Beleidslijn informatieveiligheid en privacy

Cloud computing

(BLD CLOUD)

INHOUDSOPGAVE

1. Inleiding

Dit document maakt integraal deel uit van de methodologie informatieveiligheid en privacy binnen de sociale zekerheid. Dit document is bestemd voor de verantwoordelijken, voor de verwerkers van informatie, voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van de sociale zekerheid (OISZ).

Dit document legt de beleidslijnen informatieveiligheid en privacy vast als een organisatie een beroep wenst te doen op Cloud Computing-diensten. Hierbij ligt de klemtoon op de validatie dat de cloud service provider (CSP) voldoende waarborgen biedt op het vlak van de bescherming van de informatie, de naleving van de privacy en op de duurzame bewaring van de informatie en de juridische en technische bepalingen die in acht moeten worden genomen bij de realisatie van de prestaties. Dit laat de organisatie toe om de verwachte kwaliteit van de dienst in te schatten alvorens te beslissen.

In het kader van deze beleidslijnen wordt onder het begrip Cloud Computing alle cloud-diensten verstaan zoals universeel vastgelegd door het NIST[1]. Cloud Computing is een model waarbij op afroep op een eenvoudige manier via een netwerk toegang verkregen wordt tot een gedeelde verzameling van configureerbare informatiesystemen (zoals servers, opslagcapaciteit, toepassingen en diensten) die snel en flexibel worden geleverd en vrijgegeven met minimale inspanning of interactie met de cloud service provider.

Dit document is relevant omdat het afnemen van cloud-diensten gevolgen heeft voor de plaats waar informatieveiligheid- en privacy-maatregelen worden uitgevoerd. Als een organisatie van cloud-diensten gebruik maakt, dan blijft de organisatie altijd verantwoordelijk voor de veiligheid van de informatie en voor het waarborgen van de privacy.

2. Veilig gebruik van cloud computing

Elke organisatie onderschrijft de volgende beleidslijnen van informatieveiligheid en privacy voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie.

2.1. Algemene beleidslijnen informatieveiligheid en privacy

1. Alvorens een beroep te doen op cloud-diensten, moet de organisatie die verantwoordelijk is voor de verwerking duidelijk de informatie, de verwerkingen of de diensten identificeren die in de cloud worden geplaatst. Bij de bepaling van de keuze moet altijd rekening gehouden worden met de informatieveiligheid- en privacy-vereisten.
2. Wanneer de classificatie van de informatie dit vereist, moet de organisatie de minimale voorwaarden of de beperkingen bij de overmaking ervan vastleggen.
3. Informatieveiligheid heeft betrekking op alle gegevens en niet enkel op de persoonsgegevens[2]. Hiertoe moeten de gegevens geïnventariseerd en geclassificeerd worden volgens hun kriticiteit overeenkomstig het model voor classificatie van de gegevens dat binnen de organisatie geldt[3].
4. Het is noodzakelijk om het geschikte type cloud voor de beoogde verwerking te identificeren in functie van het huidige aanbod inzake cloud-diensten.
5. Het is essentieel om de eigen minimale vereisten te bepalen rond informatieveiligheid en privacy. De bedoeling van de cloud is om de organisatie van bepaalde operationele taken te ontlasten. Daarom moet de organisatie zich ervan vergewissen dat de cloud service provider minstens even hoge eisen stelt als zijzelf. Wat de gegevens en de

[1] National Institute of Standards & Technology : http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[2] Krachtens de definitie opgenomen in de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator

[3] De organisatie moet de gegevens voor de cloud klasseren in lijn is met de beleidslijnen data classificatie

verwerking betreft, moet de organisatie zich vergewissen van de omkeerbaarheid[4] en van een afdoend beschikbaarheidsniveau.

6. In functie van de scope van het cloud project, de kriticiteit van de activa (op het vlak van beschikbaarheid, integriteit en vertrouwelijkheid) en het verwachte model van cloud computing dient de organisatie altijd een formele risico-beoordeling te verrichten om op basis daarvan de gepaste informatieveiligheid- en privacy-maatregelen te eisen van de cloud service provider.

