Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Implementatiekader risicoafweging cloudgebruik

Versie 1.1

Datum 5 januari 2023
Status Definitief

Colofon

Naam	Implementatiekader risicoafweging cloudgebruik
Type	Beleid en verplicht
Status	Concept
Versie	1.1
Vastgesteld door	ICBR
Datum vaststelling	20 december 2022
Beheer	CIO Rijk
Contact	CISORijk@minbzk.nl

Versiebeheer

Versie	Datum	Wie	Wijziging	Status
0.1	13-09-2022	CIO Rijk	Eerste opzet voor interne afstemming	Concept
0.2	21-9-2022	CIO Rijk	Concept voor kick-off en Stuurgroep Digitale Weerbaarheid	Concept
0.3	28-9-2022	CIO Rijk	Aanpassingen naar aanleiding van opmerkingen uit Kick-off	Concept
0.4	5-10-2022	CIO Rijk	Aanpassingen naar aanleiding van opmerkingen uit Werkgroep 3-10	Concept
0.5	11-10-2002	CIO Rijk	Aanpassingen n.a.v. input vanuit werkgroep en klankbordgroep	Concept
0.6	17-10-2022	CIO Rijk	Aanpassingen naar aanleiding van opmerkingen uit Werkgroep 17-10 en individuele telefonische gesprekken	Concept
0.7	27-10-2022	CIO Rijk	Aanpassingen naar aanleiding van input vanuit werkgroep en klankbordgroep en DT CIO Rijk	Concept
0.8	11-11-2022	CIO Rijk	Aanpassingen naar aanleiding van input vanuit werkgroep, klankbordgroep, CISO-raad, PAR, SIB, AP en CIO-beraad	Concept
0.9	30-11-2022	CIO Rijk	Aanpassingen naar aanleiding van input vanuit werkgroep, klankbordgroep en individuele gesprekken en e-mailberichten	Concept
0.95	12-12-2022	CIO Rijk	Aanpassingen naar aanleiding van verdiepingssessie met de Staatssecretaris en externe stakeholders en besluitvorming CIO-beraad	Concept
1.0	20-12-2022	CIO Rijk	Aanpassingen naar aanleiding van besluitvorming in ICBR	Definitief
1.1	05-01-2023	CIO Rijk	Inleiding aangepast n.a.v. overleg met de Staatssecretaris.	Definitief

Inhoud

1 Inleiding

In augustus 2022 is het 'Rijksbreed cloudbeleid 2022', hierna cloudbeleid, door de Ministerraad vastgesteld en aangeboden aan de Tweede Kamer.

Het gebruik van clouddiensten kan interessante voordelen opleveren rondom innovatie, flexibiliteit, schaalbaarheid, samenwerking, privacy en informatiebeveiliging. Ook zijn er risico's aan verbonden zoals beperking van de digitale autonomie, vendor-lock-in en privacycompromissen. Het cloudbeleid staat gebruik van public cloud toe maar onder een aantal voorwaarden om die risico's te beheersen. Goed risicomanagement is dus cruciaal. Vanwege de voordelen en risico's die het gebruik van de public cloud biedt is het van groot belang dat de overwegingen van de risicoanalyse(s), de exit-strategie en op het gebied van mensenrechten in acht genomen worden bij het maken van de keuze om gebruik te gaan maken van de public cloud. Het cloudbeleid stelt ook dat CIO Rijk met de departementale CIO's een 'implementatierichtlijn risicoafweging cloudgebruik', dit document, opstelt. Vanwege het verplichtende karakter is gekozen voor de term 'kader'.
De totstandkoming van het implementatiekader is onderdeel van de Routekaart Digitale Weerbaarheid en van de Werkagenda Waardengedreven Digitaliseren van het Rijk van de staatssecretaris Koninkrijksrelaties en Digitalisering.

