: een *cloud computing* dienst waarbij applicaties op een cloudinfrastructuur worden aangeboden. De applicaties zijn toegankelijk vanaf verschillende devices via een thin client-interface, zoals een webbrowser (bijv. webgebaseerde e-mail), of een programma-interface. De klant beheert of controleert geen onderliggende cloudinfrastructuur inclusief netwerk, servers, besturingssystemen, opslag of zelfs individuele applicatiefunctionaliteiten, met de mogelijke uitzondering van beperkte gebruikersspecifieke applicatieconfiguratie-instellingen.

Platform as a Service (PaaS)[1]: een *cloud computing* dienst waarbij cloudinfrastructuur wordt aangeboden waarop de klant eigen gemaakte applicaties of aangekochte applicaties kan implementeren. De klant voert geen beheer op de onderliggende cloudinfrastructuur, inclusief netwerk, servers, besturingssystemen of opslag. De klant heeft controle over de geïmplementeerde applicaties en mogelijke configuratie-instellingen voor de applicatie-hostingomgeving.



Figuur 2: Soorten clouddiensten

Infrastructure as a Service (IaaS)[1]: een *cloud computing* dienst waarbij rekencapaciteit, opslag, netwerken en andere fundamentele verwerkingscapaciteit wordt aangeboden waarmee de klant willekeurige software kan implementeren en draaien, zoals operating systems en applicaties. De klant voert geen beheer op de onderliggende cloudinfrastructuur. De klant beheert de besturingssystemen, opslag en geïmplementeerde applicaties. De klant beheert mogelijk een beperkt deel van de netwerkcomponenten (bijvoorbeeld: firewalls).

[2] https://www.gartner.com/en/information-technology/glossary/business-process-as-a-service-bpaas

Backend as a Service (BaaS)[3]: een *cloud computing* dienst specifiek voor ontwikkelaars van apps om hun applicaties uniform te koppelen aan backend cloudopslag en backend applicaties die functionaliteiten bieden voor gebruikersbeheer, push meldingen en integratie met sociale netwerkdiensten.

2.4 Cloud rollen

Er zijn een aantal rollen te onderscheiden bij het gebruik van clouddiensten:

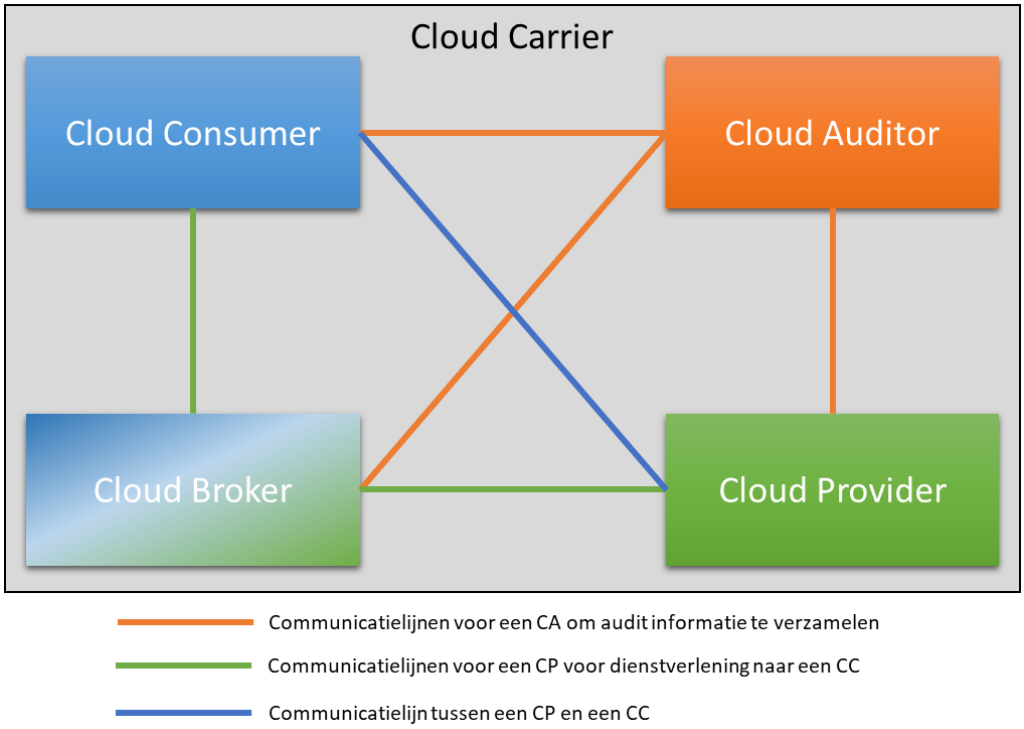
Cloud Consumer (CC)[4]: een persoon of organisatie die een zakelijke relatie onderhoudt met en gebruik maakt van clouddiensten van Cloud Providers.

Cloud Provider (CP)[4]: een persoon of organisatie die verantwoordelijk is voor het aanbieden van clouddiensten voor geïnteresseerden.

Cloud Broker (CB)[4]: een organisatie(onderdeel) die het gebruik, de prestaties en de levering van de clouddiensten beheert en onderhandelt over relaties tussen Cloud Providers en Cloud Consumers.

Cloud Auditor (CA)[4]: een partij die onafhankelijk onderzoek kan doen naar clouddiensten, systeembeheeractiviteiten, prestaties en beveiliging van de cloud implementatie.

Cloud Carrier[4]: een tussenpersoon die zorgt voor connectiviteit en transport van de clouddiensten van Cloud Providers tot Cloud Consumers.



Figuur 3: Cloud rollen en hun communicatielijnen

[3] https://en.wikipedia.org/wiki/Mobile_backend_as_a_service
[4] NIST 500-292, Cloud Computing Reference Architecture

2.5 Overige begrippen

2.5.1 *Verwerken*

Een bewerking of een geheel van bewerkingen met betrekking tot gegevens of een geheel van gegevens (administratie), al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

[bron: AVG, artikel 4, lid 2 en veralgemeniseerd naar alle soorten gegevens]

2.5.2 *Te Beschermen Belang*

Personen, informatie, informatiesystemen, materieel, goederen, imago en objecten, waarbij in geval van compromittering, of de mogelijkheid van compromittering, nadelige gevolgen, of een risico daarop, kan ontstaan voor de vertrouwelijkheid, beschikbaarheid en integriteit van de primaire processen van de rijksoverheid, delen daarvan of voor andere belangen van de Staat, van zijn bondgenoten of van één of meer ministeries.

[bron: Artikel 1, lid k, Besluit BVA-stelsel Rijksdienst 2021]

2.5.3 *Materieel public cloudgebruik*

Materieel public cloudgebruik is gebruik van public 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. Ter verduidelijking: hieronder vallen ook daarbij ondersteunende bedrijfsvoeringsprocessen voor zover van wezenlijk belang voor de primaire taken.

[bron: Implementatiekader Risicoafweging Cloudgebruik]

Er is sprake van "wezenlijk belang" als ten minste aan één van onderstaande criteria wordt voldaan:

- Essentieel voor het kunnen uitvoeren van de kerntaken van de organisatieonderdelen van het Ministerie van Financiën (zoals o.a. beschreven in het Introductiedossier Bewindspersonen);
- Verwerking van een – niet openbaar - significant deel van de gegevens van een bedrijfsvoeringsfunctie (bijvoorbeeld: financiële gegevens en gegevens op gebied van inkoop, personeel, (fysieke) beveiliging, etc.);
- Beheer en monitoring van de digitale infrastructuur en panden;
- Beveiliging van te beschermen belangen.

2.5.4 *Risicoanalyse*

De term risicoanalyse wordt in het Rijksbreed Cloudbeleid en het IRC vaak gebruikt in de context van informatiebeveiliging. In deze beleidsstukken wordt niet het deelproces risicoanalyse als onderdeel van risicomanagement bedoeld, maar alle deelprocessen van risicomanagement vanaf vaststelling van de context tot en met het kiezen en implementeren van maatregelen en accepteren van de rest risico's (risicobehandeling).

Voor de herkenbaarheid en herleidbaarheid wordt de terminologie van het Rijksbreed Cloudbeleid en het IRC overgenomen, maar moet het dus gelezen worden als de processen van risicomanagement zoals beschreven in de ISO31000 en ISO27005.

2.5.5 Formele DPIA

Een DPIA zoals bedoeld in artikel 35 van de AVG.
[bron: Implementatiekader Risicoafweging Cloudgebruik]

2.5.6 Pre-scan DPIA

Een analyse om conform de AVG vast te stellen of een formele DPIA noodzakelijk is.
[bron: Implementatiekader Risicoafweging Cloudgebruik]

De criteria om te bepalen of een formele DPIA noodzakelijk is staan in artikel 35 (lid 1,3,4 en 5) van de AVG en het Besluit lijst verplichte DPIA van de Autoriteit Persoonsgegevens (conform artikel 35, lid 4 van de AVG).

