PRIVACY EN CLOUD

Knelpunten:

- Wat is cloud?
- Soorten clouddiensten en de verschillen
- Wie is de verantwoordelijke?
- Wie heeft de beveiligingsverplichting?
- Is een bewerkersovereenkomst nodig?
- Waar staan de gegevens:
    - Worden de gegevens in de cloud aan een derde verstrekt?
    - Worden de gegevens doorgegeven naar een land buiten Europa?

Aanbevelingen & Aandachtspunten:

Wat is cloud

- Cloud betekent natuurlijk gewoon “wolk” in het Engels. Deze naam omschrijft ongeveer wat cloud computing is: losse onderdeeltjes die met elkaar in verbinding zijn, maar telkens een andere vorm kunnen aannemen.
- Cloud computing is een dienst, in tegenstelling tot een product. Bij cloud computing wordt dus niets tastbaars (zoals een server of hardware) geleverd, maar wordt een dienst geleverd.
- Bij cloud computing wordt een dienst aangeboden door een zogenoemde Cloud Service Provider (cloud dienstverlener) die mogelijk maakt dat je via een (internet)verbinding een programma kan gebruiken. Kenmerkend voor cloud is dat sprake is van gedeelde resources (rekencapaciteit, opslag, geheugen, servers, netwerk, besturingssystemen) en dat de mogelijkheid bestaat om zelf het gebruik te starten en dat sprake is van toegankelijkheid vanaf elke gewenste locatie.

Soorten clouddiensten en de verschillen

- Cloud computing kent een aantal soorten:
    - Software as a service (Saas), waarbij applicatiefunctionaliteiten via internet worden aangeboden. De gebruiker heeft geen controle over het applicatieplatform, de software of de onderliggende ict.
    - Platform as a service (Paas), waarbij een applicatieplatform en/of besturingssysteem via internet wordt aangeboden. De gebruiker kan eigen toepassingen plaatsen of ontwikkelen. Ook is er geen controle over de onderliggende ict.
    - Infrastructure as a service (Iaas), waarbij ict-onderdelen via internet worden aangeboden, zoals rekencapaciteit, netwerk of dataopslag.
- Voorbeelden van cloud computing diensten: Google Docs, Microsoft Office 365, Gmail, hotmail, Yahoo mail, Amazon Simple Queue, Amazon Simple, Verizon Caas, Keynote systems, Dropbox.
- De wijze waarop cloud computing wordt aangeboden, kent ook varianten:
    - Private cloud
      de infrastructuur wordt slechts door 1 organisatie gebruikt. Hosting kan intern of extern.

- Community cloud
  Is ter ondersteuning van een groep businesspartners die samen werken aan één project of product. Een van de partners beheert de cloud of een externe partij doet dit.
- Public cloud
  Is een cloud infrastructuur voor het grote publiek. De gebruikers zijn geen eigenaar van de middelen, want dat is de cloudleverancier.
- Hybrid cloud
  Is een combinatie van de andere varianten, modellen. De afzonderlijke varianten zijn met elkaar verbonden zodat de gegevens en applicaties van de verschillende modellen samen kunnen worden gebruikt.

