

Cloudbeleid

2022-2024



Inleiding

Gebruik van applicaties voor primaire en secundaire processen in de cloud is niet meer uit de praktijk weg te denken. Onder opslag in de cloud vallen alle applicaties en data die bij derden voor beheer zijn ondergebracht: software as a service (SAAS) en platform as a service (PAAS). Voorbeelden hiervan zijn Sharepoint, het personeelsinformatiesysteem Motion en de opslag van de digitale bestemmingsplannen. In de toekomst is het denkbaar dat het e-depot (duurzaam beheer van digitale archiefbescheiden.) ook als dienst in de cloud zal worden afgenomen. De laatste tijd neemt de ontwikkeling een vlucht. In dit beleidsdocument zijn beleidsregels en beheerafspraken opgenomen voor applicaties in de cloud.

Bij cloudvoorzieningen gelden de eisen die voor iedere uitbesteding van diensten gesteld worden: beheer en controle van de afspraken met de leverancier moeten goed belegd zijn bij de gemeente. In dit document worden de taken en verantwoordelijkheden toegewezen. Daarnaast is het uitgangspunt om zoveel mogelijk aan te sluiten bij de standaarden die gelden volgens de GIBIT¹, de BIO², en de wettelijke eisen die voortvloeien uit de AVG (afspraken vastleggen in een verwerkersovereenkomst wanneer er persoonsgegevens verwerkt worden).

Uitgangspunt.

De gemeentesecretaris is namens de organisatie eindverantwoordelijk voor de betrouwbaarheid (beschikbaarheid, exclusiviteit en integriteit) van de uitbestede diensten. Managers zijn per afdeling verantwoordelijk voor hun eigen systemen waarbij de teamleiders proceseigenaar zijn en daarbij verantwoordelijk voor de ingerichte processen in hun vak-applicatie.

De proceseigenaar wordt hierbij ondersteund door de adviseurs informatievoorziening van de afdeling Dienstverlening. Door hen tijdig te betrekken kunnen aspecten als privacy, beveiliging, architectuur en archivering worden meegenomen in het programma van eisen en bij de contractonderhandelingen.

Ook in de huidige 'on-premise' situatie zijn bovenstaande verantwoordelijkheden actueel en als zodanig bekend.

¹ Gemeentelijke Inkoop bij IT

² Baseline Informatiebeveiliging Overheid

1. Organisatie niveau

Rollen en verantwoordelijkheden

a. Systeemeigenaar

Binnen een afdeling wordt gebruik gemaakt van verschillende vak applicaties (systemen). De manager van de afdeling is systeemeigenaar van de systemen die in zijn of haar afdeling worden gebruikt.

b. Proceseigenaar

Het team levert interne of externe diensten, waartoe processen zijn ingericht. De procesafhandeling wordt ondersteund met ICT middelen en applicaties. De teamleider van het team waarbinnen het systeem wordt gebruikt, is proceseigenaar. Dit betekent ook dat de proceseigenaar verantwoordelijk blijft voor de gegevens en diensten die zij in de Cloud opslaat en gebruikt, en dient een afgewogen keuze te maken of een informatiesysteem in de Cloud gebruikt mag en kan worden.

c. Informatieadviseur, inkoopadviseur en adviseur privacy.

De adviseurs van de afdeling Dienstverlening zijn beschikbaar om de teamleider te ondersteuning bij het proces van oriëntatie, vergelijking en selectie van een nieuwe cloud ICT dienst. Het door deze adviseurs uitgebrachte advies telt zwaarwegend mee in de keuze voor een dienst of dienstverlener.

d. Eindverantwoordelijke

De gemeentesecretaris is namens de organisatie eind verantwoordelijk voor de betrouwbaarheid (beschikbaarheid, exclusiviteit en integriteit) van uitbestede diensten. Voor inwoners en bedrijven is er geen onderscheid tussen betrouwbaarheid van de diensten, in de cloud of niet.

e. Een uitbesteding is goedgekeurd door de voor het informatiesysteem verantwoordelijke systeemeigenaar.

2. Governance

- a. De governance vindt plaats in overleg tussen de wijzigingsadviescommissie (³WAC) en het strategisch informatie overleg (⁴SIO)
- b. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheidseis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald, zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen. Bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen.
- c. Er zijn voor beide partijen eenduidige aanspreekpunten.
- d. Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen.
- e. In het geval van verwerken van persoonsgegevens is er een verwerkersovereenkomst waarin helder alle rechten en plichten van de leverancier en de gemeente zijn vastgelegd. De vastgelegde beveiligingsmaatregelen worden jaarlijks door de gemeente geaudit bij de leverancier.
- f. Er worden afspraken gemaakt tussen de systeemeigenaar en de leverancier over de inhoud van rapportages, zoals over het melden van incidenten en autorisatiebeheer.
- g. Er zijn continuïteitsplannen voor het herstel van incidenten, zoals aanvallen met malware waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.

