INFORMATIE
BEVEILIGINGS
DIENST

CLOUD COMPUTING

Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Cloud Computing

Versienummer
1.2

Versiedatum
Juni 2016

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie:

Versie	Datum	Opmerkingen
1	11-11-2013	Eerste versie van de BIG
1.01	03-08-2015	Kleine tekstuele aanpassingen
1.2	03-06-2016	Aanpassing obv huidige wet- en regelgeving

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Voorwoord

De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. Aanleiding voor de oprichting van de IBD vormen enerzijds de leerpunten uit een aantal grote incidenten op informatiebeveiligingsvlak en anderzijds de visie Digitale Overheid 2017.
De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen.

De IBD heeft drie doelen:

1. het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.
2. het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
3. het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen. De ondersteuning die de IBD biedt bij het ICT-Beveiligingsassessment DigiD is een voorbeeld van zo'n project.

Hoe realiseert de IBD haar doelen?
Om invulling te kunnen geven aan haar doelen is door de IBD op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) een vertaalslag gemaakt naar een baseline voor de gemeentelijke markt. Deze Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) betreft twee varianten, een Strategische- én een Tactische Baseline. Beide varianten van de BIG zijn beschikbaar voor alle gemeenten op de community van de IBD, zodat door iedere gemeente tot implementatie van de BIG kan worden overgegaan. Bestuur en management hebben met deze baseline een instrument in handen waarmee zij in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging. Om de implementatie van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD in samenwerking met de Taskforce Bestuur en Informatieveiligheid Dienstverlening producten ontwikkeld op operationeel niveau. Dit heeft een productenportfolio opgeleverd, genaamd de Operationele Baseline Nederlandse Gemeenten. Onderhavig product is onderdeel van het productenportfolio.

Naast een productenportfolio, heeft de IBD voor gemeenten ook een dienstenportfolio ontwikkeld. Voor een volledig overzicht van het producten- en dienstenportfolio, kunt u terecht op de website van de IBD.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: WBP, GBA, SUWI, BAG en PUN, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er in de naleving van dat kader ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Doel
Dit document geeft uitgangspunten weer, gezien vanuit informatiebeveiliging, voor een invulling van het Cloud Computing beleid voor gemeenten. Deze beleidsuitgangspunten informatiebeveiliging zijn afkomstig uit de BIG en het beleid is daarmee compliant aan de BIG. Deze beleidsuitgangspunten zijn opgenomen in hoofdstuk 4 'Gemeentelijk Cloud Computing beleid'.

Doelgroep
Dit document is van belang voor het Bestuur (voor het beleid), het Management, het Systeembeheer en voor de gebruikers.

Relatie met overige producten

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
  - Tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
- Gemeentelijk beveiligingsbeleid
- Contracten, waaronder SLA's of bewerkersovereenkomsten

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
Maatregel 10.2

Cloud Computing raakt alle maatregelen die de gemeente zelf moeten nemen in de eigen infrastructuur. Deze maatregelen worden vervolgens gedeeld door de Cloud- leverancier en door de gemeente uitgevoerd.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Inhoud

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN

1 Inleiding

Cloud Computing wordt door gemeenten gebruikt om via het internet, of een andere breedbandige verbinding gebruik te maken van hardware, software en gegevens. Deze Cloud kan zich overal bevinden.

Het woord Cloud komt van het woord 'wolk' waarmee in een netwerk ontwerpen vaak het internet of een netwerk wordt getekend. Deze wolk staat voor een netwerk dat met al de computers die erop aangesloten zijn een soort 'wolk van computers' vormt. De eindgebruiker weet niet waar de computers zich in de Cloud bevinden en ook niet waar de software draait of waar gegevens zich bevinden. Afhankelijk van het type Cloud is men meer of minder eigenaar van de infrastructuur. Omdat men niet precies weet waar afgenomen Cloud-diensten zich bevinden, is wetgeving relevant voor de afgenomen Cloud-diensten.

Cloud Computing is volgens de NIST1 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 is relevant voor de BIG omdat het afnemen van Cloud-diensten gevolgen heeft voor de plaats waar informatiebeveiligingsmaatregelen worden uitgevoerd. Hierbij is het van belang dat als een gemeente van Cloud-diensten gebruik maakt de gemeente altijd verantwoordelijk blijft voor de juiste beveiliging van haar gegevens en ook de privacy waarborgt.