2.2. Minimale contractuele waarborgen voor de cloud service provider

Elke organisatie die professionele, vertrouwelijke of gevoelige gegevens wenst te verwerken in een cloud moet de volgende minimale contractuele waarborgen in acht nemen:

1. Clausule met betrekking tot de mogelijkheid voor een cloud service provider om een deel van zijn activiteiten uit te besteden naar andere (cloud service) partijen.
   a) De CSP is als enige verantwoordelijk ten opzichte van de organisatie voor de uitvoering van zijn verplichtingen, dus ook wanneer de CSP bepaalde van zijn taken op zijn beurt verder uitbesteedt.
   b) Bij uitbesteding van bepaalde specifieke taken aan onderaannemers, moet in de overeenkomst worden vastgelegd dat de CSP de organisatie altijd vooraf op de hoogte moet brengen. Bovendien moet de CSP zich formeel ertoe verbinden alle verplichtingen die hem zijn opgelegd, over te nemen in de verbintenissen die hij met de onderaannemers zal afsluiten.
   c) De CSP moet zich ervan vergewissen dat deze verbintenissen worden nageleefd door de onderaannemers. Hiertoe verricht hij de nodige controles. De uitvoeringsvoorwaarden van deze controles moeten in de overeenkomst worden vastgelegd.

2. Clausule met betrekking tot de integriteit, continuïteit en kwaliteit van de dienstverlening door de cloud service provider
   a) De CSP moet alle maatregelen treffen om de integriteit van de informatie die tijdens de duur van de overeenkomst worden verwerkt te garanderen (bijvoorbeeld back-up-systemen voorzien en testen).
   b) Een verbintenis met betrekking tot een service-niveau (SLA: Service Level Agreement) moet in een akkoord geformaliseerd worden dat wordt bijgevoegd bij de overeenkomst tussen de organisatie en de CSP. Daarin worden onder andere bepaald, inclusief voor de garantieperiode, de beschikbaarheid van de dienstverlening en de maximale opstarttijd na onderbreking te wijten aan een incident en alle andere criteria met betrekking tot het heropstarten van de activiteiten (RTO en RPO)[5].
   c) De gedetailleerde maatregelen die de continuïteit van de dienstverlening waarborgen moeten worden opgenomen in de SLA die wordt bijgevoegd bij de overeenkomst.

3. Clausule met betrekking tot de teruggave van de gegevens door de cloud service provider
   a) De CSP verbindt zich ertoe om de gegevens van de organisatie niet langer te bewaren dan voor de duur die met de organisatie werd afgesproken.
   b) Bij vroegtijdige verbreking of bij einde prestatie verbindt de CSP zich er toe om alle gegevens van de organisatie binnen de afgesproken termijn en op de afgesproken manier terug te geven in een gestructureerd en courant gebruikt formaat zodat de organisatie de continuïteit van haar dienstverlening kan garanderen. Na teruggave van de gegevens en mits het akkoord van de organisatie verbindt de CSP zich ertoe alle kopieën van gegevens in zijn bezit (inclusief back-ups en archief) op een veilige en professionele manier te vernietigen binnen een redelijke termijn. De CSP zal daarna direct het bewijs van de vernietiging leveren aan de organisatie.

[4] Definitie: de omkeerbaarheid is de mogelijkheid om terug te keren naar een vroegere leefbare situatie of organisatie. Hierdoor wordt een blokkerende situatie vermeden waarbij het niet mogelijk is om naar een vroegere situatie terug te keren of waarbij er een afhankelijkheid is ten opzichte van één enkele dienstverlener.

[5] RTO (Recovery Time Objective): Maximaal aanvaardbare duur van de onderbreking – RPO (Recovery Point Objective): Maximaal aanvaardbaar verlies van gegevens

4. Clausule met betrekking tot de overdraagbaarheid van de gegevens en de interoperabiliteit van de systemen
   a) Bij het einde van de prestatie verbindt de CSP zich ertoe om volgens de in de overeenkomst afgesproken voorwaarden de nodige hulp te bieden bij de migratie van de bewerkingen van zijn cloud naar een andere oplossing.

5. Clausule met betrekking tot de auditregeling
   a) De CSP verbindt zich ertoe om audits op initiatief van de organisatie toe te laten, om nauw samen te werken en om zo snel mogelijk de vastgestelde tekortkomingen te verhelpen. Deze audits kunnen door een erkende audit organisatie worden verricht.
   b) De CSP kan zelf ook audits en certificering laten uitvoeren door erkende audit organisaties en deze auditrapporten of -certificeringen op verzoek integraal en gratis ter beschikking stellen van de organisatie (zoals ISAE 3402, ISO27001, CSA). De organisatie kan dan nagaan of de scope en de resultaten voldoen aan haar vereisten.
   c) Bij volledige of gedeeltelijke uitbesteding legt de CSP aan alle onderaannemers clausules op waarbij het recht van de organisatie wordt gegarandeerd om audits uit te voeren mits naleving van de voormelde regels.