Bij de uitvoering van het cloudbeleid is het toepassen van dit implementatiekader verplicht. Het implementatiekader geeft invulling aan een aantal aspecten die in het cloudbeleid globaal waren ingevuld. De inhoud is een verdieping en uitwerking van het cloudbeleid.
De focus conform het cloudbeleid ligt op informatiebeveiliging en de Algemene Verordening Gegevensbescherming (AVG). Dit cloudbeleid is ook van toepassing op gegevens die vallen onder alle andere relevante wet- en regelgeving zoals de Wjsg, Wpg, Vreemdelingenwet, Woo, NIS2, Archiefwet en ook specifieke uitvoeringswetgeving. Ook moet rekening worden gehouden met inkoopkaders zoals de 'Quickscan en Risicoanalyse Nationale veiligheid', en informatiehuishouding in het algemeen zodat informatie volledig, actueel en vindbaar is, en met bescherming van grond- en mensenrechten. Voldoen aan wet- en regelgeving is een minimum. Nederland wil digitaal koploper zijn: regel het cloudgebruik dus goed en zet in op kwaliteit.

Naast het cloudbeleid en het implementatiekader is er de (facultatieve) 'Handreiking risicobeheersing toepassing public cloud'. Deze geeft praktische handvatten voor het stapsgewijs beheersen van risico's. Deze wordt in het CIO-beraad vastgesteld en periodiek geactualiseerd.

1.1 Actualisatie implementatiekader

Voortdurend komen er nieuwe kaders en wetgeving. Ook wordt het cloudbeleid geëvalueerd en indien nodig aangepast en in samenhang daarmee dus ook dit implementatiekader. Er zijn twee type wijzigingen op dit document:

- Wijzigingen waarbij de inhoud van de artikelen wordt aangepast. In die gevallen wordt het reguliere afstemmingsproces gevolgd via voorportalen, het CIO-beraad en de ICBR.
- Kleine wijzigingen waarbij een toelichting, een link of een voorbeeld wordt aangepast. Deze wordt vastgesteld door CIO Rijk en gaat ter informatie naar het CIO-beraad.

2 Implementatiekader risicoafweging Cloudgebruik

Artikel 1 – Algemeen

a. Dit implementatiekader is van toepassing op al het materieel public[1] cloudgebruik door de Rijksdienst[2]. Deze kan in voorkomend geval ook van toepassing zijn op hybride clouddiensten. Dit implementatiekader is niet verplicht voor het gebruik van private clouddiensten. Bij de inzet van private clouddiensten wordt geadviseerd de onderdelen uit dit implementatiekader mee te nemen.
b. Alle onderdelen van de Rijksdienst formuleren hun eigen departementale cloudbeleid en -strategie binnen de kaders van het Rijksbreed cloudbeleid en dit implementatiekader.
c. Besluitvorming, risicoacceptatie, toezicht en monitoring volgt de reguliere afspraken: ministeriële verantwoordelijkheid, departementale mandateringsregeling, CIO-stelsel, BVA-stelsel en de rol van toezichthouders zoals de Algemene Rekenkamer, de Auditdienstrijk en andere specifieke inspectiediensten.
d. Onderdelen van de overheid die niet tot de Rijksdienst behoren zijn niet verplicht om gebruik te maken van dit implementatiekader. Zij worden wel geadviseerd om dit implementatiekader te volgen conform de reguliere besturingslijn.
e. Het Ministerie van Defensie valt buiten de scope van dit implementatiekader.
f. Het gebruik van public clouddiensten is niet toegestaan voor staatsgeheim gerubriceerde informatie. Dit geldt dus ook voor NATO-informatie boven het niveau van NATO Restricted.

Artikel 2 – Definities

	Term	Definitie
a.	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 hier vallen ook daarbij ondersteunende bedrijfsvoeringsprocessen voor zover van wezenlijk belang voor de primaire taken.
b.	Formele DPIA	Een Data Protection Impact Assessment conform artikel 35 AVG.
c.	Pre-scan DPIA	Een analyse om conform de AVG vast te stellen of een formele DPIA noodzakelijk is[3].
d.	DTIA	Data Transfer Impact Assessment: nodig bij internationale overdracht naar landen buiten de EER zonder een adequaatheidsbesluit. Deze term is geïntroduceerd vanwege de aanbevelingen van European Data Protection Board voor het realiseren van voldoende waarborgen.
e.	Public/Private/	Bij de *public cloud* worden de computermiddelen aangeboden

[1] In het cloudbeleid worden publiek en public cloud beide gebruikt. In dit implementatiekader passen we alleen de term public cloud toe.
[2] Zie artikel 2 Besluit CIO- Stelsel Rijksdienst 2021.
[3] Zie bv schema AP: schema_dpia_na_25_mei.pdf (autoriteitpersoonsgegevens.nl).