1.1 Doelstelling handreiking

De hier voorgestelde Cloud Computing gemeenten handleiding beschrijft een good practice voor Cloud Computing. De leidraad biedt handvatten om rekening mee te houden als men over Cloud Computing nadenkt of dit wil implementeren.

[1] NIST is National Institute of Standards and Technology (USA)

2 Cloud Computing

Bij Cloud Computing worden hardware, software en gegevens beschikbaar gesteld via het internet. De eindgebruiker weet vaak niet meer op welke computers en waar (fysiek) zich de diensten bevinden die hij of zij afneemt. Bij Cloud Computing wordt vaak gebruik gemaakt van hardware die het mogelijk maakt om flexibel te schalen naar de behoefte van de eindgebruiker. Bovendien is de eindgebruiker vaak geen eigenaar meer van de hard- en of software. Men zou kunnen zeggen dat het gaat om virtuele infrastructuur en diensten. Met Cloud Computing worden servers, desktops en ook applicaties gevirtualiseerd. Dit heeft zowel voordelen als nadelen.

Het NCSC heeft een document gemaakt over Cloud Computing, in deze handreiking wordt ingegaan op specifieke aandachtspunten voor organisaties met betrekking tot Cloud Computing. Daarnaast heeft het Instituut voor Informatierecht van de Universiteit van Amsterdam in 2012 een onderzoek gepubliceerd over Cloud-diensten in het hoger onderwijs en de USA Patriot Act. Tilburg University heeft in opdracht van SURFnet uitgebreid onderzoek gedaan naar de privacy aspecten bij het gebruik van Cloud services in het onderwijs. Hoewel toegespitst op het onderwijs, staan er veel algemene privacyaspecten in uitgelegd.

Dit document is geen juridisch sluitend stuk. In dit document wordt algemeen ingegaan op wetgeving. Het is raadzaam om bij twijfel over de omgang met Cloud Computing en/of de verwerking van (persoons) gegevens in het buitenland een jurist te raadplegen. Alvorens gebruik te maken van diensten op basis van Cloud Computing dient door het management een afgewogen keuze gemaakt te worden waarin alle argumenten worden meegewogen.

Bij het afnemen van Cloud-diensten door de gemeente wordt geen verantwoordelijkheid overgedragen. De gemeente is en blijft verantwoordelijk voor de manier waarop een Cloud-leverancier omgaat met informatiebeveiliging. In het geval van persoonsgegevens is dit geregeld in de WBP Artikel 14.

Links:
Een volledig overzicht betreffende Cloud Computing is te vinden bij het NCSC:
https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-Cloud Computing.html

Het onderzoek van de afdeling Instituut voor informatierecht van de UVA naar het gebruik van Cloud-diensten in het hoger onderwijs en de USA Patriot Act:
http://www.ivir.nl/publicaties/vanhoboken/Clouddiensten_in_HO_en_USA_Patriot_Act.pdf

Het onderzoek van het Tilburg Institute for Law, Technology and Society (Tilburg University) naar privacy aspecten bij Cloud services:
http://www.surfsites.nl/Cloud/download/De_wolk_in_het_onderwijs_feb2011.pdf

Cloud Computing op de KING website:
https://www.kinggemeenten.nl/sites/king/files/Handreiking_CloudOverheden_Taskforce_LR.pdf

Kamerbrief over Cloud Computing:
http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/04/20/kamerbrief-over-cloud-computing.html

Karakteristieken van Cloud Computing
Cloud Computing wordt soms als synoniem gezien van Shared Service Centra er zijn echter enkele kenmerkende verschillen. Cloud Computing kent een aantal karakteristieken, deze zijn:

- Zelfbediening (On-demand self-service)

De afnemer van Cloud diensten kan servertijd en opslag zonder tussenkomst van de aanbieder wijzigen als dat nodig is.

- Breedbandige toegang

Er is toegang mogelijk via breedbandverbindingen met verschillende soorten cliënt platvormen (fat cliënt, thin cliënt, mobiele apparatuur etc.).

- Gedeelde middelen (resource pooling)

De fysieke en logische middelen van de Cloud-aanbieder worden door alle afnemers gebruikt en dynamisch toegewezen indien nodig. De afnemers gebruiken dezelfde applicatie instantie waarbij data wel per afnemer gescheiden wordt opgeslagen (Multi Tenancy Model). De afnemer heeft geen weet van de locatie waar de middelen zich bevinden. Voorbeelden van middelen zijn: opslag, rekenkracht, geheugen en netwerk bandbreedte.