2.5.7 Data Transfer Impact Analysis (DTIA)

Nodig bij internationale overdracht naar landen buiten de Europese Economische Ruimte (EER) zonder een adequaatheidsbesluit. Deze term is geïntroduceerd vanwege de aanbevelingen van European Data Protection Board voor het realiseren van voldoende waarborgen.
[bron: Implementatiekader Risicoafweging Cloudgebruik]

De DTIA ziet op een analyse van de privacy impact wanneer een doorgifte van persoonsgegevens naar een ontvanger buiten de EU/EER plaatsvindt. De DPIA ziet op een analyse van de privacy impact van de voorgenomen verwerking van persoonsgegevens op de betrokkene.

2.5.8 Bijzondere persoonsgegevens

De AVG ziet deze persoonsgegevens als bijzondere persoonsgegevens:

- persoonsgegevens waaruit ras of etnische afkomst blijkt;
- persoonsgegevens waaruit politieke opvattingen blijken;
- persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;
- persoonsgegevens waaruit het lidmaatschap van een vakvereniging blijkt;
- gegevens over iemands gezondheid;
- gegevens over iemands seksueel gedrag of seksuele gerichtheid;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon.

[bron: AVG, Artikel 9, lid 1 en Autoriteit Persoonsgegevens]

3 Beleidskader

3.1 Uitgangspunten

Deze paragraaf bevat de uitgangspunten die zijn gehanteerd bij de formulering van het beleidskader:

1. De inzet van clouddiensten wordt niet bij voorbaat uitgesloten vanuit het oogpunt van privacy.
2. Clouddienstverlening is in de meeste opzichten niet anders dan andere soorten van IV-dienstverlening. Veel van de kaders en regels die gelden voor on-premise oplossingen, gelden ook voor cloud toepassingen. Bijvoorbeeld: AVG, BIO en archiefwet.
3. Toezicht (bijvoorbeeld door de BVA, CIO, CISO en FG) vindt plaats conform de taken, bevoegdheden en verantwoordelijkheden zoals van toepassing bij andere soorten van IV-dienstverlening.
4. Cloud is een vorm van uitbesteding, waarbij de organisatieonderdelen van het Ministerie van Financiën[5] altijd zelf integraal verantwoordelijk blijven, ongeacht de leverancier.

3.2 Beleidsregels

In deze paragraaf staan beknopt de beleidsregels beschreven. Er zijn 3 soorten beleidsregels:

1. Restricties: regels die beschrijven wanneer een clouddienst, aangeboden door een commerciële CP, niet gebruikt mag worden.
2. Mogelijkheden: regels die specifieke situaties beschrijven wanneer een clouddienst, aangeboden door een commerciële CP, gebruikt mag worden
3. Verplichtingen: regels die procedurele, inhoudelijke en administratieve verplichtingen beschrijven.

De beleidsregels zijn geen keuzemenu. Ze zijn aanvullend op elkaar van toepassing. De beleidsregels kennen nog detaileisen en zijn relevant voor specifieke rollen. Die uitwerking staat in hoofdstuk 4.

CIO Rijk heeft haar Rijksbreed Cloudbeleid gericht op publieke clouddiensten en geadviseerd om het ook van toepassing te laten zijn voor private clouddiensten. Het Ministerie van Financiën heeft dat advies overgenomen en de formuleringen van CIO Rijk in die bredere context aangepast in de beleidsregels (zie ook paragraaf 10.2).

In de beleidsregels van CIO Rijk staan op een aantal plaatsen de verplichting tot consultering of het informeren van CIO Rijk. Hierbij wordt CIO Rijk als organisatie entiteit bedoelt en niet "de" CIO Rijk. Feitelijk wordt "de" CISO Rijk bedoelt die onder de CIO Rijk ressorteert[6]. De formuleringen van CIO Rijk zijn in die context aangepast in de beleidsregels.

[5] De minister is primair accountable voor het voldoen aan het Rijksbreed Cloudbeleid en via het mandaatbesluit de DG

[6] Conform artikel 10, lid 3 CIO stelsel

3.2.1 Restricties

Rijksbreed Cloudbeleid	
R1.	Informatie met een VIR-BI rubricering Staatsgeheim Confidentieel of hoger mag niet met clouddiensten verwerkt worden die, direct of indirect, aangeboden worden door commerciële CP's[7]. Aanvulling vanuit Implementatiekader Risicoafweging Cloudgebruik Dit geldt ook voor NATO-informatie met een classificatie hoger dan NATO Restricted.
R2.	Bijzondere persoonsgegevens mogen in principe niet verwerkt worden met clouddiensten die, direct of indirect, aangeboden worden door commerciële CP's[7]. Uitzonderingen hierop zijn mogelijk op basis van 'pas-toe-of-leg-uit' (comply or explain).
R3.	Een basisregistratie, of bronnen van basisregistraties, mag/mogen in principe niet met clouddiensten verwerkt worden die, direct of indirect, aangeboden worden door commerciële CP's[7]. Uitzonderingen hierop zijn mogelijk op basis van 'pas-toe-of-leg-uit' (comply or explain) en als vooraf advies wordt ingewonnen bij de CISO Rijk. De restrictie komt voort uit beschikbaarheidsrisico's voor de vele processen die afhankelijk zijn van de basisregistraties.
R4.	Er worden nooit clouddiensten, direct of indirect, afgenomen van CP's[7] uit landen met een offensief cyberprogramma[8] tegen de 6 Nationale Veiligheidsbelangen.

Aanvullend beleid Ministerie van Financiën	
R5.	Verwerking van persoonsgegevens met clouddiensten die, direct of indirect, aangeboden worden door commerciële CP's[7] is alleen toegestaan als voldaan kan worden aan ten minste één van de vereisten inzake doorgiften van persoonsgegevens (hoofdstuk V van de AVG): 1. binnen de Europese Economische Ruimte (EER), of 2. in landen waarvoor een adequaatheidsbesluit bestaat of 3. op basis van een passend doorgiftemechanisme dat voldoet aan de vereisten (van art. 46, hoofdstuk V) van de AVG, zoals een door de Autoriteit Persoonsgegevens goedgekeurd modelcontract (standaard contractbepalingen of 'standard contractual clauses'). Het Rijksbreed Cloudbeleid laat ruimte open om van de AVG verordening af te wijken[9]. Het Ministerie van Financiën houdt zich strikt aan de verordening.
R6.	Concreet betekent R3 voor het Ministerie van Financiën dat de Basisregistratie Inkomen (BRI) en de relevante bronnen uit de Inkomensheffing en van het UWV in principe niet met clouddiensten verwerkt mogen worden.

[7] Zie verantwoording paragraaf 10.2

[8] De veiligheidsdiensten bepalen dit en is o.a. terug te vinden in het jaarlijkse Cybersecuritybeeld Nederland.

[9] Het Rijksbreed Cloudbeleid stelt: "Indien niet aantoonbaar aan één van de 3 eisen is voldaan, dan wordt voor die verwerking en alle daarbij behorende subverwerkingen de uitgevoerde DPIA zo spoedig mogelijk na vaststelling aan CIO Rijk toegezonden."

Aanvullend beleid Ministerie van Financiën	
	Wanneer er toch redenen (comply or explain) zijn om de verwerking middels clouddiensten plaats te laten vinden, dan mag dit alleen middels private clouddiensten. Dit ter verkleining van vertrouwelijkheidsrisico's.
R7.	Het Ministerie van Financiën heeft aan het Ministerie van Binnenlandse zaken de vraag gesteld of R3 ook van toepassing is op administraties die grote kopie-populaties van basisadministraties bevatten. Het antwoord daarop is: nee. Het Ministerie van Financiën sluit niet uit dat voor dit soort administraties gelijksoortige risico's spelen als voor de basisadministraties zelf. Daarom stelt het Ministerie van Financiën expliciet dat alle andere beleidsregels die in dit document staan wel van toepassing zijn en in het bijzonder V1 en V8.

3.2.2 *Mogelijkheden*

Rijksbreed Cloudbeleid	
M1.	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.

Implementatiekader Risicoafweging Cloudgebruik	
M2.	Indien een departement vragen heeft over de juiste toepassing van het cloudbeleid of het implementatiekader, wordt advies gevraagd aan de CISO Rijk.

Aanvullend beleid Ministerie van Financiën	
M3.	Gebruik van community clouddiensten samen met organisaties die niet gehouden zijn aan het Rijkscloudbeleid maar wel gehouden zijn aan de Baseline Informatiebeveiliging Overheid (BIO), 2019 is toegestaan. De juridische constructie en daaraan gekoppelde verantwoordelijkheden van de deelnemende organisaties moet duidelijk zijn. De desbetreffende CISO moet vooraf geïnformeerd worden. Deze beleidsregel komt voort uit bestaande casussen. Het Rijksbreed Cloudbeleid geeft op dit punt te weinig richting.
M4.	Gebruik van community clouddiensten samen met organisaties die niet vallen onder de criteria van M3 is in principe mogelijk, mits vooraf aantoonbaar afstemming heeft plaatsgevonden met en aantoonbaar toestemming is verleend door de desbetreffende CISO.