   Audits maken het mogelijk om na te gaan of de overeenkomst, de informatieveiligheid- en de privacy-regels worden nageleefd en of ze in overeenstemming zijn met de goede praktijken zoals aanbevolen door internationale instanties (zoals NIST, ENISA, ISO, CSA, ISACA, enz.). Audits moeten een organisatie toelaten om na te gaan of de informatieveiligheid- en privacy-maatregelen niet (kunnen) worden omzeild zonder dat de organisatie hiervan op de hoogte is.

6. Clausule met betrekking tot de verplichtingen van de cloud service provider inzake vertrouwelijkheid van de gegevens
   a) De CSP moet zich ertoe verbinden, voor de CSP zelf, de onderaannemers en eventuele overnemers, geen gegevens voor eigen rekening of die van een derde te gebruiken of te verspreiden.
   b) De CSP moet zich ertoe verbinden om alle toegangslogbestanden (die nodig zijn om te kunnen bepalen wie wat waar wanneer gedaan heeft) tot de gegevens, de toepassingen en systeeminstrumenten ter beschikking te houden van de organisatie gedurende de periode die in de overeenkomst is vastgelegd en deze professioneel te beveiligen.
   c) De CSP moet de organisatie onmiddellijk en volledig op de hoogte brengen van elke anomalie in de toegangslogbestanden zoals toegangspogingen door onbevoegde personen. Dit moet toelaten aan een organisatie om binnen de 72 uur te kunnen escaleren naar de privacy commissie indien een data breach[6] heeft plaatsgevonden.
   d) De CSP moet de organisatie onmiddellijk op de hoogte brengen van ieder onderzoek of aanvraag tot onderzoek afkomstig van een Belgische of buitenlandse administratieve of gerechtelijke overheid.

7. Clausule met betrekking tot de soevereiniteit
   a) De CSP moet aan de organisatie de waarborg bieden dat de CSP en eventuele onderaannemers niet onderworpen zijn aan onderzoeksdaden door overheden buiten België en de Europese Unie.

8. Clausule met betrekking tot de verplichtingen van de cloud service provider inzake informatieveiligheid
   a) De CSP moet de goede praktijken rond informatieveiligheid naleven, zoals de minimale veiligheidsnormen binnen de sector van de sociale zekerheid of standaarden zoals ISO 27017 cloud security[7], Cloud Security Alliance STAR[8].
   b) De CSP moet aan de organisatie het volledige informatieveiligheidsbeleid bezorgen met betrekking tot de diensten die de provider aanbiedt en de organisatie op de hoogte houden van de evolutie van dit beleid.
   c) De CSP moet jaarlijks de identiteit en de contactgegevens van de informatieveiligheidsverantwoordelijke (CISO) en van de functionaris voor gegevensbescherming (DPO) van de CSP meedelen aan de organisatie.

[6] https://www.privacycommission.be/nl/aangifte

[7] http://www.iso.org/iso/catalogue_detail?csnumber=43757 Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[8] https://cloudsecurityalliance.org/star/

d) De CSP moet de organisatie jaarlijks een formele evaluatie bezorgen over de toestand van de informatieveiligheid- en privacyvereisten (via de SLA afgesloten tussen de partijen).

2.3. Beleidslijnen informatieveiligheid voor de cloud service provider

Elke organisatie die professionele, vertrouwelijke of gevoelige gegevens wenst te verwerken in een cloud moet de volgende minimale contractuele waarborgen in acht nemen:

De goede praktijken die hieronder vermeld worden, vormen een minimale, niet exhaustieve lijst van informatieveiligheidsmaatregelen die de cloud service provider verplicht moet naleven. De uitgevoerde risico-beoordeling van de organisatie kan aanleiding geven tot bijkomende informatieveiligheidsmaatregelen. In functie van het cloud-model dient de verantwoordelijkheid voor het beheer van de informatieveiligheidsmaatregelen duidelijk vastgesteld te worden.