- Elasticiteit

Middelen kunnen op korte termijn (automatisch) worden toegewezen en vrijgegeven op basis van vraag. De middelen lijken op elk moment onbeperkt voor de afnemer.

- Meetbare service

De Cloud-systemen controleren en optimaliseren middelen door middel van toepasselijke metingen (opslag, geheugen, rekenkracht etc). Het gebruik van middelen wordt transparant gemonitord, gecontroleerd en gerapporteerd aan de afnemer en de aanbieder van de gebruikte dienst.

De risico’s en beveiligings-aandachtspunten van Cloud Computing en Shared Service Centra zijn gelijk, in dit document wordt niet verder ingegaan op deze verschillen.

Soorten Cloud Computing (deployment model)
Cloud Computing kan op verschillende manieren worden toegepast. Er zijn 3 verschillende vormen: een externe of publieke Cloud, waarbij diensten en gegevens bij een externe partij zijn opgeslagen, een private Cloud binnen bijvoorbeeld een rekencentrum van een gemeente, en er is een hybride vorm.

- Bij een **publieke of externe Cloud** staan de hardware, software en de gegevens volledig bij de externe dienstverlener en er wordt een generieke (voor alle afnemers gelijke) dienst geleverd.

- Bij een **private Cloud** werkt men op een private ICT-infrastructuur waarop servers / desktops en applicaties worden gevirtualiseerd. In deze Cloud heeft de gemeente de volledige controle over gegevens, beveiliging en kwaliteit van de dienst. Vaak ligt de verantwoordelijkheid voor onderhoud en beheer bij de gemeente zelf maar in de praktijk wordt dit vaak door een leverancier uitgevoerd. De private Cloud kan in een gemeentelijk datacentrum draaien, maar ook bij een leverancier. In dat geval wordt de gevirtualiseerde infrastructuur niet gedeeld met andere klanten.

- Een bijzondere vorm van een private Cloud is de **Community Cloud**, hierbij wordt Cloud-infrastructuur gebruikt door een specifieke groep afnemers die een gemeenschappelijk belang hebben. Denk hierbij aan taak, missie, beveiligingseisen, beleid en naleving eisen. Deze Cloud kan in eigendom zijn en beheerd worden door een van de deelnemers, een derde partij of een combinatie. Men kan hierbij denken aan een overheids Cloud of een gemeentelijke Cloud.

- De **hybride Cloud** is een combinatie van een publieke en private Cloud. Dat wil zeggen dat er Cloud-diensten worden afgenomen van een derde aanbieder terwijl men daarbij ook gebruik maakt van een eigen Cloud.

Als een private Cloud niet in een gemeentelijk rekencentrum staat, maar op een aparte infrastructuur bij een leverancier dan is dat technisch gezien een dienst die in een externe Cloud wordt afgenomen op specifieke gevirtualiseerde omgevingen. Dan zijn de eisen in dit document onverkort van toepassing.

Servicemodellen Cloud Computing
De volgende manieren van het aanbieden van Cloud Computing worden onderkend:

- SaaS – Software as a Service
- PaaS – Platform as a Service
- IaaS – Infrastructure as a Service

Deze drie vormen staan bewust in deze volgorde, van onder af aan begint men met infrastructuur waarop platforms draaien die het mogelijk maken applicaties te draaien.

Cloud-applicaties: Software as a Service (SaaS)

Bij Software as a Service worden applicaties via de Cloud aangeboden aan eindgebruikers. Er zijn verschillende gemeenten die applicaties nu al via een SaaS-model afnemen en dat gebeurt in publieke en private Clouds. Vaak worden hier webapplicaties aangeboden die met moderne technologieën zoals Ajax en HTML5 gemaakt zijn. Voor de eindgebruiker is volledig onduidelijk waar de applicatie zich bevindt, op welk platform de applicatie draait en waar de gegevens zich bevinden.

Cloud-platforms: Platform as a Service (PaaS)

Als de gemeente zelf software wil installeren in een Cloud dan kan gebruik gemaakt worden van PaaS. Bij PaaS kan men binnen grenzen de software en de configuratie zelf regelen. De eindklant van een PaaS-oplossing is vaak de eigen ICT-organisatie. Op de PaaS-omgeving worden vaak uiteindelijk weer de eigen applicaties geplaatst voor de eindgebruiker.