³ WAC: A.H.Grooten, D.Venhuis, J.Hoekman, M.Kruijswijk, P.Harders, R.Weeseman

⁴ SIO: G.J. van der Zanden, A.H.Grooten, M.Kruijswijk, A.Kramer, R.Weeseman, J.Hoekman, J.Davidse

3. Data opslag

a. Algemeen

- i. Voor cloudopslag is Microsoft Azure de standaard. Afwijkingen kunnen alleen worden gebruikt na toestemming van de teamleider ICT.
- ii. Opslag binnen landen in de Europese Unie is verplicht.
- iii. Opdrachten aan kleine zelfstandigen voor data-opslag en het delen van data moeten eerst overlegd worden met de teamleider ICT.
- iv. Data-uitwisseling in informatieketens moet gemeld worden bij de teamleider ICT en het SIO.
- v. Er moet worden voldaan aan de continuïteitseisen zoals worden uitgewerkt in hoofdstuk 4. Hosting van de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT), artikel 32. Waarborgen continuïteit. Data-Escrow is hier een voorbeeld van.

b. Bijzonder: 'Sharepoint'

- i. Medewerkers blijven verantwoordelijk voor gegevens die worden opgeslagen op persoonlijke drive's in de Cloud (en lokaal).
- ii. Data opgeslagen op de Sharepoint omgeving (Cloud) binnen Microsoft Teams blijft een verantwoordelijkheid voor de eigenaar van het ingerichte Team. Dat betekent dus ook voor de zaakgerichte archivering van de data in Decos Join.
- iii. Gebruik van Cloud opslag diensten als Dropbox etc is voor bedrijfsgegevens niet toegestaan.

4. Aandachtspunten bij inkoop.

- a. Bij de inkoop van clouddiensten wordt gebruik gemaakt van de GIBIT, en wordt naast de hoofdovereenkomst een verwerkersovereenkomst en een SLA opgesteld.
- b. Beheerafspraken dienen in een Service Level Agreement (SLA) te worden vastgelegd dat onderdeel uitmaakt van de overeenkomst. In een SLA beschrijft de door de dienstleverancier geleverde diensten en specificaties van de applicatie, systeem of dienst, zoals deze aan de gemeente wordt aangeboden.
- c. Beveiligingskenmerken, niveaus van dienstverlening en beheers-eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
- d. De details hiervan zijn uitgewerkt in hoofdstuk II. Privacy, beveiliging en archivering van de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) in de artikelen Artikel 24. Bewerkersrelatie, Artikel 25. Verwerking persoonsgegevens, Artikel 26. Informatiebeveiliging, Artikel 27. Meldplicht beveiligingsincidenten.
- e. Zodra de gemeente de verwerking van persoonsgegevens uitbesteedt, moeten er afspraken worden gemaakt over de verwerking. Die afspraken moeten schriftelijk worden vastgelegd. Het document waarin deze afspraken worden vastgelegd noemen we een verwerkersovereenkomst. Wanneer de gemeente bijvoorbeeld een cloudopslagdienst afneemt bij een leverancier en hier onder andere persoonsgegevens in wil opslaan, dan kan de leverancier aangemerkt worden als verwerker. De opdracht betreft namelijk het opslaan van persoonsgegevens – het verwerken van persoonsgegevens in de cloud.
- f. We maken daarbij gebruik van de door de VNG opgestelde standaard verwerkersovereenkomst waar een groot aantal ICT leveranciers zich aan hebben gecommitteerd.
- g. De in de verwerkersovereenkomst of dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld door audits of rapportages en gebeurt minimaal eens per jaar (voor ieder systeem). De details zijn uitgewerkt in bijlage 2: Aantonen passend niveau van beveiliging (van de standaard verwerkersovereenkomst).
- h. Bij transport van vertrouwelijke informatie over onbetrouwbare netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast. De details zijn uitgewerkt in hoofdstuk 13, Communicatiebeveiliging van de Baseline Informatiebeveiliging Overheid (BIO)
- i. Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware, zoals uitgewerkt in artikel 12.2 van de BIO.