Hybride cloud door een commerciële partij. Zowel de Rijksoverheid als andere bedrijven en particulieren kunnen een deel van die middelen op hetzelfde platform afnemen. Als één overheidsorganisatie toegang heeft tot computermiddelen, dan spreken we van een *private cloud*. Een private cloud kan in beheer zijn van de Rijksoverheid zelf of exclusief door een marktpartij worden aangeboden. Ter verduidelijking, dit exclusieve karakter heeft betrekking op alle hard- en software voor de dienstverlening. Een mengvorm van de private en public cloud heet een hybride cloud. Een hybride cloud is opgebouwd uit meerdere delen, waarvan sommige in een public en sommige in een *private cloud* zijn ondergebracht.

Artikel 3 – Scope

De scope van dit implementatiekader betreft het materieel public cloudgebruik door de Rijksdienst.

Artikel 3a – Taakverdeling

In het cloudbeleid op pagina 5 staat een algemene taakverdeling. Hierin is in enkele gevallen sprake van een 'gedelegeerde'. De departementen bepalen wie dat per geval is. Ze leggen dat vast in bijvoorbeeld het departementale cloudbeleid of de departementale mandateringsregeling. In onderstaande RACI-tabel zijn de diverse rollen en verantwoordelijkheden verder uitgewerkt:

Tabel 1. RACI-tabel Cloudgebruik

Activiteit	*Proces-eigenaar*	*Dep. Bestuursraad (gedelegeerde)*	*CIO Rijk*	*AIVD en/of MIVD*	*FG / PAR[4] (RPFG)*	*SLM/ inkoop*
Uitvoeren risicoafweging	R	A (R)				C
Uitvoeren (pre-scan) DPIA en evt. DTIA	R	A (R)			C	C
Beoordelen C2000-criteria	R	A (R)		C		
Opstellen Exit-strategie	R	A (R)				C
Verwerking (bijzondere) persoonsgegevens in de cloud	R	A (R)	(I)		C	
Verwerking basisregistraties in de cloud	R	A (R)	C			
Bijhouden en rapporteren materieel cloudgebruik door departementen	R	A (R)	I			
Rapporteren over cloudbeleid aan TK			R/A			
Monitoren uitvoeren cloudbeleid			R/A			

R = Responsible
A = Accountable
C = Consulted
I = Informed

[4] De PAR moet geconsulteerd worden bij rijksbrede voorzieningen. De PAR betrekt hierbij het Rijksplatform FG's.

Artikel 4 – Risicoafweging informatiebeveiliging

1. De departementen en hun onderdelen hebben een formeel vastgestelde risicomanagementmethodiek conform de BIO.
2. Voorafgaand aan het gebruik van public clouddiensten wordt conform die methodiek een risicoanalyse uitgevoerd. Hierbij wordt conform cloudbeleid SLM geraadpleegd[5] ten behoeve van hergebruik van eerdere analyses en waar mogelijk een gezamenlijke aanpak.
3. In die toegespitste risicoanalyse zijn ten minste de volgende onderdelen herkenbaar:
   a. De context van het cloudgebruik en de karakteristieken van het betreffende cloudgebruik zoals beoogde baten, de selectie van de hoofdleverancier en zijn toeleveranciers (zie artikel 5), het type dienstverlening (IAAS, SAAS, PAAS), de gevoeligheid van de type gegevens, de geografische regio van verwerking en opslag van gegevens;
   b. De relevante risico's waarbij aandacht is voor:
      - De C2000 criteria (zie artikel 6 en bijlage 1), de public cloud risicoscenario's (zie bijlage 2) en de vergelijking met de on-premise verwerking;
      - Risico's voor veiligheid van personen voor wie er extra risico's zijn indien persoonsgegevens gelekt worden[6]; en
      - Continuïteitsrisico's onder meer voor de uitvoering van taken.
   c. De analyse van de getroffen technische en organisatorische maatregelen waaruit blijkt dat de eigen implementatie, de dienstverlening door en de leverancier zelf voldoen aan de gestelde informatiebeveiligingseisen met inachtneming van hoofdstuk 15 van de BIO. Hierbij is aandacht voor:
      - Het door de cloudleverancier toelaten van verantwoordingsonderzoeken of rapportages daarover;
      - Een beschrijving van de exit-strategie; en
      - De wijze waarop de leverancier zijn leveranciers beoordeeld, onder meer voor ketenrisico's.
   d. De beoordeling van de opzet, bestaan en, bij de eerste actualisatie, de werking van de maatregelen.
   e. De afweging dat de risico's voldoende gemitigeerd worden met eventuele rest-risico's en de borging daarvan.
4. Die risicoanalyse is formeel vastgesteld conform het cloudbeleid en de departementale mandateringsregeling.