INFORMATIE BEVEILIGINGS DIENST

Cloud-infrastructuur: Infrastructure as a Service (IaaS)

Indien men nog meer vrijheden wil hebben kan men alleen de (gevirtualiseerde) infrastructuur afnemen. Hier vindt men servers, netwerk componenten, opslagcapaciteit en andere infrastructuur. Dit geeft de gemeentelijke ICT-afdeling volledige vrijheid over de hardware die virtueel wordt afgenomen, bovenop de IaaS hardware kan de ICT-afdeling weer platform services draaien en daar bovenop weer eigen software. Beheer kan op afstand worden gedaan vanaf iedere plek.

Schematisch wordt dit als volgt weergegeven:

Servicemodellen	Eigen rekencentrum	Infrastructuur als een service	Platform als een service	Software als een service
Lagen	Applicatie	Applicatie	Applicatie	Applicatie
	Applicatie platform	Applicatie platform	Applicatie platform	Applicatie platform
	Fysieke infrastructuur	Fysieke infrastructuur	Fysieke infrastructuur	Fysieke infrastructuur

Blauw = zelf doen, wit = laten doen

Voordelen van Cloud Computing.

- De Cloud-diensten zijn via internet te benaderen, het ondersteunt in dat geval ook flexibel (plaats en tijd onafhankelijk) werken.
- Cloud-diensten kunnen flexibel omgaan met wijzigende vragen. Men kan eenvoudig groeien en krimpen al naar gelang de behoefte, en dat in korte tijdsspannen.
- Er zijn flexibele verreken mechanismes: betalen per gebruiker, betalen per virtuele machine of dienst.
- Men gaat uit van een hogere beschikbaarheid, hoewel dit afhankelijk is van het service niveau van de aanbieder.
- De aanbieder heeft vaak de beschikking over voldoende gespecialiseerd personeel, men heeft zelf minder gespecialiseerde beheerders nodig. Met gebruik van Cloud worden dus niet alleen gegevensop afstand gezet, maar ook de complexiteit van de systemen.

Nadelen en risico's van Cloud Computing.

- Bij publieke/externe Clouds is voor een gebruiker niet inzichtelijk op welke systemen en in welke landen gegevens zich bevinden. Dit kan ook op plaatsen zijn waar gegevens niet mogen staan volgens onze wetgeving of waar andere wetgeving geldt dan in Nederland of Europa
- Voor de toepasselijkheid van wetgeving maakt het niet uit *waar* data fysiek staat. Als een Amerikaans bedrijf een dochteronderneming met datacenters in Ierland heeft, dan is het Amerikaans recht op die gegevens in Ierland van toepassing. In zoverre dat die gegevens onder de reikwijdte van een Amerikaans data-vorderingsbevel kunnen vallen. Ook ingeval een Amerikaans bedrijf dochterondernemingen heeft met datacenters over de hele wereld, dan heeft dat Amerikaanse moederbedrijf in principe toegang tot die data, en valt daarmee die data onder de reikwijdte van Amerikaanse wetgeving. Een ander perspectief: als een Nederlandse gemeente gebruik maakt van een Cloud-dienst uit de Verenigde Staten (VS), dan is die Nederlandse gemeente wettelijk gezien ervoor verantwoordelijk dat de gegevens in de VS behandeld worden volgens de Nederlandse privacy wetgeving. Dat dit in de praktijk lastig waar te maken is behoeft weinig verdere uitleg

- Cloud is niet altijd storingsvrij. Bij het gebruik van een externe Cloud ben je voor de continuïteit afhankelijk van een derde partij. Hoe meer diensten en gegevens er in de Cloud staan, hoe problematischer storingen kunnen zijn
- Aangezien Clouds via internet kunnen worden benaderd, zijn ze daarmee ook inherent lastiger te beveiligen.
- Als men al weet waar de Cloud-dienst draait is het ook zaak om na te gaan via welke weg deze Cloud-diensten benaderd worden. Het kan goed zijn dat de Cloud-dienst zich in Nederland bevindt maar dat de netwerk leverancier een niet Europees bedrijf is.
- Bij het aangaan van een Cloud service is het zaak goed af te spreken wat de gevraagde en afgesproken dienstverlening is. Dat voorkomt dat na het aangaan van de overeenkomst opeens allerlei zaken buiten de afspraak blijken te vallen en dan als 'extra' en tegen vaak hogere tarieven gefactureerd worden.
- Met name bij externe Clouds is niet te controleren in hoeverre de leverancier jouw diensten en gegevens inziet.
- Als gegevens eenmaal in de Cloud staan, is het heel lastig ze er weer uit te halen, of te migreren naar een andere Cloud provider. Houd dus rekening met een lock-in probleem. Het is dus zaak voor een gemeente om een Exit- strategie te hebben voordat een overeenkomst wordt aangegaan met een externe partij.

