



# Tweede Kamer

DER STATEN-GENERAAL

**Titel/onderwerp : Afwegingskader Cloudtoepassingen Tweede Kamer**

**CIO/ CIO Office**

juli 2021

---

In dit document zijn de elementen van het afwegingskader cloudtoepassingen<sup>1</sup> vastgelegd. Deze worden ter toetsing gebruikt voorafgaand aan elke mogelijke aanschaf van cloudtoepassingen binnen de Tweede Kamer. Daarbij gelden de volgende beleidsuitgangspunten voor cloudtoepassingen:

- Bij de vervanging en vernieuwing van systemen wordt de cloudtechnologie als alternatief meegewogen. Er is (nog) geen sprake van een zogeheten cloud first strategie.
- Parlementair kritische systemen zoals Parlis en Vlos komen vooralsnog niet in aanmerking voor migratie naar de cloud.
- De door de Tweede Kamer ontwikkelde software en data blijft eigendom van de Tweede Kamer.
- Het moet in geval van de beëindiging van een cloud overeenkomst altijd mogelijk zijn de data en software terug te plaatsen in het eigen datacenter. Dit moet worden opgenomen in de hoofdovereenkomst. Evenals afspraken over wat te doen bij faillissement van de leverancier.

Het afwegingskader cloudtoepassingen van de Tweede Kamer omvat de volgende elementen, in aanvulling op de richtlijnen en uitgangspunten die bij opdrachtverstrekking aan leveranciers vanuit de Tweede Kamer al gelden:

Juridische zaken:

1. Bij de afname van clouddiensten en cloudtoepassingen hanteert de Tweede Kamer op het gebied van informatiebeveiliging en bescherming van persoonsgegevens minimaal de eisen die in de BIO gesteld worden.
2. Over de wijze waarop persoonsgegevens door derden worden verwerkt worden afspraken gemaakt in de hoofdovereenkomst dan wel in een aparte verwerkersovereenkomst. Indien de leverancier de primaire taak heeft om persoonsgegevens te verwerken wordt een verwerkersovereenkomst afgesloten. In de andere gevallen is een passage in de hoofdovereenkomst voldoende.
3. De Tweede Kamer behoudt bij het gebruik van clouddiensten het intellectuele eigendomsrecht op de in de cloud geplaatste data en behoudt tevens de zeggenschap over alle gegevens (inclusief persoonsgegevens).
4. Voorafgaand wordt vastgesteld/vastgelegd wie bevoegd is bij een gerechtelijk geschil.

---

<sup>1</sup> Software kan beschikbaar worden gesteld voor installatie in het datacenter van de Tweede Kamer, maar ook als dienst. Dit gebeurt vanuit "de cloud". De "cloud" kan zowel het datacenter van de software leverancier zijn of de leverancier maakt gebruik van een generieke ICT voorziening voor bijvoorbeeld dataopslag. Naast de software die vanuit de cloud wordt aangeboden, kan er ook voor worden gekozen om de onderliggende infrastructuur vanuit de cloud te betrekken, zoals databases, rekenkracht en opslag. Binnen deze cloud-concepten is nog allerlei onderscheid mogelijk, bijvoorbeeld een applicatie wel in de cloud, maar data deels of geheel nog binnen het eigen datacenter. 'De Cloud' biedt een gedifferentieerd en groot scala aan mogelijkheden om de mogelijkheden van ICT en informatievoorziening binnen organisaties te verruimen.



# Tweede Kamer

DER STATEN-GENERAAL

## Informatiebeveiliging:

5. 4.1.4

6.

7.

8.

9.

10.

## Routing van het dataverkeer:

11. De Tweede Kamer heeft slechts beperkte invloed op de wijze waarop het datatransport met de cloudleverancier via internet gerouteerd wordt. Daarom stelt de Tweede Kamer in beginsel als eis dat het dataverkeer met versleuteling beveiligd wordt om zo de integriteit en authenticiteit van die data waarborgen.

## Bescherming Persoonsgegevens/AVG:

12. De Tweede Kamer moet bij contracten met clouddiensten, wanneer de data persoonsgegevens bevatten, altijd nagaan wat de locatie is van de data, om te kunnen bepalen wat het beveiligingsniveau voor de data moet zijn. Data moeten bij voorkeur binnen de EER worden opgeslagen. Wanneer dit niet mogelijk is en de data persoonsgegevens bevat, moet vooraf een TIA (Transfer Impact Assessment) worden uitgevoerd, om vast te stellen of in het derde land van bestemming een in wezen gelijkwaardig beschermingsniveau voor de persoonsgegevens wordt geboden als in de EU/EER.

---

2 4.1.4

3 4.1.4



# Tweede Kamer

## DER STATEN-GENERAAL

13. Aangezien de data-eigenaar bij een datalek aansprakelijk blijft, stelt de Tweede Kamer als eis dat er passende preventieve, repressieve en correctieve maatregelen moeten worden genomen om een data-lek zoveel mogelijk te voorkomen en bij een incident de schade te minimaliseren. Datalekken moeten altijd gemeld worden aan de data-eigenaar (de Tweede Kamer) en worden behandeld volgens de datalekprocedure van de Tweede Kamer.
14. De Tweede Kamer stelt als eis dat een cloudtoepassing aan de AVG-richtlijnen moet voldoen.
15. Tijdens het proces en ter finale toetsing is een aanvullende DPIA (privacy analyse) vereist.
16. Bij het inhuren van IT-bedrijven als verwerker moet een IT-leverancier aantonen te voldoen aan de Data Pro Code<sup>4</sup>.
17. Bij twijfel over de veiligheid van verwerkingen buiten de Economische Europese Ruimte (EER) wordt besloten om de data binnen de EU te houden.

### Exit-strategie:

18. Er dienen bij het afsluiten van een clouddienst ook ontbindende afspraken worden gemaakt om het contract te kunnen beëindigen (contract beëindiging)
19. Deze ontbindende exit-afspraken omvatten zowel de data, als de gebruikte software, inclusief de mogelijke gevolgen voor de beschikbare functionaliteit.
20. De opzegtermijn dient voldoende tijd te geven om te migreren van cloud naar eigen beheer. Eventuele data en configuratiegegevens mogen niet verwijderd worden, totdat de migratie van de cloud naar systemen van de Tweede Kamer succesvol is uitgevoerd.
21. Er worden afspraken gemaakt over hoe gecontroleerd wordt dat alle data is aangeleverd en geen data achterblijft bij de leverancier.

---

<sup>4</sup> <https://www.nldigital.nl/data-pro-code/> De Data Pro Code is een nadere uitwerking van de verplichtingen voor dataverwerkers op grond van artikel 28 AVG en is van toepassing op verwerkingen in Nederland. De Data Pro Code geeft concrete gedragsregels voor verwerkers. De kern daarvan vormen de informatieplichten voor de dataverwerker en de verantwoording door middel van toezicht