3.2.3 *Verplichtingen*

Rijksbreed Cloudbeleid	
V1.	Voor de verwerking van persoonsgegevens met clouddiensten die, direct of indirect, aangeboden worden door commerciële CP's[7] dient een pre-scan DPIA en bij een hoog risico een formele DPIA gemaakt te worden.

Rijksbreed Cloudbeleid	
V2.	Alle typen clouddienstverlening moeten voldoen aan bestaande voorwaarden voor ICT-dienstverlening[10].
V3.	Er dient een 'exit strategie' opgenomen te zijn in de overeenkomst met de CP.
V4.	Er dient in de overeenkomst te staan hoe de CP controle en verantwoordings-onderzoeken toelaat of daarover rapporteert; er bestaat een 'right-to-audit' voor de CC of er is hierover contractueel voldoende zekerheid via Strategisch Leveranciers Management (SLM[11]).
V5.	Besluitvorming over het gebruik van een clouddienst moet door de verantwoordelijk minister[12] toetsbaar en auditeerbaar zijn.
V6.	Besluitvorming over het gebruik van een clouddienst moet in het kader van de Wet open overheid (Woo) openbaar gemaakt worden[13].

Implementatiekader Risicoafweging Cloudgebruik	
V7.	Als een departement zich niet kan houden aan het cloudbeleid of het implementatiekader, bijvoorbeeld omdat (onderdelen van) de analyses informatie bevatten die niet gedeeld mogen worden, wordt door de desbetreffende CISO in overleg getreden met de CISO Rijk. Hierdoor wordt CISO Rijk in staat gesteld zijn monitorende en adviserende rol uit te voeren.

Aanvullend beleid Ministerie van Financiën	
V8.	Het uitvoeren van een risicoanalyse is altijd verplicht, ongeacht de soort gegevens die verwerkt worden[14].
V9.	Concreet betekent V3 dat de CC een exit-strategie voor zichzelf maakt en als onderdeel daarvan alleen de exit-afspraken in de overeenkomst met de CP laat opnemen.
V10.	De verwerving van clouddiensten vindt altijd plaats via de desbetreffende inkoop-organisatie voor het organisatieonderdeel. Hierdoor kan er centraal zicht gehouden worden op de afhankelijkheden van leveranciers en worden kwaliteitswaarborgen geleverd.
V11.	De ontsluiting van clouddiensten vindt altijd plaats via de interne ICT dienstverlener in de rol van Cloud Broker. Hierdoor wordt de benodigde schaarse kennis benut en worden noodzakelijke veilige koppelingen met de eigen infrastructuur ingericht.

[10] Zie hoofdstuk 6

[11] SLM richt zich op het vergroten van de bijdrage van leveranciers aan de strategische doelen van het Rijk en op optimale benutting van contracten waardoor rijksbrede voordelen kunnen worden behaald. Zie ook https://zoek.officielebekendmakingen.nl/kst-33326-13.html

[12] De minister van Financiën wordt hier bedoeld.

[13] Behoudens voor zover de artikelen 5.1, eerste, tweede en vijfde lid, en 5.2 van Wet open overheid aan openbaarmaking in de weg staan.

[14] Zie verantwoording paragraaf 10.5

Aanvullend beleid Ministerie van Financiën	
V12.	Communicatie vanuit de organisatieonderdelen met CISO Rijk vindt plaats in afstemming met of via de departementale CISO.
V13.	De ondernemingsraad wordt in staat gesteld zijn rechten uit te oefenen conform Artikel 24 (informatierecht), Artikel 25 (adviesrecht) en Artikel 27 (instemmingsrecht) van de Wet op de ondernemingsraden. Het gebruik van clouddiensten kan gekoppeld zijn aan de verwerking van medewerkergegevens in de cloud en gevolgen hebben voor het takenpakket van de interne ICT dienstverlener.

Aanvullend beleid alleen voor DG's Belastingen, Toeslagen en Douane	
V14.	De keuze voor de inzet van een clouddienst vindt plaats binnen het voortbrengingsproces door een domein volgens de kaders van de relevante concerndirecties.

4 RACI

Onderstaande RACI[15] tabel geeft een overzicht van rollen en verantwoordelijkheden die voortkomen uit de beleidsregels. De minister is primair accountable (eindverantwoordelijk) voor het voldoen aan het Rijksbreed Cloudbeleid en via het mandaatbesluit de DG en daaronder de directies. De RACI tabel heeft als vertrekpunt de directies en toont daarbinnen de nuances.

Activiteit	Paragraaf	CC	CB	CP	CA	Inkoop	CISO	CIO	CPO[16]	DG	MinFin	CISO Rijk
1. Opstellen Business Case	4.1	A	C			C						
2. Opstellen/onderhouden risicoanalyse	4.2	A	C	C		C	C			A[17]		I
3. Borgen privacybescherming	4.3	A	C	C		C	I		C		C (FG/dCPO)	I
4. Vaststellen van de explain voor de verwerking van bijzondere persoonsgegevens	4.4	R					C		C	A	I (FG/dCISO)	I
5. Vaststellen van de explain voor de verwerking (van een bron) van een basisregistratie	4.5	R					C	C			A (dCISO)	C
6. Toestemmen in het gebruik van community clouddiensten samen met organisaties die niet vallen onder het Rijksbreed Cloudbeleid en de BIO	4.6	R					R				A	
7. Opstellen exit-strategie	4.7	R	C	C		C		C		A	I (dCISO)	
8. Opstellen/onderhouden overeenkomst	4.8	A	C	C		R						
9. Periodiek uitvoeren audit	4.9	A	R	C	C	R[18]	I	I				
10. Beheren administratie	4.10	R	R			R		A				
11. Jaarlijks rapporteren aan CISO Rijk	4.11	C	C			C	R	I			A	I
12. Openbaar maken besluitvorming	4.12	A										

Tabel 1: RACI tabel

In onderstaande tabel staat aangegeven wie binnen het Ministerie van Financiën welke cloudrollen vervult.

Rol	Wie (Ministerie excl. DG's Belastingen, Toeslagen, Douane)	Wie (DG's Belastingen, Toeslagen, Douane)
Cloud Consumer (CC)	Directies	Ketens of directies die geen onderdeel van een keten zijn. Deze partijen worden door domeinen ondersteund bij de uitvoering van het cloudbeleid.
Cloud Broker (CB)	SG-Cluster/Directie Digitalisering en Informatisering/Dienstverlening	Directie IV
Cloud Auditor (CA)	SG-Cluster/Directie Digitalisering en Informatisering/Beleid	Directie IV
Inkoop	BZK/Rijks Inkoop Samenwerking	SSO CFD/Inkoopuitvoeringscentrum en Directie IV/CTO/Supplier Management

Tabel 2: Invulling rollen

In de hierna volgende paragrafen worden de activiteiten uit Tabel 1 nader beschreven voor de verschillende rollen. De omkaderde tekst komt uit het Rijksbreed Cloudbeleid. De overige tekst bevat nadere eisen of duiding van de omkaderde tekst en is deels een invulling van het IRC.

[15] Afkorting voor Responsible, Accountable, Consulted, Informed. Voor meer uitleg over het RACI model zie https://nl.wikipedia.org/wiki/RACI-model

[16] Chief Privacy Officer

[17] Normaliter is 1 partij eindverantwoordelijk (accountable). Hier gaat het om een specifieke taak binnen de activiteit.

[18] Dit is alleen van toepassing voor de DG's Belastingen, Toeslagen en Douane

4.1 Opstellen business case

CC	CB	CP	CA	Inkoop	CISO	CIO	CPO	DG	MinFin	CISO Rijk
A	C			C						

1. Bij verwerving of uitbesteding van ICT-diensten, direct of indirect, bij een commerciële partij, 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.
2. De business case, die onder verantwoordelijkheid van de CC[19] gemaakt wordt, bevat de onder 1 genoemde afweging. Binnen de DG's Belastingen, Toeslagen en Douane wordt de CC ondersteund door een domein. Het domein consulteert de directie IV in de rollen CB en exploitant van het Datacenter Belastingdienst. Door de overige organisatieonderdelen wordt de directie Digitalisering & Informatisering geconsulteerd.
3. De inkoop-organisatie wordt geconsulteerd voor o.a. de financiële paragraaf van de business case.
4. Onderbouw de noodzaak (subsidiariteit) van het cloudgebruik.