3 Cloud-aandachtspunten

Gegevens in het buitenland

In de Wet Bescherming Persoonsgegevens (WBP) hoofdstuk 11, Artikelen 76-78 staan regels omtrent gegevensverkeer met landen *buiten* de Europese Unie (EU). Binnen de EU zijn data-uitwisselingen zonder meer toegestaan, omdat de Europese privacywetgeving daar van kracht is. Het verzenden en opslaan van persoonsgegevens in landen buiten de EU is toegestaan als:

- Er door dat land een passend niveau van gegevensbescherming wordt geboden. Welke landen dit zijn, wordt bepaald door de Europese Commissie. Momenteel zijn dit: Noorwegen, IJsland, sommige Kanaaleilanden, Argentinië, Canada, Zwitserland
- In februari 2016 zijn de EU en de VS het eens geworden over het EU-VS privacyshield[2]. Dit is de opvolger van het Safe Harbor verdrag, dat in 2015 door het Europese hof ongeldig is verklaard. De Artikel 29-werkgroep, het overlegorgaan van de Europese privacytoezichthouders, heeft inmiddels laten weten dat ze gebreken heeft geconstateerd in de Privacy Shield-overeenkomst en stelt voor aanpassingen door te voeren.Er geen passend beschermingsniveau is, maar er wordt voldaan aan een uitzondering in de WBP. Hieronder zijn begrepen de situaties waarbij degene op wie de gegevens betrekking hebben hiertoe ondubbelzinnige toestemming heeft verleend; de minister hiertoe een vergunning heeft verleend en de verwerking noodzakelijk is in het kader van de uitvoering van een contract. Zie verder Art. 77 WBP.

De VS

Op basis van het EU-VS Privacyshield mogen persoonsgegevens naar Amerika worden verzonden en daar worden verwerkt. Het EU-VS Privacyshield bevat principes die gebaseerd zijn op de Europese privacy wetgeving.

Verplichtingen Amerikaanse bedrijven

Voor Amerikaanse bedrijven die persoonsgegevens uit Europa willen invoeren, gelden verplichtingen inzake de verwerking van persoonsgegevens en het waarborgen van individuele rechten. Het Department of Commerce zal erop toezien dat ondernemingen hun verbintenissen bekendmaken, zodat de nakoming daarvan op grond van de Amerikaanse wetgeving kan worden afgedwongen door de Federal Trade Commission van de VS. Bovendien moet elke onderneming die personeelsgegevens uit Europa verwerkt, zich ertoe verbinden besluiten van Europese gegevensbeschermingsautoriteiten na te leven.

Waarborgen t.a.v. toegang door de Amerikaanse overheid

De Verenigde Staten hebben de EU schriftelijke garanties gegeven dat de toegang die overheidsinstanties ten behoeve van rechtshandhaving en de nationale veiligheid hebben tot gegevens, wordt onderworpen aan duidelijke beperkingen, waarborgen en controlemechanismen. Uitzonderingen gelden alleen wanneer zij noodzakelijk en evenredig zijn. De VS heeft uitgesloten dat persoonsgegevens die in het kader van de nieuwe regeling naar de VS worden doorgegeven, willekeurig en op grote schaal worden gecontroleerd. Elke burger die vindt dat zijn gegevens in het kader van de nieuwe regeling zijn misbruikt, zal over verschillende beroepsmogelijkheden beschikken.