Artikel 5 – Selectie van de hoofdleveranciers

Hou bij het selecteren van de hoofdleverancier rekening met:

1. Onderbouwing van de noodzaak (subsidiariteit) van het cloudgebruik;
2. Privacyvoorwaarden en het vooraf onderhandelen daarover; en
3. Kaders voor publieke waarden zoals voor open source, mensenrechten en duurzaamheid.

Artikel 6 – Beoordeling C2000 criteria

Conform het cloudbeleid worden de C2000 criteria (zie bijlage 1) als volgt beoordeeld:

1. De Rijksorganisaties beoordelen de criteria in samenhang en deze zijn aanvullend op elkaar;

[5] Zie https://slmrijk.pleio.nl/.
[6] Bewindslieden, BN'ers, medewerkers van inlichtingendiensten, getuigen en advocaten in megaprocessen e.d.

2. Als er sprake is van risico's voortkomende uit deze criteria wordt conform cloudbeleid tijdig dreigings- en beveiligingsadvies ingewonnen van AIVD en/of MIVD; en
3. Indien nationale veiligheidsrisico's niet voldoende kunnen worden beheerst (criterium 3B), worden waar mogelijk dergelijke partijen uitgesloten[7].

Artikel 7 – Exit-strategie

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. Onderdelen in de exit-strategie zijn:

1. Voorwaarden aan de leverancier (en toeleveranciers) met aandacht voor dataportabiliteit, serviceportabiliteit en datavernietiging inclusief de processen en voorzieningen die daarvoor nodig zijn;
2. Een alternatieve leverancier of interne landingsplaats;
3. Een strategie, voorwaarden en budget, voor direct vertrek in verband met een crisis of plotselinge (geopolitieke) ontwikkelingen; en
4. Een strategie en budget bij de reguliere afloop van de overeenkomst.

Artikel 8 – (Pre-scan) DPIA[8]

Indien er persoonsgegevens verwerkt gaan worden dient er conform het cloudbeleid en de AVG[9] voorafgaand aan feitelijke verwerking een pre-scan DPIA uitgevoerd te worden en voor hoog-risico verwerkingen een formele DPIA. Vanwege het materiële cloudgebruik, zal naar verwachting een DPIA vrijwel altijd van toepassing zijn. De DPIA moet formeel vastgesteld zijn, conform het cloudbeleid en de departementale mandateringsregeling.

1. In een pre-scan DPIA moeten ten minste de volgende onderdelen herkenbaar zijn[10]:
   a. Een beschrijving van de verwerking inclusief een beschrijving van het type persoonsgegevens (content, telemetrie, diagnostisch, website en helpdesk), de omvang van de gegevensset de omvang van de verwerking, de betrokkenen en het te ondersteunen proces.
   b. Omschrijving van de gebruikersgroepen waaronder de afnemers van de dienst en de afnemers van de informatie.
   c. Een onderbouwde conclusie waarom wel of geen formele DPIA noodzakelijk is.
2. Voor de formele DPIA dient het rijksbrede model toegepast te worden.
3. Indien geen DPIA wordt uitgevoerd, een beschrijving hoe voldaan wordt aan de gestelde privacy-eisen, de beoordeling dat de maatregelen daarvoor feitelijk functioneren en de (lage) rest-risico's.