4.2 Opstellen/onderhouden risicoanalyse

CC	CB	CP	CA	Inkoop	CISO	CIO	CPO	DG	MinFin	CISO Rijk
A	C	C		C	C			A[17]		I

1. 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.
2. De CC (directie of keten), voor wiens business vraagstuk een clouddienst als oplossingsrichting wordt voorgesteld, voert altijd een risicoanalyse uit als verantwoordelijke voor bescherming van zijn bedrijfsmiddelen en personeel.
3. De implementatie en werking van beschermingsmaatregelen wordt gemonitord (zie ook paragraaf 4.8 en paragraaf 4.9).
4. De risicoanalyse wordt elke 3 jaar, of eerder als daartoe aanleiding is, geactualiseerd om te borgen dat genomen maatregelen en geaccepteerde restrisico's nog steeds juist zijn.
5. De geactualiseerde risicoanalyse wordt opnieuw gedeeld met de CISO Rijk, wanneer er eerder sprake was van het verplicht delen van de risicoanalyse (zie paragraaf 4.4 punt 2 en paragraaf 4.5 punt 1).
6. De risicoanalyse wordt gemaakt conform de door de desbetreffende CISO vastgestelde risicomanagementmethodiek.
7. De DG's Belastingen, Toeslagen en Douane maken de risicoanalyse in het IV Voortbrengingsproces.
8. Een risicoanalyse wordt altijd ter informatie naar de desbetreffende CISO gestuurd voordat een overeenkomst met de CP wordt gesloten of gebruik gemaakt wordt van een clouddienst die reeds ontsloten is voor het organisatieonderdeel.
9. Het dreigingsbeeld van het desbetreffende organisatieonderdeel wordt als vertrekpunt gehanteerd voor het bepalen van relevante dreigingsactoren en dreigingen die daarvan uit kunnen gaan.
10. In de risicoanalyse worden de C2000 criteria aantoonbaar in ogenschouw genomen. Zie Bijlage – C2000-criteria.

[19] Formeel is het nog geen Cloud Consumer, want in deze fase moet de keuze voor cloud nog gemaakt worden.

11. Ten minste de volgende dreigingsscenario's worden door de CC expliciet meegenomen in de risicoanalyse:
    a. De scenario's zoals vermeld in Bijlage – Risicoscenario's public cloud NBV.
    b. De data die nu wordt vercijferd, verstuurd of opgeslagen, kan worden onderschept en vanaf ongeveer 2030 met een quantumcomputer worden ontcijferd.
    c. Risico's voor veiligheid van personen[20] voor wie er extra risico's zijn indien persoonsgegevens gelekt worden.
    d. Continuïteitsrisico bij het langere tijd onbeschikbaar zijn van de clouddienst.
    e. CP medewerkers hebben toegang tot gegevens en systemen van de Belastingdienst.
12. Bij de CB wordt advies ingewonnen voor het in beeld krijgen van risico's en maatregelen die betrekking hebben op de CP (zie ook paragraaf 5.1).
13. Indien van toepassing wint de CC, via Inkoop, informatie in bij SLM Rijk m.b.t beveiligingsrisico's en maatregelen. SLM heeft vaak al gekeken naar beveiligingsrisico's en maatregelen afgesproken met de CP. Het is uiteindelijk aan de CC om te bepalen of dit afdoende is voor de context van het gebruik door de CC.
14. Beveiligingsmaatregelen te nemen door de CC zijn ten minste de relevante overheidsimplementatiemaatregelen uit de Baseline Informatiebeveiliging Overheid (BIO), 2019 en de relevante implementatierichtlijnen uit de ISO27002.
15. Beveiligingsmaatregelen te nemen door de CP zijn te minste de relevante implementatierichtlijnen uit de ISO27002, ISO27017 en ISO27018 of vergelijkbaar.
16. Beveiligingsmaatregelen te nemen door de CB zijn ten minste de relevante overheidsimplementatiemaatregelen uit de Baseline Informatiebeveiliging Overheid (BIO), 2019 en de relevante implementatierichtlijnen uit de ISO27002. Wanneer de CB een externe niet overheidspartij is, geldt alleen de ISO27002 of vergelijkbaar als eis.
17. Restrisico's op het niveau van het desbetreffende organisatieonderdeel moeten voor acceptatie aangeboden worden aan de DG (eindverantwoordelijk) met een advies van de desbetreffende CISO op advies van de desbetreffende CPO.
18. Mocht er een risico zijn op dreiging van statelijke actoren (o.a. criterium 1 en/of 3 uit de C2000 criteria), wordt tijdig dreigings- en beveiligingsadvies ingewonnen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en/of Militaire Inlichtingen- en Veiligheidsdienst (MIVD).
19. Wanneer sprake is van een risico van statelijke actoren wordt de desbetreffende CISO geconsulteerd. De CISO wint, indien noodzakelijk, dreigings-en beveiligingsadvies in bij de AIVD en/of MIVD. Dit in afstemming met de departementale CISO.

4.3 Borgen privacybescherming

CC	CB	CP	CA	Inkoop	CISO	CIO	CPO	DG	MinFin	CISO Rijk
A	C	C		C	I		C		C (FG/dCPO)	I

1. Met een pre-scan DPIA wordt door de CC vastgesteld of er sprake is van een hoog risico bij de verwerking van persoonsgegevens. Een formele DPIA moet gemaakt worden wanneer uit de pre-scan DPIA blijkt dat er sprake is van een hoog privacy risico. De (pre-scan) DPIA wordt gemaakt conform de voor het

[20] Bewindslieden, BN'ers, medewerkers van inlichtingendiensten, getuigen en advocaten in megaprocessen e.d.

organisatieonderdeel geldende procedure. Bijvoorbeeld: de GEB[21] procedure binnen het IV Voortbrengingsproces van DG Belastingen. Binnen die procedure staat ook de rol van de CPO en FG uitgewerkt. Onderdeel van de DPIA is de risicoanalyse die moet voldoen aan de eisen uit paragraaf 4.2.

2. Het Ministerie van Financiën hanteert het Model DPIA Rijksdienst en het rapportagemodel DPIA Rijksdienst.
3. Bij overdracht naar landen buiten de EER zonder een adequaatheidsbesluit, is een DTIA nodig conform aanbevelingen van de EDPB en bij bijzondere persoonsgegevens is extra terughoudendheid geboden conform cloudbeleid en eerder genoemde aanbevelingen van de EDPB. Zie ook Bijlage – Ontwikkelingen en consequenties Cloud Act e.a..
4. Indien van toepassing wint de CC, via Inkoop, informatie in bij SLM Rijk m.b.t. privacyrisico's en maatregelen. SLM heeft vaak al gekeken naar privacyrisico's en maatregelen afgesproken met de CP. Het is uiteindelijk aan de CC om te bepalen of dit afdoende is voor de context van het gebruik door de CP.
5. De privacyrisico's worden bepaald en voldoende gemitigeerd voor medewerkers die de clouddienst gebruiken. Denk hierbij aan telemetriegegevens en andere gebruikersinformatie.
6. Elke 3 jaar, of eerder als een situatie daarom vraagt, wordt een gemaakte DPIA geëvalueerd.
7. De geactualiseerde DPIA wordt opnieuw gedeeld met de CISO Rijk, wanneer er eerder sprake was van het verplicht delen van de DPIA (zie paragraaf 4.4 punt 2 en paragraaf 4.5 punt 1).
8. Advies wordt ingewonnen, door de CC bij de Privacy Adviseur Rijk via de departementale CPO en FG, wanneer er sprake is van privacygerelateerde vraagstukken bij clouddiensten die ministerie overstijgend worden aangeboden voor Rijksbrede Dienstverlening.

4.4 Vaststellen explain voor verwerking van bijzondere persoonsgegevens

CC	CB	CP	CA	Inkoop	CISO	CIO	CPO	DG	MinFin	CISO Rijk
R					C		C	A	I (FG/ dCISO)	I

1. Vaststelling van de explain[22] op de afwijking van beleidsregel R2 (zie paragraaf 3.2.1) moet aantoonbaar plaatsvinden door de DG met een appreciatie van de desbetreffende CISO en CPO. Dat wil zeggen dat de CISO een advies geeft waarin het advies van CPO is opgenomen. De FG wordt van het advies en de reactie van de DG op de hoogte gesteld.
2. Een DPIA en een explain moeten zo spoedig mogelijk na vaststelling gestuurd worden aan de CISO Rijk, wanneer Bijzondere Persoonsgegevens verwerkt worden bij een CP 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').
3. De (pre-scan of formele) DPIA en explain in het onder 2 benoemde scenario worden ter informatie door de desbetreffende CISO, via de departementale CISO, aangeboden aan de CISO Rijk.