1. Vertrouwelijke gegevens beschermen:

De cloud service provider garandeert dat:

- de fysieke opslagplaats van de vertrouwelijke gegevens gekend is en voldoet aan de eisen van de organisatie (datacenter, servers, enz.,);
- de back-up- en herstel-systemen en het desbetreffende continuïteitsplan worden geïmplementeerd en periodiek worden uitgetest;
- het over een ethische gedragscode beschikt dat op zijn personeel en onderaannemers van toepassing is en door hen wordt toegepast. De provider oefent geen activiteiten uit die tot een belangenconflict kunnen leiden;
- de personeelsleden regelmatig bewust worden gemaakt van het belang van informatieveiligheid en privacy;
- het over tools beschikt waardoor inbreuken op bijzondere rechten of kwaadaardige activiteiten kunnen worden opgespoord;
- het over een incidentprocedure beschikt waarin zowel de opsporing, het escaleren, de verwerking tot en met de oplossing, de identificatie van de oorzaken en de communicatie aan de organisatie worden besproken.

2. Datacenter veiligheid

De cloud service provider garandeert dat

- er beveiligde systemen zijn van fysieke toegangscontrole, van inbraak-, brand- en overstromingsdetectie en van videobewaking;
- enkel de gemachtigde personen toegang krijgen tot een datacenter na een adequate goedkeuringsprocedure; bovendien worden de toegangen opgevolgd en regelmatig herzien;
- de vertrouwelijkheidsclausules die in een overeenkomst zijn vastgelegd ook van toepassing zijn op alle onderaannemer (in het bijzonder voor het onderhoud van de systemen waarin vertrouwelijke gegevens worden bewaard);
- elk opslagmedium met vertrouwelijke gegevens dat wordt hergebruikt, verwijderd of gerecycleerd moet eerst een doeltreffende procedure doorlopen.

3. Logische toegangsveiligheid

De cloud service provider garandeert dat

- het de toegangsmodaliteiten tot de gegevens toepast volgens de aanwijzingen meegedeeld door de organisatie (aanmaak, raadpleging, wijziging en verwijdering);
- de toegangen van de gebruikers en de administrators tot de systemen met vertrouwelijke gegevens gebaseerd zijn op mechanismen die de vertrouwelijkheid en de traceerbaarheid garanderen (zoals audit op de toegang tot de gegevens, problematiek van de generieke accounts);
- het een authenticatiebeleid toepast dat in overeenstemming is met dat van de organisatie.

4. Systeemveiligheid

De cloud service provider garandeert dat

- de back-upgegevens, ongeacht de drager waarop ze worden opgeslagen, vercijferd worden aan de hand van een gepast middel (algoritme, lengte van de sleutel, ...) afhankelijk van het gekozen cloud-model en in lijn met wat de organisatie nuttig acht;
- het de kwetsbaarheden van het systeem beheert en minstens jaarlijks veiligheidstesten organiseert; de kritische kwetsbaarheden worden daarbij onmiddellijk verbeterd;
- de servers waarop de vertrouwelijke gegevens worden beheerd, worden geconfigureerd met een zeer streng veiligheidsniveau;
- de veiligheidspatches op gecentraliseerde wijze beheerd worden, op voorhand uitgetest en geïnstalleerd worden binnen een redelijke termijn en in functie van hun kriticiteit;
- de veiligheidssoftware (zoals antivirus, antispam, antimalware, antiransomware) op de servers en de werkposten wordt geïnstalleerd en dat deze software regelmatig wordt bijgewerkt en bewaakt;
- het gebruik van USB-sleutels en andere mobiele opslagmedia wordt beheerd en gecontroleerd;
- de beheerprocedures en –praktijken inzake risicobeheer, incidentenbeheer en veranderingsbeheer worden toegepast en correct gedocumenteerd.

5. Netwerkveiligheid

De cloud service provider garandeert dat

- de toegangen tot het netwerk beperkt en beveiligd worden en dat ze worden gefilterd;
- het beheer van de systemen vanuit een beveiligd, afgezonderd en speciaal daartoe bestemd netwerk wordt verricht met gebruik van sterke authenticatie;
- de wijzigingen aan de netwerkuitrusting worden op voorhand goedgekeurd, opgevolgd en gedocumenteerd;
- in het geval van een gedeelde service van cloud computing:
  - de toegang tot het netwerk enkel wordt toegelaten voor vertrouwde terminals;
  - het netwerk met de systemen met vertrouwelijke gegevens afgezonderd zijn van het netwerk van andere organisaties.