Het is aan te raden bij het gebruik van Cloud-technologie zich goed af te vragen aan welk recht een Cloud provider moet voldoen. Lees hiervoor ook het volgende document van het CBP:

[2] http://europa.eu/rapid/press-release_IP-16-216_nl.htm

http://www.cbpweb.nl/downloads_med/med_20120910-zienswijze-toepassing-wbp-SURFmarket-Cloud-computing.pdf

Cloud en Privacy

De Wet Bescherming Persoonsgegevens (WBP) stelt eisen aan het verwerken van persoonsgegevens en aan de verantwoordelijke en de bewerkers van die gegevens, en de relatie tussen beiden. Zie Art. 14 Wbp. Een leverancier van Cloud-diensten kan als bewerker worden gezien, waarmee de verantwoordelijke, in dit geval de gemeente een aantal zaken moet regelen. Deze vereisten staan opgesomd in Art. 14 WBP. Dit zijn wettelijke vereisten waaraan men moet voldoen.
Daarnaast staan in het NCSC stuk de verantwoordelijkheden en verdeling van beveiligingsmaatregelen van alle partijen goed weergegeven. In ieder geval moeten bij het afnemen van Cloud-diensten, waarbij persoonsgegevens worden bewerkt een aantal maatregelen worden genomen:

1. Passende maatregelen nemen. De baseline voor Nederlandse gemeenten is een goede start. Bij twijfel moet door de verantwoordelijke (de gemeente) altijd een risicoanalyse worden uitgevoerd op het gebruik van de Cloud-dienst. Daarnaast geeft het eerder genoemde stuk van het NCSC een goed vertrekpunt
2. Toezien op naleving van de maatregelen. Als verantwoordelijke is de gemeente verplicht om Opzet, Bestaan en Werking van maatregelen te (laten) toetsen.
3. Alle beveiligingsafspraken dienen te worden vastgelegd in een bewerkersovereenkomst of een contract. Deze bewerkersovereenkomst is een apart product dat de IBD als voorbeeld heeft geleverd.

Uitgangspunt is dat het management te allen tijde een bewust keuze moet maken of persoonsgegevens in de Cloud kunnen worden verwerkt. De verantwoordelijke, in dit geval de gemeente, is eindverantwoordelijk voor de naleving van de WBP.

Bijzondere persoonsgegevens

Het verwerken van bijzondere persoonsgegevens, zoals beschreven in artikel 16 van de WBP, dient te worden vermeden in de Cloud. Deze mogen slechts zeer beperkt worden verwerkt. Onder bijzondere persoonsgegevens zijn onder meer begrepen persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid en seksuele leven.
Bij het verwerken van medische gegevens rondom een inwoner van de gemeente kan beter geen gebruik gemaakt worden van een Cloud-oplossing als de bewerker (leverancier van Cloud-diensten) toegang kan hebben tot deze gegevens. Ook hier geldt dat de WBP moet worden nageleefd en dat er altijd een risicoanalyse nodig is om het juiste beveiligingsniveau vast te stellen en te controleren op naleving. Het gaat er om dat de vastgestelde eisen bij de leverancier geborgd worden. Het management dient een bewuste keuze te maken omtrent het verwerken van bijzondere gegevens in de Cloud en bij voorkeur wordt vooraf juridisch advies gevraagd. Zie hiervoor ook:
http://www.cbpweb.nl/downloads_inf/inf_va_geheimhouding_medische_gegevens.pdf

Informatiebeveiliging en de Cloud

Voor het handhaven van vertrouwelijkheid, integriteit en beschikbaarheid van de gemeentelijke informatiesystemen en/of gegevens in de Cloud zijn beveiligingsmaatregelen nodig die door de gemeente en de Cloud-leverancier uitgevoerd moeten worden. Voor de verdeling van maatregelen tussen beide partijen kan het eerder genoemde stuk van het NCSC goed gebruikt worden (zie in het betreffende stuk bijlage J). Op basis van de BIG maatregelen en eventuele maatregelen uit een aanvullende risicoanalyse dient een vergelijkbare verdeling te worden gemaakt waarbij de

verantwoordelijkheid voor het uitvoeren van maatregelen en de controle erop wordt vastgelegd. Een voorbeeld:

- Gebruiksbeheer (wie heeft toegang tot een systeem) is een gemeentetaak, evenals het maken van toegangsbeleid. Het maken van een auditlog over toegang is weer een leverancierstaak.
- Het maken van back-ups van een Cloud-systeem is een leverancierstaak, bij IaaS is dit weer een gemeentetaak.
- Encryptie, hoe wordt de eigen data beschermd.

Zie tevens de nieuwe versie van de bewerkersovereenkomst waar op basis van verschillende cloud servicemodellen aandacht is voor verschillende beveiligingsmaatregelen.