[21] De termen GEB en DPIA betekent hetzelfde. Recent is besloten de term GEB te vervangen door de term DPIA, maar dat is nog niet in alle stukken doorgevoerd.
[22] Zie verantwoording paragraaf 10.3

4.5 Vaststellen explain voor verwerking (van een bron) van een basisregistratie

CC	CB	CP	CA	Inkoop	CISO	CIO	CPO	DG	MinFin	CISO Rijk
R					C	C			A (dCISO)	C

1. 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 de CISO Rijk toegezonden zodat zijn advies kan worden meegenomen in de besluitvorming.
2. Vaststelling van de explain[22] op de afwijking van beleidsregel R3 (zie paragraaf 3.2.1) moet aantoonbaar plaatsvinden. In geval van:
   a. een basisregistratie, is de acceptatie van de explain maatwerk. Hiervoor wordt de desbetreffende CISO geconsulteerd. Het Ministerie van Financiën is volgens het stelsel basisregistraties opdrachtgever en daarmee verantwoordelijk voor de Basisregistratie Inkomen (BRI).
   b. een bron van een basisregistratie, vindt de acceptatie van de explain plaats door de pSG in de rol van departementale CIO.
3. Als (bronnen van) basisregistraties al van clouddiensten van commerciële CP's gebruik maken, dan wordt dat zo snel mogelijk bij de CISO Rijk gemeld.

4.6 Toestemmen in het gebruik van community clouddiensten

CC	CB	CP	CA	Inkoop	CISO	CIO	CPO	DG	MinFin	CISO Rijk
R					R				A	

1. Gebruik van community clouddiensten samen met organisaties die niet vallen onder het Rijksbreed Cloudbeleid en de BIO is in principe mogelijk, mits vooraf aantoonbaar afstemming heeft plaatsgevonden met en aantoonbaar toestemming is verkregen van de desbetreffende CISO.
2. De organisatieonderdelen zijn en blijven verantwoordelijk voor de gegevens die zij beheren en zijn daarmee gehouden aan het Rijksbreed Cloudbeleid, ongeacht de samenwerkingspartner.
3. Of en onder welke condities het gebruik van een community clouddienst verantwoord is hangt sterk van de situatie af. Daarbij spelen o.a. de volgende zaken een rol:
   a. Het gehanteerde dreigingsbeeld;
   b. Welke classificatiemethoden de verschillende deelnemers hanteren en welke beveiligingseisen daar mogelijk aan vast zitten;
   c. De soort gegevens en processen die in de clouddienst verwerkt worden;
   d. De soort koppelingen met de on-premise omgeving;
   e. Of er een samenwerkingsverdrag aan ten grondslag ligt.
4. Inhoudelijk wordt met de desbetreffende CISO vastgesteld wat verantwoord is. Afhankelijk van de casus wordt samen met de desbetreffende CISO bepaald op welk niveau vervolgens toestemming gegeven moet worden. Hierbij wordt o.a. de verantwoordelijkheidsverdeling gehanteerd zoals beschreven in het CIO-stelsel, BVA-stelsel, de VIR-BI en de VIR.

4.7 Opstellen exit-strategie

CC	CB	CP	CA	Inkoop	CISO	CIO	CPO	DG	MinFin	CISO Rijk
R	C	C		C		C		A	I (dCISO)	

1. Een exit-strategie in het kader van het cloudbeleid borgt de continuïteit van bedrijfsprocessen en het opruimen van data bij beëindiging van de dienstverlening. De borging gaat zowel via maatregelen voor de eigen organisatie, waaronder budget, als via contractuele afspraken met de leverancier.
2. Onderdelen in de exit-strategie zijn:
   a. Voorwaarden aan de leverancier (en toeleveranciers) met aandacht voor dataportabiliteit, serviceportabiliteit en datavernietiging inclusief de processen en voorzieningen die daarvoor nodig zijn;
   b. Een alternatieve leverancier of interne landingsplaats;
   c. Een strategie, voorwaarden en budget, voor direct vertrek in verband met een crisis of plotselinge (geopolitieke) ontwikkelingen;
   d. Een strategie en budget bij de reguliere afloop van de overeenkomst.
3. De inkoop-organisatie wordt geconsulteerd bij het opstellen van de exit-strategie en het formuleren van exit-afspraken als onderdeel van het contract.
4. De exit-strategie wordt elke 3 jaar, of eerder als daartoe aanleiding is, geactualiseerd om te borgen dat de genomen strategie nog passend is.

4.8 Opstellen/onderhouden overeenkomst

CC	CB	CP	CA	Inkoop	CISO	CIO	CPO	DG	MinFin	CISO Rijk
A	C	C		R						

1. De inkoop-organisatie is verantwoordelijk voor het verwerven, opstellen en onderhouden van de overeenkomst tussen de CC en de CP. Hiervoor heeft Inkoop informatie nodig van de CC, CB en CP.
2. De overeenkomst dient te voldoen aan de eisen aan ICT dienstverlening (zie hoofdstuk 6).
3. Bij de selectie van de hoofdleverancier wordt rekening gehouden met de kaders voor publieke waarden zoals voor open source, mensenrechten en duurzaamheid.
4. In de overeenkomst dienen ten minste de volgende zaken opgenomen te zijn:
   a. De ‘exit-strategie’. Hierin staat hoe, bij beëindiging van de overeenkomst, data worden overgedragen en hoe wordt geregeld dat de verzameling data bij de leverancier vernietigd wordt. Zie paragraaf 4.7, punt 2a.
   b. Hoe geregeld is dat de CP controle en verantwoordings- onderzoeken toelaat of daarover rapporteert; er bestaat een 'right-to- audit' voor de CC of er is hierover contractueel voldoende zekerheid via Strategisch Leveranciers Management (SLM).
5. Aanvullend verwacht het Ministerie van Financiën het volgende ook in de overeenkomst:
   a. De security controls waaraan de CP moet voldoen. De security controls komen uit de eisen aan ICT dienstverlening en als resultaat van een risicoanalyse (zie paragraaf 4.2).
   b. De SLA die is overeengekomen met de CP.
   c. De wijze waarop de CP zijn leveranciers beoordeeld, onder meer voor ketenrisico’s.

4.9 Periodiek uitvoeren audit

CC	CB	CP	CA	Inkoop	CISO	CIO	CPO	DG	MinFin	CISO Rijk
A	R	C	R	R	I	I				

1. De CC is verantwoordelijk (zie paragraaf 3.1, uitgangspunt 3) voor de bescherming van gegevens en processen die verwerkt worden met clouddiensten. Dit betekent dat periodiek audits uitgevoerd moeten worden bij de CP op de security controls die vastgelegd zijn in de overeenkomst (zie paragraaf 4.8). De inkoop-organisatie initieert en coördineert op basis van de contractafspraken het uitvoeren en afhandelen van de audits namens de CC. Hierbij wordt een CA ingezet.
2. Voor het beleidsdepartement geldt dat de CC zelf, op basis van de contractafspraken, het uitvoeren en afhandelen van de audit initieert en coördineert.
3. De CB laat audits uitvoeren op die zaken bij de CP die relevant zijn voor de kwaliteit van dienstverlening door de CB.
4. Wanneer de CB rol wordt ingevuld door een organisatieonderdeel binnen het Ministerie van Financiën, dan vinden audits op die CB plaats via de reguliere governance en compliance processen.
5. De audit resultaten vormen input voor de risico- en contractevaluatie.

4.10 Beheren administratie

CC	CB	CP	CA	Inkoop	CISO	CIO	CPO	DG	MinFin	CISO Rijk
R	R			R		A				

1. 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.
2. Informatie moet niet alleen voor bovengenoemde rapportageverplichting bewaard worden, maar wordt ook vereist vanuit privacy- en informatiebeveiligingsbeleid, beheer en contractmanagement. Daarom dient voor alle vormen (niet alleen materieel) van cloudgebruik administratie te worden gevoerd. Zie ook paragraaf 10.1.
3. De CC administreert:
   a. Het bedrijfsproces waarbinnen de clouddienst wordt gebruikt
   b. De verantwoordelijke voor het bedrijfsproces
   c. Welke soorten gegevens met welke labeling en BIV classificatie verwerkt worden met de clouddienst.
   d. De interfaces van de clouddienst met andere processen of applicaties in geval van SaaS clouddiensten.
   e. Voor de DG's Belastingen, Douane en Toeslagen geldt: 3a t/m 3d worden vastgelegd door het CC ondersteunende domein in de architectuurrepository conform archimate en de IPK voorschriften die daarvoor gelden.
   f. Een door de CC (directeur dienstonderdeel of ketenvoorzitter) geaccordeerde risicoanalyse incl. acceptatie van de restrisico's (zie paragraaf 4.2).
   g. Een door de verwerkingsverantwoordelijke (directeur dienstonderdeel of ketenvoorzitter) vastgestelde (pre-scan en/of formele) DPIA in geval van verwerking van persoonsgegevens (zie paragraaf 4.3).
   h. De explains voortkomend uit de restricties R2 en R3 (zie paragraaf 0).
   i. Alle adviezen en akkoorden die verkregen moeten worden voor het gebruik van een clouddienst.