2.4. Beleidslijnen privacy voor de cloud service provider

Alvorens cloud-diensten in te voeren, moet elke organisatie altijd op voorhand de risico's evalueren op het vlak van informatieveiligheid en privacy in de cloud oplossing. In functie van de gevoeligheid van de informatie zoals vastgelegd door de organisatie en de risico-beoordeling, zal de organisatie al dan niet een beroep kunnen doen op de diensten van een cloud service provider.

De volgende regels zijn van toepassing bij gebruik van de cloud-diensten waarbij persoonsgegevens worden verwerkt:

- In functie van haar activiteiten moet elke organisatie niet alleen de Belgische en Europese wetgeving naleven maar ook de specifieke wetgeving eigen aan een sector;
- De organisatie blijft altijd verantwoordelijk voor de naleving van de bescherming van de persoonsgegevens (europese privacy verordening[9]) bij de verwerking van dergelijke informatie in een cloud-dienst voor die informatie waarvan het eigenaar is;
- Er moet altijd een formele risico-beoordeling[10] uitgevoerd, gevalideerd, gecommuniceerd en onderhouden te worden om het juiste niveau van informatieveiligheid en privacy vast te stellen. De vastgestelde vereisten dienen bij de cloud service provider gegarandeerd worden;

[9] http://www.privacycommission.be/nl/privacywet-en-uitvoeringsbesluiten en http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[10] Risicobeoordelingsmodellen voor cloud computing vindt men bij ENISA https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment , bij ISACA http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Controls-and-Assurance-in-the-Cloud-Using-COBIT-5.aspx , bij NIST https://www.nist.gov/news-events/news/2012/01/nist-issues-cloud-computing-guidelines-managing-security-and-privacy en bij Smals https://www.smalsresearch.be/tools/cloud-security-model-nl/

- Behoudens een toegelaten afwijking, moet de organisatie in geval van uitbesteding van persoonsgegevens of gevoelige gegevens zich bij de keuze van de cloud service provider beperken tot cloud-diensten van het type “gemeenschappelijke cloud” of “private cloud”;
- Behoudens een toegelaten afwijking, is voor elke uitbesteding van persoonsgegevens of gevoelige gegevens altijd een vercijfering van informatie geschieden tijdens het transport (“in transit”) en de bewaring (“in rest”). De vercijferingsmiddelen moeten steeds onder controle van de organisatie worden beheerd en mogen niet worden uitbesteed.

Het verwerken van bijzondere[11] en medische gegevens dient te worden vermeden in de cloud als de cloud service provider toegang kan hebben tot deze informatie, omdat deze slechts zeer beperkt mogen worden verwerkt en zeer beperkt toegankelijk mogen zijn. De organisatie dient een bewuste keuze te maken omtrent het verwerken van bijzondere en medische gegevens in de cloud en vraagt altijd vooraf juridisch en technisch advies.

Een organisatie moet altijd vooraf een bewuste keuze maken of professionele, vertrouwelijke, gevoelige of persoonsgegevens in de cloud verwerkt kunnen worden. De organisatie is en blijft altijd de eindverantwoordelijke voor de informatie en voor de naleving van informatieveiligheid en privacy.

[11] Onder bijzondere persoonsgegevens zijn onder meer begrepen persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid en seksuele leven.

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2014		V2014	Eerste versie	19/03/2014	01/04/2014
2017		V2017	Integratie EU GDPR	07/03/2017	07/03/2017

Fouten en weglatingen

Wanneer bij het lezen van dit document fouten of problemen worden vastgesteld, dan wordt u als lezer verzocht om een korte beschrijving van de fout of het probleem en de locatie in het document samen uw contactinformatie door te geven aan de informatieveiligheidsconsulent (CISO) / functionaris van gegevensbescherming (DPO) van de organisatie.

Definities

Om consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten, worden alle definities met betrekking tot informatieveiligheid en privacy gecentraliseerd in één document genaamd “Definities informatieveiligheid en privacy”.