Contracten en de Cloud

In contracten met een Cloud-leverancier dient aandacht te zijn voor de volgende zaken:

- Specifieke beveiligingsmaatregelen afkomstig uit een risicoanalyse of de BIG
- Het verplicht melden van beveiligingsincidenten aan de gemeente
- Looptijd van het contract
- Beschrijving van basispakket en aanvullende (optionele) diensten en de daarvoor gehanteerde tarieven
- Een escrow regeling (of Cloud escrow regeling)[3]
- Software licenties (van wie zijn deze en mogen deze in een Cloud worden gebruikt)
- Conversie van gegevens
- Overdacht van gegevens van- en naar de Cloud-omgeving
- Vernietiging van gegevens bij contract beëindiging
- Continuïteit van het systeem
- Overdracht naar een andere leverancier
- Back-up en uitwijk voorzieningen
- Locatie gegevens en programmatuur
- Additionele regels bij persoonsgegevens (bewerkersovereenkomst)
- Geheimhoudingsovereenkomst
- Encryptie, versleutelen van gegevens
- Onderaanneming en overdracht van rechten en plichten (of geen onderaanneming toestaan)
- Opschortingsrecht
- Naleving wet- en regelgeving
- Logging gegevens kunnen opvragen en inzien
- Het recht om audits te mogen (laten) uitvoeren over alle afspraken
- Welk recht van toepassing is
- Exit regels: wat als je de Cloud provider wilt verlaten, of de gegevens/diensten wilt migreren naar een andere provider? Hier wordt in de praktijk weinig over nagedacht
- Beheerafspraken, zie onder

Cloud en beheer van informatiesystemen

Beheerafspraken dienen in een Service Level Agreement (SLA) te worden vastgelegd dat onderdeel uitmaakt van het contract. Veel Cloud-leveranciers hanteren een standaard SLA omdat hun Cloud-dienst generiek is opgezet voor meerdere afnemers en het eenvoudiger (en goedkoper) is om hun eigen dienstverlening zo generiek mogelijk in te richten.

[3] Bij een escrow worden afspraken gemaakt om broncode of programmatuur bij een escrow agent te stallen zodat in het geval van een faillissement van de leverancier de eindgebruiker de beschikking krijgt over de broncode of software. Zie : http://nl.wikipedia.org/wiki/Broncode_escrow

Laat in dat geval de standaard leveranciers SLA beoordelen door een aantal mensen binnen de gemeente zoals een ICT-beheerder, het management en/of een informatiemanager. Neem geen genoegen met een standaard SLA als men meer wil, bedenk wel dat hier een prijskaartje aan kan hangen. Bij een aanbesteding dient hier in het programma van eisen al aandacht voor te zijn.

Alle beheerafspraken dienen in de SLA te staan.
Er moet een duidelijke hiërarchie zijn tussen het contract, een SLA en de bewerkersovereenkomst zodat duidelijk is welke eisen waar staan en wat de verhouding is tussen de documenten.
Accepteer niet dat voor afspraken of eisen wordt verwezen naar een website (die is veranderlijk).

Cloud en de IBD
De IBD heeft interesse in de zogenaamde 'gemeentelijke ICT-foto' om daarmee de dienstverlening optimaal af te stemmen op de gemeentelijke ICT-systemen die in gebruik zijn en de software die daarbij hoort. In het kader van de gemeentelijke foto is het raadzaam dat men ook doorgeeft dat systemen in een vorm van Cloud-diensten worden afgenomen, inclusief de leveranciersgegevens.

Risico's bij Cloud Computing
In dit document komen een aantal risico's voorbij die betrekking hebben op Cloud Computing, deze risico's zijn onder andere:

Verlies van besturing (governance).
De afnemer legt een deel van de besturing in handen van de leverancier, dit betreft ook informatiebeveiliging.

Leverancier lock-in.
Leveranciers hebben nog weinig te bieden aan tools, procedures of services om te kunnen migreren naar een andere Cloud-leverancier. Daarmee ontstaat het risico dat men, met een eenmaal gemaakte keuze, voor langere tijd vastzit aan die leverancier en dat het lastig wordt om Cloud-diensten te verhuizen.

Omgeving afschermingsfouten bij gedeelde omgevingen (isolation failure).
In de definitie van Cloud Computing staat onder andere dat meerdere afnemers kunnen werken met software die hetzelfde is waarbij de data wel geschieden wordt. Dit brengt het risico met zich mee dat de mechanismes falen die zorgen voor het scheiden van opslag, geheugen en routering tussen de verschillende afnemers.