   j. De CA auditrapporten (zie paragraaf 4.9).
4. De CB administreert:
   a. De naam en omschrijving van de clouddienst
   b. Welk dienstonderdeel gebruik maakt van de clouddienst
   c. Voor de DG's Belastingen, Douane en Toeslagen geldt: 4a en 4b worden vastgelegd door het CB ondersteunende domein in de architectuurrepository conform archimate en de IPK voorschriften die daarvoor gelden.
   d. Het cloud implementatiemodel (publieke/private/hybride/community cloud).
   e. Het soort clouddienst (SaaS, PaaS, IaaS).
   f. De interfaces van de clouddienst:
      i. met de on-premise omgeving;
      ii. met andere clouddiensten afgenomen door het Ministerie van Financiën;
      iii. andere samenwerkingspartijen;
      iv. met de devices van de medewerkers.
   g. De (hoofd-) Cloud Provider en eventuele onder-dienstverleners.
   h. De geografische regio van verwerking en opslag van gegevens met de clouddienst.
   i. De CA auditrapporten (zie paragraaf 4.9).
   j. De SLA rapportages.
5. Inkoop administreert de overeenkomst met de CP.

4.11 Jaarlijks rapporteren aan CISO Rijk

CC	CB	CP	CA	Inkoop	CISO	CIO	CPO	DG	MinFin	CISO Rijk
C	C			C	R	I			A	I

1. Vanuit de verplichting tot het bijhouden van materieel cloudgebruik en de risico's daarvan rapporteren departementen jaarlijks over de verwerking van persoonsgegevens in clouddiensten die, direct of indirect, aangeboden worden door commerciële CP's. Dit gebeurt als onderdeel van het rapportageproces voor het IB-beeld, conform de departementale taken en volgens het besluit CIO-stelsel.
2. In paragraaf 4.10 zijn administratieve verplichtingen beschreven waar de CC, de CB en Inkoop aan moeten voldoen. Hiermee is het onder andere mogelijk jaarlijks de gevraagde rapportages aan de CISO Rijk te leveren. De departementale CISO krijgt hiervoor de benodigde informatie van de CISO's van de organisatieonderdelen.

4.12 Openbaar maken besluitvorming

CC	CB	CP	CA	Inkoop	CISO	CIO	CPO	DG	MinFin	CISO Rijk
A										

1. Besluitvorming over het gebruik van een clouddienst, waaronder de *besluitvorming* over de DPIA's en adviezen van de Privacy Adviseur Rijk, moet in het kader van de Weten open overheid (Woo) openbaar gemaakt worden. Er wordt hier nadrukkelijk gesproken over de besluitvorming. Een DPIA bevat ook een risicoanalyse met informatie over kwetsbaarheden en maatregelen. Deze zijn niet geschikt voor openbaarmaking.
2. Openbaarmaking gebeurt uiterlijk 3 maanden na ingebruikname.

5 Cloud Broker & Cloud Auditor

Het Rijksbreed Cloudbeleid onderkent 2 rollen in de context van cloud, namelijk CC en CP. In voorliggend CB-MinFin zijn er 3 rollen toegevoegd (zie paragraaf 2.4), waarvan de Cloud Broker (CB) en de Cloud Auditor (CA) de belangrijkste zijn.

In hoofdstuk 4 zijn deze rollen al een paar keer benoemd. Deze rollen en daarbij horende verantwoordelijkheden zijn belangrijk en nieuw voor het Ministerie van Financiën. Daarom wordt in dit hoofdstuk dieper ingegaan op de rollen CB en CA.

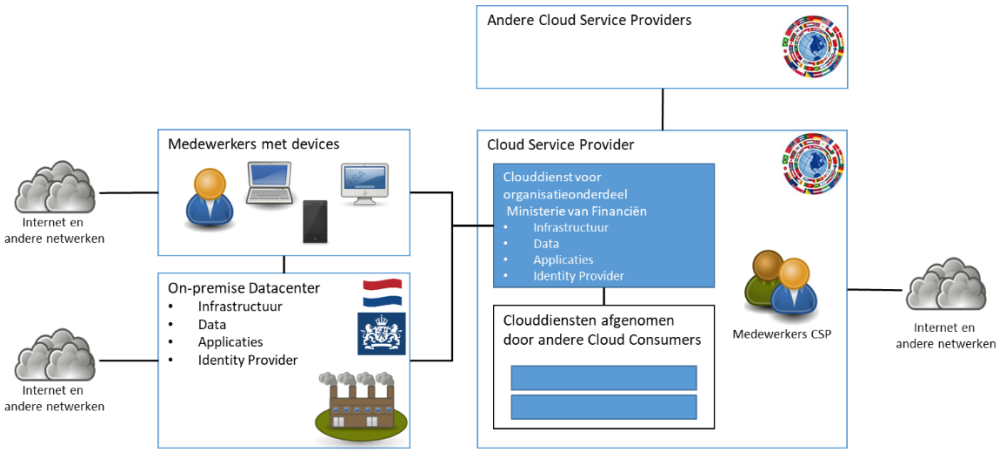
5.1 Cloud Broker

De CB is in hoofdlijnen verantwoordelijk voor:

- Het beschikbaar stellen/ontsluiten van clouddiensten. Het betreft hier clouddiensten die zijn aangeschaft of waar op basis van afspraken van gebruik gemaakt wordt. In dat laatste geval dient de CB aan de CC inzichtelijk te maken waar de clouddienst geschikt voor is in termen van beveiliging.
- Het bewaken dat gemaakte SLA afspraken nagekomen worden door de CP.

Het gebruik van clouddiensten vergroot het aanvalsoppervlak voor kwaadwillenden (zie Figuur 4). De risico's die daaruit voortkomen moeten binnen acceptabele grenzen beheerst worden. Daarom worden de volgende eisen aan de CB gesteld:

- Borgen dat geavanceerde aanvallen op de clouddiensten van de organisatieonderdelen van het Ministerie van Financiën niet kunnen leiden tot ongeautoriseerde toegang op de on-premise omgeving of andere clouddiensten van de organisatieonderdelen of devices van medewerkers.
- Borgen dat geavanceerde aanvallen op de on-premise omgeving of devices van medewerkers niet kunnen leiden tot ongeautoriseerde toegang tot de clouddiensten afgenomen door de organisatieonderdelen.
- Afspraken maken met de CP over detectie, communicatie en mitigatie van geavanceerde aanvallen op de cloud infrastructuur van de CP.
- Borgen dat de basisinrichting/-configuratie van de clouddienst veilig is door o.a. *hardening* en SOC monitoring.
- Borgen dat identiteiten- en autorisatiebeheer beheerst en veilig is ingericht over de on-premise en clouddiensten heen
- Bepalen van aansluitvoorwaarden voor veilige data interfaces die domeinen dienen te hanteren. Hierbij rekening houdend met verplichte standaarden die van binnen en van buiten het Ministerie van Financiën opgelegd kunnen zijn.
- Afspraken maken met de CP over handelingswijze bij calamiteiten en onbeschikbaarheid van de clouddiensten.



Figuur 4: Schets aanvalsoppervlak cloud

5.1.1 *Interne ICT dienstverlener in de rol van CB*

Organisatieonderdelen nemen hun ICT-diensten af van of via een interne dienstverlener. In geval van de DG's Belastingen, Douane en Toeslagen is dat de directie IV. Voor de andere organisatieonderdelen van het Ministerie van Financiën is dat SSC-ICT of SG-Cluster/Directie Digitalisering en Informatisering/IT specials. Clouddiensten worden ook altijd via de interne ICT dienstverlener, in de rol van Cloud Broker, verworven en ontsloten. Hiermee heeft de CC één aanspreekpunt en wordt ontzorgd m.b.t. veilige integratie met de on-premise omgeving en suppliermanagement.

Figuur 5: Directie IV in de rol van CB

5.2 Cloud Auditor

De CC is integraal verantwoordelijk voor de bescherming van zijn processen en gegevens. Door middel van audits bij de CP's kan de CC inzicht krijgen in hoeverre de bescherming daar op orde is. Dit is gespecialiseerd werk wat door een CA wordt uitgevoerd/gecoördineerd. De CA heeft voor de audits informatie nodig van de CC, CB en de CP's.

5.2.1 *Interne ICT dienstverlener in de rol van CA*

De security audit functie bij uitbesteding is anno 2022 nog nauwelijks ingericht binnen de Belastingdienst. De interne ICT dienstverlener is bij uitstek geschikt om de rol van de CA te vervullen namens de CC en als CB. De interne ICT dienstverlener heeft zelf ervaring met het moeten voldoen aan security controls als dienstverlener. De interne ICT dienstverlener kan binnen de CA verantwoordelijkheid bekijken welke kennis zij zelf in huis wil hebben en wanneer ze bepaalde audit taken uitbesteedt.