Bijlage B: Referenties

Hieronder staan documenten vermeld die hebben gediend als inspiratie voor dit document:

- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, september 2013, 23 blz.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, september 2013, 80 blz.
- EU, WG29, “Advies 05/2012 over cloud computing”, 1 juli 2012, 31 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.
- ISACA, “Security considerations for cloud computing”, September 2012, 80 blz.
- CNIL[12], « Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud Computing », juni 2012, 21 blz.
- Smals Research, « Cloud security evaluatiemodel », December 2014

Hieronder staan referenties naar websites die hebben gediend als inspiratie voor dit document:

- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- https://www.privacycommission.be/nl/cloud-computing
- http://www.isaca.org/cloud
- http://www.ccb.belgium.be/nl/work
- https://www.cybersimpel.be/nl
- https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
- https://www.sans.org/reading-room/whitepapers/cloud
- https://www.smalsresearch.be/tools/cloud-security-model-nl/

[12] Commission Nationale de l’Informatique et des libertés, http://www.cnil.fr

Bijlage C: Cloud computing uitgelegd

Inleiding

Bij cloud computing worden hardware, software en informatie beschikbaar gesteld via het internet. De medewerker 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 toelaat om flexibel te schalen naar de behoefte van de organisatie en de medewerkers. Bovendien is de organisatie vaak geen eigenaar meer van de hardware en/of de software. Het gaat om “virtuele infrastructuur en diensten”. Met cloud computing worden servers, desktops en ook toepassingen gevirtualiseerd met voordelen en nadelen.

Het is raadzaam om bij twijfel over de omgang met cloud computing en/of de verwerking van (persoons) gegevens in het buitenland altijd de juridische dienst te raadplegen. Alvorens gebruik te maken van cloud diensten dient een formele risico-beoordeling en business case gemaakt te worden met alle argumenten.

Bij het afnemen van cloud-diensten door de organisatie wordt geen enkele verantwoordelijkheid overgedragen naar de cloud service provider. De organisatie is en blijft altijd verantwoordelijk voor de manier waarop een cloud service provider omgaat met informatiebeveiliging. In het geval van persoonsgegevens is dit geregeld in de europese regelgeving EU GDPR.

Wat is het verschil tussen IT-uitbesteding en cloud computing?

Er is geen verschil wat betreft veiligheidsvereisten. IT-uitbesteding is een gekende methode waarbij een derde partij een of meerdere taken van de onderneming op zich neemt, taken waarvoor men vaak te weinig resources (tijd, expertise) heeft. Deze IT-uitbesteding kan gaan tot de opslag van informatie en verwerkingssystemen. Cloud Computing is een evolutie van IT-uitbesteding. In dat kader kan dit document ook in overweging genomen worden bij IT-uitbestedingen.

Kenmerken van cloud Computing

Cloud Computing wordt soms gelijkgesteld met Shared Service Centra maar er zijn enkele fundamentele verschillen. Cloud computing is enkel van toepassing als aan de volgende kenmerken voldaan is:

1. Zelfbediening (on-demand self-service): de afnemer van cloud diensten kan servertijd en opslag zonder tussenkomst van de cloud service provider wijzigen als dat nodig is.
2. Breedbandige toegang: er is toegang mogelijk via breedbandverbindingen met verschillende soorten cliënt platvormen (fat cliënt, thin cliënt, mobiele apparatuur enz.).
3. Gedeelde middelen (resource pooling): de fysieke en logische middelen van de cloud service provider worden door alle afnemers gebruikt en dynamisch toegewezen indien nodig. De afnemers gebruiken dezelfde toepassing instantie waarbij data wel per afnemer gescheiden wordt opgeslagen (multi tenancy model[13]). De afnemer heeft geen weet van de locatie waar de middelen zich bevinden. Voorbeelden van middelen zijn: opslag, rekenkracht, geheugen en netwerk bandbreedte.
4. 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.
5. Meetbare service: de cloud-systemen controleren en optimaliseren middelen door middel van toepasselijke metingen (opslag, geheugen, rekenkracht enz.). Het gebruik van middelen wordt transparant gemonitord, gecontroleerd en gerapporteerd aan de afnemer en de service provider van de gebruikte dienst.

Cloud computing modellen

Het huidige aanbod inzake cloud computing kan volgens drie basis service-modellen en vier basis implementatie-modellen worden ingedeeld.