Compliance risico's.
Het is lastig om bijvoorbeeld als afnemer, zelf een audit uit te (laten) voeren over een dienst die heel ergens anders wordt gehost of geleverd. Afgezien daarvan moet men ook kunnen vertrouwen op auditrapporten of -certificeringen die op verzoek kunnen worden aangeleverd. Men kan ook slecht controle uitoefenen of er wel binnen de kaders van bepaalde wetten wordt omgegaan met gegevens van de afnemer.

Gegevensbeveiliging.
Het beheer van de Cloud door de Cloud-aanbieder voegt een risico toe dat beheerders overal bij kunnen van alle Cloud-afnemers.

Gegevensbeveiliging verwachting.

De verwachting van de beveiliging van de Cloud-dienst van de afnemer kan verschillen met die van de Cloud-aanbieder Daarnaast kan de aanbieder in het kader van kosten reductie keuzes maken die de beveiliging doen afnemen die de afnemer niet zou willen.

Onveilige of onvolledige verwijdering van gegevens.
Als een gegeven in de Cloud verwijderd moet worden hoeft dat niet te resulteren in echte verwijdering, bijvoorbeeld doordat er data op andere plaatsen staat die vergeten wordt (back-up). Bovendien is het fysiek verwijderen van data door het vernietigen van het opslag medium vaak niet te doen omdat andere afnemers van Cloud-diensten ook gebruik maken van bijvoorbeeld een disk. Daarnaast heeft men geen controle over hergebruik van apparaatuur of herinzet van Cloud resources voor andere Cloud-afnemers.

Uitbreiding perimeter
Met het afnemen van Cloud-diensten wordt ook het eigen domein vergroot waar men verantwoordelijk voor is. Dus waar men standaard alleen hoefde te kijken naar het eigen fysieke pand of de panden wordt de beveiligingsfocus nu verlegd naar een grotere en moeilijker te controleren omgeving.

Beschikbaarheid en continuïteit.
Met het gebruiken van Cloud-diensten wordt Internet connectiviteit, (of een andere breedbandige verbinding), van de afnemer ineens een grotere afhankelijkheid.

4 Gemeentelijk Cloud Computing beleid

1. Het management is en blijft verantwoordelijk 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.
2. Uitbesteding is goedgekeurd door de voor het informatiesysteem verantwoordelijke lijnmanager.
3. De gemeenten blijft verantwoordelijk voor de betrouwbaarheid (beschikbaarheid, exclusiviteit en integriteit) van uitbestede diensten.
4. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheids eis 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.
5. 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.
6. Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen.
7. Er zijn continuïteitsplannen voor het herstel van incidenten, zoals aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.
8. Bij transport van vertrouwelijke informatie over onbetrouwbare netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe BIG hoofdstuk 12.3.1.3.
9. Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
10. Er worden afspraken gemaakt over de inhoud van rapportages, zoals over het melden van incidenten en autorisatiebeheer.
11. De in de bewerkersovereenkomst of dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld door audits of rapportages en gebeurt minimaal eens per jaar (voor ieder systeem).[4]
12. Er zijn voor beide partijen eenduidige aanspreekpunten.
13. In het geval van verwerken van persoonsgegevens is er een bewerkersovereenkomst waarin helder alle rechten en plichten van de leverancier en gemeente zijn vastgelegd. De vastgelegde beveiligingsmaatregelen worden jaarlijks door de gemeente geaudit bij de leverancier (zie ook 11).

Aldus vastgesteld door burgemeester en wethouders van *[gemeente]* op *[datum],*

[Naam. Functie] [Naam. Functie]

_____ _____

[4] Daarnaast kan men met de leverancier afspreken dat met een TPM kan worden voldaan aan de auditeis, echter dan moet deze wel dezelfde dekking hebben als de afspraken met de gemeente.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE BEVEILIGINGS DIENST

INFORMATIEBEVEILIGINGSDIENST
V00R GEMEENTEN (IBD)

NASSAULAAN 12
2514 JS DEN HAAG

POSTBUS 30435
2500 GK DEN HAAG

HELPDESK 070 373 80 11
ALGEMEEN 070 373 80 08
FAX 070 363 56 82

INFO@IBDGEMEENTEN.NL
WWW.IBDGEMEENTEN.NL