---

[7] Conform dreigingsbeeld Statelijke Actoren 2, AIVD, MIVD en NCTV, november 2022: Rusland, China, Iran en Noord-Korea.
[8] Data Protection Impact Assessment; ook wel gegevensbeschermingseffectbeoordeling genoemd.
[9] Of andere relevante wetgeving zoals de Wet justitiële en strafvorderlijke gegevens (Wjsg) en de Wet politiegegevens (Wpg).
[10] Artikel 35, lid 1,3 4 en 5 AVG. Aanvullende lijst AP conform artikel 35, lid 4, opgehaald van: https://autoriteitpersoonsgegevens.nl/nl/nieuws/definitieve-dpia-lijst-beschikbaar#:~:text=Een%20DPIA%20is%20verplicht%20als,ook%20wel%20een%20gegevensbeschermingseffectbeoordeling%20genoemd.

4. Bij overdracht naar landen buiten de EER zonder een adequaatheidsbesluit[11], is een DTIA nodig conform aanbevelingen van de EDPB[12] en bij bijzondere persoonsgegevens extra terughoudendheid conform cloudbeleid en dezelfde aanbevelingen van de EDPB.

Indien geen formele DPIA nodig is, moet op een andere wijze aantoonbaar worden voldaan aan de AVG waaronder een onderbouwing van de rechtmatigheid, proportionaliteit, subsidiariteit e.d.

Artikel 9 – Actualisatie analyses

1. Clouddiensten veranderen snel in functionaliteiten, de technische inrichting, de geografische inrichting en de toeleveranciers. De toegespitste risicoanalyse, exit-strategie en (pre-scan of formele) DPIA worden bij wezenlijke wijzigingen in de dienstverlening of wezenlijke verandering van de risico's geactualiseerd inclusief de te nemen passende acties. Dit vindt ten minste iedere drie jaar plaats of vaker als daar aanleiding toe is.
2. Indien analyses op basis van het cloudbeleid met CIO Rijk moeten worden gedeeld, worden de geactualiseerde analyses opnieuw gedeeld met CIO Rijk.
3. Voor bestaande clouddiensten moet conform BIO een risicoanalyse zijn uitgevoerd en conform AVG een DPIA. Ook deze analyses worden binnen hun huidige levenscyclus en ten minste binnen drie jaar herijkt aan het cloudbeleid en het implementatiekader.

Artikel 10 – Openbaarheid van besluitvorming

De eigenaar maakt conform het cloudbeleid gegevens openbaar waaronder de besluitvorming over de DPIA's en, indien van toepassing, adviezen van de PAR. Dit gebeurt uiterlijk drie maanden na de ingebruikname.

Artikel 11 – Melding verwerking persoonsgegevens

Conform voorwaarden 9 en 10 en de tabel op pagina 5 van het cloudbeleid moet in sommige gevallen de DPIA, en waar relevant een explain, aan CIO Rijk worden gestuurd. Die explain omvat minimaal de uitleg waarom het cloudgebruik noodzakelijk is en de (pre-scan of formele) DPIA. De departementen sturen de documenten binnen drie maanden na ingebruikname naar de functionele mailbox van CIO Rijk (CISORijk@minbzk.nl). De ontvangst wordt bevestigd.

Artikel 12 – Advies CIO Rijk vooraf voor basisregistraties

Bij de opslag en verwerking van een basisregistratie in de public cloud adviseert CIO Rijk vooraf conform voorwaarde 11 van het cloudbeleid. Een verzoek tot advies wordt gestuurd naar de functionele mailbox van CIO Rijk (CISORijk@minbzk.nl) inclusief de explain. De explain omvat minimaal de uitleg waarom cloudgebruik noodzakelijk is, de risicoanalyse en, bij verwerking van persoonsgegevens, de (pres-scan of formele) DPIA en eventueel een DTIA en eventuele rest-risico's voor privacy

Voor de doorlooptijd van een advies moet rekening worden gehouden van een maand nadat alle stukken zijn opgeleverd. De feitelijke doorlooptijd

[11] Voorwaarde 9.c uit het Rijksbreed Cloudbeleid 2022.
[12] Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, vastgesteld op 18 juni 2021, opgehaald van: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

hangt af van de aard, omvang en complexiteit van de clouddienst. CIO Rijk werkt hierbij waar mogelijk samen met andere instanties die vanuit hun rol hetzelfde traject beoordelen.
Als basisregistraties of bronnen daarvan al van public clouddiensten gebruik maken, dan wordt dat zo snel mogelijk bij CIO Rijk gemeld.