- De basis service-modellen

[13] https://en.wikipedia.org/wiki/Multitenancy

- SaaS: « Software as a Service » bij SaaS worden toepassingen via de cloud aangeboden aan eindgebruikers. Er zijn organisaties die toepassingen nu al via een SaaS-model afnemen en dat gebeurt in publieke en private clouds. Vaak worden hier web-applicaties aangeboden die met moderne technologieën gemaakt zijn. Voor de eindgebruiker is volledig onduidelijk waar de toepassing zich bevindt, op welk platform de toepassing draait en waar de informatie zich bevindt.
- PaaS: « Platform as a Service », als de organisatie zelf software wil installeren in een cloud, dan kan gebruik gemaakt worden van PaaS. Bij PaaS kan een organisatie 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 toepassingen geplaatst voor de eindgebruiker.
- IaaS: « Infrastructure as a Service », een organisatie kan alleen de (gevirtualiseerde) infrastructuur afnemen. Hier vindt men servers, netwerk componenten, opslagcapaciteit en andere infrastructuur. Dit geeft de ICT-afdeling van een organisatie de volledige vrijheid over de hardware die virtueel wordt afgenomen, bovenop de IaaS hardware kan de ICT-afdeling van de organisatie weer platform services draaien en daar bovenop weer eigen software. Beheer kan op afstand worden gedaan vanaf iedere werkplek.

- De basis implementatie-modellen:
  - «Publiek»: de infrastructuur is toegankelijk voor een breed publiek en is volledig eigendom van een cloud service provider (CSP) , in dit geval wordt een dienst met veel klanten gedeeld;
  - «Privaat»: de cloud-infrastructuur werkt voor één enkele organisatie, ze kan door de organisatie zelf (interne private cloud) of door een derde worden beheerd (externe private cloud). In een private cloud heeft de organisatie de volledige controle over informatie, veiligheid en kwaliteit van de dienst. Vaak ligt de verantwoordelijkheid voor onderhoud en beheer bij de organisatie 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;
  - «Gemeenschappelijk/Community»: Het betreft een cloud-infrastructuur die gebruikt wordt door een specifieke groep afnemers die een gemeenschappelijk belang hebben of aan dezelfde (wettelijke) eisen moeten voldoen. Denk hierbij aan taak, missie, veiligheidsvereisten, beleid en naleving vereisten. De gemeenschappelijke 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 overheidscloud of een Organisatie-Cloud. Zoals voor de private cloud kan deze infrastructuur door de organisaties zelf of door een derde worden beheerd;
  - «Hybride»: Deze infrastructuur bestaat uit minstens twee cloud types (privaat, gemeenschappelijk of publiek) die apart blijven bestaan maar die met elkaar zijn verbonden door een standaard of eigen technologie waardoor de overdraagbaarheid van de informatie of van de toepassingen wordt gegarandeerd. Met andere woorden er worden cloud-diensten afgenomen van een derde aanbieder terwijl men daarbij ook gebruik maakt van een eigen cloud.

Als een private cloud niet in een datacentrum van de organisatie 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 vereisten in dit document van toepassing.

Voorbereiding bij migratie van een interne infrastructuur naar een Cloud Computing-infrastructuur

- Een rentabiliteitsanalyse voorbereiden en de kosten en baten met betrekking tot een migratie naar een leverancier van Cloud Computing evalueren.
- De middelen (informatie, toepassingen, processen) in het toepassingsgebied van Cloud Computing identificeren en classificeren.
- De sleutelfiguren van de organisatie (wettelijk, veiligheid, financieel, etc.) betrekken bij het beslissingsproces van de migratie naar een Cloud Computing-service alvorens een beslissing te nemen.
- Het design en de vereisten van de oplossing die voorgesteld werd door de kandidaat voor de transfer naar Cloud Computing grondig bestuderen. Ook vragen dat de leverancier van de Cloud Computing-service voor een testperiode zorgt, zodat mogelijke problemen opgespoord kunnen worden.

Contracten en de Cloud

In contracten met een cloud service provider dient aandacht te zijn voor de volgende zaken:

- Specifieke veiligheidsmaatregelen afkomstig uit een risico-beoordeling
- Het verplicht direct melden van veiligheids- en privacy-incidenten aan de organisatie
- Looptijd van het contract

- Beschrijving van basispakket en aanvullende (optionele) diensten en de daarvoor gehanteerde tarieven
- Een escrow regeling (of cloud escrow regeling)
- 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 (verwerkersovereenkomst)
- 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 de organisatie de cloud service provider wilt verlaten, of de gegevens/diensten wenst te migreren naar een andere cloud service provider?
- Beheerafspraken

Bijlage D: Cloud computing voordelen, nadelen en risico's

Voordelen van Cloud Computing.