De security audit op de interne ICT dienstverlener in de rol van CB vindt plaats via de reguliere BIO compliance processen van het Ministerie van Financiën.

6 Bijlage – Eisen aan ICT dienstverlening

Algemeen
- Rijksbreed Cloudbeleid 2022, d.d. 19 augustus 2022
- Implementatiekader Risicoafweging Cloudgebruik, d.d. 5 januari 2023
- Privacybeleid Ministerie van Financiën
- Informatiebeveiligingsbeleid Financiën, 2021
- Integrale Beveiligingsbeleid Belastingdienst (IBB), 2019

Informatiebeveiliging
- Besluit CIO-stelsel Rijksdienst, 2021
- Besluit voorschrift informatiebeveiliging rijksdienst (VIR), 2007
- Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIR-BI), 2013
- Baseline Informatiebeveiliging Overheid (BIO), 2019
- Overeenkomst tussen de lidstaten van de Europese Unie betreffende de bescherming van in het belang van de Europese Unie uitgewisselde gerubriceerde informatie, 2011/C 202/05
- Beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie, 2013/488/EU
- Kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie, 2018/1807/EU
- Network and Information Systems 2 (NIS 2) Directive, 2022/2555/EU
- Wet beveiliging netwerk- en informatiesystemen

Privacybescherming
- Algemene Verordening Gegevensbescherming (AVG), 2016
- Adequaatheidsbesluiten EU
- Deelnemers Data Privacy Framework EU-V.S.

Archivering
- De regels voor archieven overheid

Open overheid
- Wet open overheid (Woo), 2022

Strafrechtketen
- Wet Politiegegevens (WPG), 2020
- Wet Justitiële en Strafvorderlijke Gegevens (WJSG), 2022

Inkoop
- Besluit vaststelling Algemene Rijksvoorwaarden voor inkoop (ARBIT-2018, ARIV-2018 en ARVODI-2018)
- Besluit vaststelling Algemene Rijksvoorwaarden bij IT-overeenkomsten 2022 (ARBIT-2022).
- Quickscan/risicomitigatie nationale veiligheid bij inkoop en aanbesteden
- In juli 2022 is de Digital Markets Act vastgesteld en zal van kracht zijn vanaf medio 2023. Deze wet stelt eisen aan o.a. grote Cloud Brokers en vormt een reactie van de EU op de behoefte om de digitale ruimte te reguleren.

Generieke IV dienstverlening binnen het Rijk
- Hoofdlijn sourcingsafwegingskader binnen het Rijk, 2012

- Sourcingsafwegingskader binnen het Rijk, 2012

C2000

- Overwegingen bij risicobeoordeling aanschaf C2000 producten
- Beleidsregels Informatiebeveiligingsbeleid C2000

7 Bijlage – C2000-criteria

Bij cloudgebruik hanteren we de C2000-criteria om risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere derde partijen te beoordelen.[23] De C2000-criteria zijn als volgt:

1. Is de partij die de dienst of product levert afkomstig, of staat hij onder controle van een partij, uit een land met wetgeving die commerciële of particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder met staatsorganen die zijn belast met een inlichtingen- of militaire taak, of is de partij een staatsbedrijf?

2. Is de partij die de dienst of product levert afkomstig uit een land met een actief offensief inlichtingenprogramma[24] gericht op Nederland en Nederlandse belangen of een land waarmee de Nederlandse relatie dusdanig gespannen is dat acties die Nederlandse belangen aantasten voorstelbaar zijn?

3.

   A. Krijgt de partij die de dienst of product levert uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen en vitale infrastructurele installaties of werken, waarbij misbruik een nationaal veiligheidsrisico kan vormen?

   B. Zijn er beheersmaatregelen mogelijk en realiseerbaar die de nationale veiligheidsrisico's die in het geding zijn voldoende beschermen?

[23] Kamerstukken II 2018/19, 25 124, nr. 96
[24] Algemene Inlichtingen- en Veiligheidsdienst, (2019), Offensief cyberprogramma een ideaal businessmodel voor Staten

8 Bijlage – Risicoscenario's public cloud NBV

Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) adviseert om in risicoanalyses voor public clouddiensten plannen te maken voor schadebeperking en disaster-recovery voor minimaal de onderstaande scenario's:

- Een (statelijke) actor heeft de overheidstenant[25] gecompromitteerd en had gedurende langere tijd toegang tot de data.
- Een (statelijke) actor heeft de cloud fabric[26] van de clouddienstverlener gecompromitteerd en had gedurende langere tijd toegang tot de overheidstenant en de data.
- Het land van de clouddienstverlener heeft, via extraterritoriale juridische mogelijkheden, toegang gekregen tot de overheidstenant en de aanwezige data.
- Het land van de clouddienstverlener, of een ander land, heeft politiek commerciële druk uitgeoefend op de clouddienstverlener waardoor verdenking ontstaat van spionage of sabotage.
- De clouddienst valt langdurig uit door storing of sabotage. Specifieke landen saboteren of blokkeren de clouddienst op hun gebied, wat buitenlandse vestigingen van de overheid raakt.
- De clouddienstverlener stopt met het tenant contract of met de hele clouddienst, al dan niet onder druk van het land van de clouddienstverlener of een ander land.

Als onderdeel van de risicobeoordeling dient rekening gehouden te worden met de koppeling tussen de on-premise omgeving en de public clouddienst(en), de hiermee gepaard gaande complexiteit en de vergroting van het aanvalsoppervlak van de gekoppelde omgevingen.

Als onderdeel van de risicobeoordeling dient ook rekening gehouden te worden met het feit dat (statelijke) actoren belangstelling hebben voor persoonsgegevens, waaronder ook grote databestanden en basisregistraties.[27]

[25] De term tenant moet hier gelezen worden als een clouddienst of een container van clouddiensten geleverd door 1 cloudprovider.

[26] De term fabric moet hier gelezen worden als datacenter(s) van een cloudprovider.

[27] Kamerbrief II 2020/21, 30 821, nr. 116

9 Bijlage – Ontwikkelingen en consequenties Cloud Act e.a.

De grootste clouddienstenleveranciers zijn anno 2023 Amerikaanse bedrijven. Bij het afnemen van clouddiensten van die partijen spelen vragen gerelateerd aan de Cloud Act (Public Law 115-141, Div. V, 132 Stat. 1213-25), de FISA Act Section 702, de USA Freedom Act en het Schrems II arrest[28] van het Hof van Justitie van de Europese Unie. In dit hoofdstuk wordt kort ingegaan op de ontwikkelingen en consequenties rondom dit vraagstuk.

Op 25 maart 2022 hebben de Verenigde Staten en de Europese Commissie een principe akkoord gesloten over een nieuw "Trans Atlantic Data Privacy Framework (TA DPF)". Het TA DPF komt tegemoet aan de zorgen die het Hof van Justitie van de Europese Unie heeft geuit in het Schrems II arrest van 16 juli 2020 m.b.t het PrivacyShield uitvoeringsbesluit.

Op 7 oktober 2022 heeft President Biden een Executive Order ondertekend voor het implementeren van het "Trans Atlantic Data Privacy Framework", ook bekend onder de naam "European Union-U.S. Data Privacy Framework (EU-U.S. DPF)". De Procureur-generaal van de V.S. Merrick Garland heeft een verordening ondertekend die invulling geeft aan het Data Privacy Framework.

Op 13 december 2022 is een concept adequaatheidsbesluit aan de European Data Protection Board (EDPB) aangeboden voor advies. Het goedkeuringsproces omvat verder een akkoord van een commissie bestaande uit vertegenwoordigers van EU-lidstaten benodigd en heeft het Europees Parlement het recht van toetsing van adequaatheidsbesluiten.

Op 28 februari 2023 heeft de EDPB een oordeel gegeven over de adequaatheid van het beschermingsniveau wat het concept adequaatheidsbesluit moet bieden. Het EDPB schrijft dat het TA DPF, hoewel het een stap in de goede richting is, nog wel verbetering behoeft. Experts delen in het Financieel Dagblad[29] hun zorgen van de EDPB. Het is een reëel risico dat de rechter ook dit systeem zal afschieten.

Op 10 juli 2023 heeft de Europese Commissie het adequaatsheidsbesluit over het European Union-U.S. Data Privacy Framework (EU-U.S. DPF) aangenomen. De EDPB heeft op 19 juli 2023 informatie gepubliceerd over de implicaties. Er hoeven geen aanvullende afspraken gemaakt te worden met bedrijven die genoemd staan in de Data Privacy Framework lijst.