Artikel 13 – Inzicht en rapportage materieel public cloudgebruik
Conform voorwaarden 3 en 5 van het cloudbeleid houden de departementen hun materieel public cloudgebruik en de risico's daarvan bij. Dit wordt bij wezenlijke wijzigingen en ten minste jaarlijks geactualiseerd.

1. De departementen houden voor het materieel public cloudgebruik ten minste de volgende zaken bij:
   a. Het organisatie-onderdeel;
   b. Het bedrijfsproces en de verantwoordelijke lijnmanager;
   c. Inzicht in de risico's via een actuele risicoanalyse en DPIA; en
   d. De leverancier van de public clouddienst en de afgenomen clouddiensten.
2. 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.

Artikel 14 - Advies en opvolging door CIO Rijk
De ontvangen rapportages, DPIA's en risicoanalyses gebruikt CIO Rijk conform het cloudbeleid en het CIO-stelsel, in de jaarlijkse cyclus van de CIO-gesprekken als onderdeel van haar monitorings- en adviesfunctie. Ook beoordeelt CIO Rijk deze op uitzonderlijke risico's, zoals departement overstijgende risico's waaronder stapelingsrisico's en configuratierisico's vanwege onvoldoende standaardisatie door SSO's. In die gevallen adviseert CIO Rijk, in samenspraak met de departementen, aan het CIO-beraad over de beheersing daarvan en kan conform CIO-stelsel een aanwijzing worden gegeven.[13]
Op basis van de aangeleverde rapportages houdt CIO Rijk een totaaloverzicht bij van het materieel public cloudgebruik. Tevens rapporteert CIO Rijk conform het Cloudbeleid over de voortgang van de implementatie van het Cloudbeleid aan de Tweede Kamer.
Daarnaast kunnen onderzoeken door de Auditdienst Rijk (vraaggestuurd), de Algemene Rekenkamer en mogelijk Inspectiediensten een rol spelen.

Artikel 15 – Overleg en afwijkingen
Indien een departement vragen heeft over de juiste toepassing van het cloudbeleid of het implementatiekader, wordt advies gevraagd aan de CIO Rijk. Als een departement zich niet kan houden aan het cloudbeleid of het implementatiekader, bijvoorbeeld omdat (onderdelen van) de analyses informatie bevatten die niet gedeeld mag worden, wordt in overleg getreden met CIO Rijk, om CIO Rijk in staat te stellen zijn monitorende en adviserende rol uit te voeren.

[13] Artikel 14 lid 2 Besluit CIO-Stelsel Rijksdienst 2021.

Bijlage 1 - 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.[14] 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[15] 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?

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

Bijlage 2 – Risicoscenario's public cloud NBV

Het 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 gecompromitteerd en had gedurende langere tijd toegang tot de data.
- Een (statelijke) actor heeft de cloud fabric 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.[16]

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

Bijlage 3 – Gebruikte afkortingen

Afkorting	*Definitie*
ADR	Auditdienst Rijk
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AP	Autoriteit Persoonsgegevens
ARK	Algemene Rekenkamer
AVG	Algemene Verordening Gegevensbescherming
BVA	Beveiligingsautoriteit
CIO	Chief Information Office
DPIA	Data Protection Impact Assessment
DTIA	Data Transfer Impact Assessment
EDPB	European Data Protection Board
EER	Europese Economische Ruimte
IB	Informatiebeveiliging
ICBR	Interdepartementale Commissie Bedrijfsvoering Rijk
ISO	Internationale Organisatie voor Standaardisatie
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NBV	Nationaal Bureau voor Verbindingsbeveiliging, onderdeel AIVD
RPFG	RijksPlatform Functionarissen Gegevensbescherming
Wjsg	Wet justitiële en strafvorderlijke gegevens
Woo	Wet Open Overheid
Wpg	Wet Politiegegevens