- 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. De organisatie kan eenvoudig groeien en krimpen al naar gelang de behoefte, en dat in korte tijdsspannen.
- Er zijn flexibele berekeningsmechanismes: betalen per gebruiker, betalen per virtuele machine of dienst.
- Een hogere beschikbaarheid lijkt logisch, hoewel dit afhankelijk is van het service niveau van de cloud service provider.
- De cloud service provider (CSP) heeft vaak de beschikking over voldoende gespecialiseerd personeel, waardoor een organisatie zelf minder experten nodig heeft. Met gebruik van cloud computing worden dus niet alleen informatie op afstand gezet, maar ook de complexiteit van de systemen.

Nadelen en risico's van Cloud Computing.

De overgang van interne IT naar Cloud Computing vereist een duidelijke en transparante aanpak op het vlak van het beheer van de veiligheid, contractuele en juridische risico's. De organisatie die een beroep wenst te doen op een CSP moet steeds een risico-beoordeling uitvoeren om na te gaan of die CSP de geschikte organisatorische, technische, procedurele en communicatieve informatieveiligheid- en privacymaatregelen toepast in de praktijk. De organisatie moet tijdens deze risico-beoordeling in het bijzonder nagaan hoe groot de risico's zijn omtrent de bescherming van persoonsgegevens (privacy) rekening houdende met de nieuwe Europese privacy normen (EU GDPR)[14]. De belangrijkste risico's die op dat vlak werden geïdentificeerd, zijn de volgende:

- een verminderde governance met betrekking tot de verwerking;
- de risico's verbonden aan de onderaannemers van de CSP, bijvoorbeeld een fout in de onderaannemingsketen wanneer de leverancier zelf een beroep doet op derden om een dienst te leveren;

[14] EU GDPR http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

- de technische afhankelijkheid ten opzichte van de CSP, bijvoorbeeld het risico dat er informatie verloren gaan bij migratie naar een andere CSP of naar een interne oplossing;
- een gegevenslek, met andere woorden het risico dat informatie die op een (virtueel) systeem zijn gehost, gewijzigd kunnen worden of toegankelijk zijn voor niet-gemachtigde derden naar aanleiding van een tekortkoming of een slecht beheer van de CSP;
- de uitvoering van juridische vorderingen op basis van een buitenlands recht zonder overleg met de nationale instanties;
- bij externe clouds is niet te controleren in hoeverre de CSP inzage heeft in diensten en informatie
- het niet-naleven van de regels die door de organisatie werden uitgevaardigd met betrekking tot de bewaring en de vernietiging van informatie, o.a. bij een ondoeltreffende of onbeveiligde vernietiging van de gegevens of een te lange bewaarduur;
- problemen bij het beheren van de veiligheid en van toegangsrechten inherent aan de directe benaderbaarheid via het internet;
- de onbeschikbaarheid van de dienst geleverd door de CSP;
- de stopzetting van de dienst door de CSP (bv. als gevolg van een gerechtelijke beslissing of de overname van de CSP door een derde of bij een faillissement);
- de niet-overeenstemming met de regelgeving, in het bijzonder met betrekking tot internationale transfers.

Een uitgebreidere lijst van risico's en risicomodellen rond cloud computing[15] kunnen mee in overweging worden genomen bij de uitvoering van de risico-beoordeling van zodra de organisatie een mogelijke overstap naar cloud computing overweegt.

Bijlage E: Link met de ISO-norm 27002:2013

Hier wijzen we op de voornaamste clausule(s) van de ISO-norm 27002:2013 die verband houden met het onderwerp van het huidige document.

ISO-norm 27002:2013	
Veiligheidsbeleid	
Organisatie van de informatieveiligheid.	
Veilig personeel	
Beheer van bedrijfsmiddelen	
Toegangsbeveiliging	
Cryptografie	**Ja**
Fysieke beveiliging en beveiliging van de omgeving	
Beveiliging processen	
Communicatieveiligheid	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	**Ja**
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	

***** EINDE VAN DIT DOCUMENT *****

[15] Risicobeoordelingsmodellen voor cloud computing vindt men bij ENISA https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment , bij ISACA http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Controls-and-Assurance-in-the-Cloud-Using-COBIT-5.aspx , bij NIST https://www.nist.gov/news-events/news/2012/01/nist-issues-cloud-computing-guidelines-managing-security-and-privacy en bij Smals https://www.smalsresearch.be/tools/cloud-security-model-nl/