De grote vraag voor de komende periode is of het EU-U.S. DPF stand houdt. De heer Schrems is een nieuwe juridische zaak aan het voorbereiden[30]. Critici[31] wijzen er op dat als een nieuwe rechtszaak wederom gewonnen wordt door de heer Schrems, bedrijven weer extra inspanning moeten leveren om hun data weg te halen bij

[28] Samenvatting: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf
https://www.autoriteitpersoonsgegevens.nl/actueel/advies-edpb-over-nieuw-eu-us-data-privacy-framework

[29] https://fd.nl/tech-en-innovatie/1470086/nieuw-verdrag-dataverkeer-eu-en-vs-biedt-onvoldoende-bescherming-kpc3calL7LLt

[30] https://fd.nl/bedrijfsleven/1481993/deal-met-vs-over-eu-data-lijkt-rond-maar-wordt-aangevochten

[31] https://fd.nl/opinie/1482152/privacy-shield-is-een-slechte-deal

Amerikaanse bedrijven of dat er gekeken moet worden naar standaard contractbepalingen. Verder is de zorg dat de Europese initiatieven (o.a. Gaia-X) rondom datasoevereiniteit weinig succesvol zullen worden, omdat er geen juridische bezwaren meer zijn voor goedkope opslag in de V.S.. Het risico op vendor lock-in wordt groter.

Voor het afnemen van clouddiensten van bedrijven die niet op Data Privacy Framework lijst voorkomen geldt nog de optie om gebruik te maken van modelcontracten (standaard contractbepalingen of 'standard contractual clauses'). In sommige gevallen is daarbij toestemming nodig van de autoriteit persoonsgegevens.

Op 4 juni 2021 heeft de Europese Commissie vernieuwde modelcontractbepalingen aangenomen om het gebruik ervan te vergemakkelijken, onder meer in het licht van de eisen die het Hof van Justitie in het Schrems II-arrest heeft gesteld[32].

Volgend uit het Schrems II-arrest is een modelcontract voor doorgifte naar de V.S. nog niet voldoende[33]. Er moeten aanvullende waarborgen getroffen worden, waarbij de EDPB aanbevelingen heeft gepubliceerd. Het bepalen van deze aanvullende waarborgen moet middels een Data Transfer Impact Assesment (DTIA) per doorgifte.

Europese bedrijven met dataverwerkingen in Europa vallen soms onder de werking van de Amerikaanse CLOUD-Act. Hierdoor kan in Europa opgeslagen data toegankelijk zijn voor de Amerikaanse overheid. Andere landen kennen ook dergelijke extraterritoriale wetgeving. Het NCSC heeft hierover een artikel gepubliceerd.

Wanneer de organisatieonderdelen van het Ministerie van Financiën gebruik maakt van contracten die afgesloten zijn via SLM Rijk, is het advies om te vragen of SLM Rijk of de Privacy Adviseur Rijk (PAR) een paraplu DPIA en/of DTIA heeft gemaakt. Deze kunnen dan als basis gehanteerd worden voor eigen DPIA en/of DTIA.

Bovenstaande zaken hebben allemaal betrekking op privacybescherming. Het risico van spionage m.b.t. niet-persoonsgegevens moet minstens zo goed beschouwd worden middels goede risicoanalyses. Ter ondersteuning hiervan heeft de AIVD de handleiding Kwetsbaarheidsonderzoek spionage gepubliceerd.

---

[32] https://ec.europa.eu/commission/presscorner/detail/nl/qanda_22_6045

[33] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal/doorgifte-binnen-en-buiten-de-eu#wanneer-mag-ik-persoonsgegevens-doorgeven-naar-de-vs-5539

10 Bijlage – Verantwoording

10.1 Scope

Het Rijksbreed Cloudbeleid beperkt zich tot materieel cloudgebruik. Het CB-MinFin richt zich op al het cloudgebruik. Veel van de beleidsregels hebben betrekking op het voldoen aan de AVG en de BIO met de daaraan gekoppelde verplichtingen. Daarbij is het niet relevant of er sprake is van een "wezenlijk belang".

10.2 Implementatiemodellen

Het Rijksbreed Cloudbeleid suggereert naar de letter dat het alleen betrekking heeft op *public cloud* diensten. De beleidsregels hebben naar de geest betrekking op het afnemen van diensten van commerciële CP's. Die partijen kunnen ook private, hybrid of community clouddiensten aanbieden. Aanpassing van het Rijksbreed Cloudbeleid op dit punt was niet meer mogelijk, omdat het al aangeboden was aan de 2e kamer. Bij de jaarlijkse evaluatie van het Rijksbreed Cloudbeleid gaat waarschijnlijk een aanpassing komen op het toepassingsgebied.

Het Cloudbeleid – Ministerie van Financiën loopt hier al op vooruit en spreekt daarom niet expliciet van *public cloud* diensten, maar van clouddiensten die afgenomen worden van commerciële CP's.

10.3 Comply or explain

Bij de comply or explain staat in het Rijksbreed Cloudbeleid niet vermeld wie de explain moet accepteren. Het CB-MinFin beschrijft hiervoor de procedures.

10.4 Rollen

In het Rijksbreed Cloudbeleid ontbreekt op een aantal plekken de aanwijzing welke rol welke verantwoordelijkheid heeft. Het CB-MinFin heeft die aangevuld.

Het NIST heeft verschillen cloudrollen beschreven die helpen bij het creëren van duidelijkheid rondom taken en verantwoordelijkheden. De NIST cloudrollen zijn verwerkt in het CB-MinFin.

Het Ministerie van Financiën heeft met de organisatieonderdelen afspraken gemaakt over wie communiceert met de departementale CIO, departementale CISO, CIO Rijk, CISO Rijk, AIVD/MIVD. Die afspraken zijn verwerkt in de tekst.

10.5 Risicomanagement

Het Rijksbreed Cloudbeleid schrijft een risicoanalyse voor wanneer er sprake is van de verwerking van persoonsgegevens. Verder worden nog aandachtspunten benoemd m.b.t. marktconcentratie, politieke en geografische spreiding van gegevensverwerkingen en dreiging van statelijke actoren.

Het Ministerie van Financiën wil dat, ongeacht de soort gegevens, altijd risicobeoordeling en -behandeling plaatsvindt. De aandachtspunten uit het Rijksbreed Cloudbeleid zijn ook van toepassing op "niet-persoonsgegevens". Verder vergroot het gebruik van clouddiensten het aanvalsoppervlak voor kwaadwillenden waar we nog weinig ervaring mee hebben.

10.6 Bronverwijzing

In het Rijksbreed Cloudbeleid wordt soms tekstueel verwezen naar wet- en regelgeving, afspraken, ontwikkelingen, etc. zonder specifieke bronverwijzing. Die zijn zoveel mogelijk toegevoegd in het CB-MinFin.

11 Beleid in een notendop

Cloudbeleid – Ministerie van Financiën

Gesloten norm

- Gegevens met een Rubricering StgC en hoger mogen niet in de cloud verwerkt worden.
- Er worden nooit clouddiensten, direct of indirect, afgenomen van CP's uit landen met een offensief cyberprogramma tegen de 6 Nationale Veiligheidsbelangen.

Open norm (comply or explain)

Hier gelden de algemene beginselen van behoorlijk bestuur (m.n. motiveringsbeginsel en zorgvuldigheidsbeginsel)

- Bijzondere persoonsgegevens mogen niet in de cloud verwerkt worden.
- Basisregistraties of bronnen van basisregistraties mogen niet in de cloud verwerkt worden. Bij een onderbouwde afwijking (explain) van deze regel is alleen het gebruik van private clouddiensten toegestaan.

Verplichtingen

- Onderbouwing noodzaak (subsidiariteit) van het cloudgebruik
- Rapportageplicht jaarlijks naar de CISO Rijk.
- Melding verwerking persoonsgegevens aan de CISO Rijk binnen 3 maanden na ingebruikname.
- Openbaarheid (woo) van besluitvorming binnen 3 maanden na ingebruikname.
- Vooraf inwinnen advies bij de CISO Rijk bij basisregistraties in de cloud.
- Vooraf inwinnen advies AIVD/MIVD wanneer sprake is van risico's voorkomend uit toetsing tegen de C2000 criteria.
- Update cloudtoets ten minste elke 3 jaar of vaker als daartoe aanleiding is.
- Voldoen aan de AVG en andere relevante wet- en regelgeving, zoals:
  - Controleren of DPIA benodigd is en deze eventueel maken incl. acceptatie verwerkingsverantwoordelijkheid;
  - Risico analyse incl. acceptatie restrisico;
  - Exit strategie;
  - Afspraken maken rondom right to audit;
  - Update DPIA of risicoanalyse ten minste elke 3 jaar;
  - Tijdig betrekken ondernemingsraad.
- Beheren administraties:
  - Cloudgebruik
  - Risicoregister
  - Verwerkingenregister