Verantwoordelijke

- De verantwoordelijke in de zin van de Wbp is degene die het doel en de middelen van de verwerking bepaalt. Dit hebben we kunnen lezen bij *#1 Privacywetgeving en uw organisatie*.
- U heeft als organisatie besloten om bepaalde persoonsgegevens te verzamelen, op te slaan, te bewaren en te gebruiken. Nu besluit u om hiervoor een cloud oplossing te gebruiken. In het geval van een Saas, Paas of Iaas oplossing is de gebruiker van deze oplossing de verantwoordelijke.
- Het is mogelijk dat de Cloud Service Provider ook als verantwoordelijke kwalificeert, maar dan hooguit als mede-verantwoordelijke. Niet als enige verantwoordelijke.
- Kortom, kiest een organisatie voor een cloud oplossing dan is die organisatie (nog steeds) verantwoordelijke in de zin van de Wbp.
- Kortom, ook bij het gebruik van cloud diensten gelden alle verplichtingen uit de Wbp. Denk aan: beveiliging, afsluiten van een bewerkersovereenkomst, verstrekking aan derde (anders dan een bewerker) is niet zomaar mogelijk, doorgifte buiten Europa is niet altijd toegestaan en de betrokkene moet zijn rechten kunnen uitoefenen.
- De organisatie die kiest voor een cloud dienst zal daarnaast ook rekening moeten houden met de knelpunten die in het algemeen bij ict-contracten spelen, zoals:
  - Beschikbaarheid van data;
  - Continuiteït van de dienstverlening waarbij de data wordt gebruikt;
  - Dataportabiliteit;
  - Service level afspraken: updates, downtime, hulp bij storing
  - Rechten van intellectuele eigendom;
  - Escrow;
  - Afhankelijkheid van de leverancier voor andere (aanvullende) diensten;
  - Mogelijkheid om zonder problemen van leverancier te wisselen;
  - Toepasselijk recht en forumkeuze.
- Een overeenkomst over cloudcomputing, het afnemen van een cloud dienst, is niks anders dan het sluiten van een ICT-overeenkomst. Bij ICT-overeenkomsten wordt vaak uitgebreid onderhandeld, maar bij cloudoplossingen wordt dit vergeten, omdat via internet de dienst snel en gemakelijk kan worden afgenomen en programma's kunnen worden geïnstalleerd.
- Beschouw het afnemen van een cloud dienst als het aangaan van een ICT-overeenkomst-plus. De plus zijn in dit geval de privacy aspecten. De keuze voor bijvoorbeeld een private cloud oplossing kan al veel privacy problemen voorkomen.

- Het kan voorkomen dat er geen echte onderhandelingsmogelijkheid is. Bijvoorbeeld omdat bepaalde overeenkomsten voor akkoord moeten worden aangeklikt. Cloud Service Providers die zo werken, hebben echter wel uitgebreide privacy policies en andere verklaringen en voorwaarden. Zorg dat deze zijn gelezen en begrepen. Maak vooral ook gebruik van het instellen van privacy settings. Wordt het te ingewikkeld en onoverzichtelijk, neem dan de dienst af bij een andere Cloud Service Provider die wél rekening houdt met de privacy eisen haar klanten.
- Vergeet bij het gebruik van clouddiensten ook niet, dat er een keuze bestaat bij het invoeren van gegevens. Zo bestaan er systemen die standaard een invulveld hebben bij klantgegevens waarin het BSN nummer kan worden ingevuld. Dit betekent niet dat je als gebruiker dit móet doen bij al je klanten. Sterker nog, deze manier van verwerken van een BSN nummer is waarschijnlijk in strijd met de Wbp.

<u>Beveiligingsverplichting</u>

- De verantwoordelijke heeft een beveiligingsverplichting volgens de Wbp. Dat is bij een cloudoplossing dus in ieder geval de gebruiker, maar kan ook de Cloud Service Provider zijn.
- De beveiligingsverplichting van de gebruiker van een clouddienst geldt ten opzichte van de personen van wie de gegevens worden gebruikt. De verplichting geldt dus van de organisatie jegens haar klanten, afnemers, patiënten, leden, personeel. Die verplichting blijft bestaan zodra de organisatie kiest voor het plaatsen van de administratie, dossiers of relatiesysteem in de cloud. Die verplichting gaat niet over op de clouddienstverlener, de organisatie zelf blijft aansprakelijk. Hooguit heeft de clouddienstverlener (ook) een beveiligingsverplichting naar de organisatie of naar degene van wie de gegevens in de cloud worden geplaatst.
- Kortom, over de beveiliging moeten duidelijke afspraken worden gemaakt met de clouddienst verlener. Afspraken in de vorm van keiharde garanties en vrijwaring.
- Afspraken over beveiliging met de clouddienstverlener zijn belangrijk, omdat vanaf 1 januari 2016 hoge boetes kunnen worden opgelegd voor onder andere het niet (goed) beveiligen van een gegevensverwerking (bijvoorbeeld een administratie). Een boete kan ook worden opgelegd voor het niet (juist of volledig of tijdig) melden van een datalek.
- De beveiligingsafspraken met een Cloud Service Provider bevatten daarom tenminste de volgende onderwerpen:
    - Inzicht in de getroffen en te treffen beveiligingsmaatregelen tegen onrechtmatige toegang tot de cloud, tot de gegevens en tegen verlies, tenietgaan of onrechtmatige bewerking van de gegevens;
    - Het maken van back ups;
    - Het gebruik van encryptietechnieken;
    - Audit bevoegdheid voor gebruiker of een andere manier waarop de beveiliging(smaatregelen) kunnen worden gecontroleerd. Wellicht is sprake van certificering en kan dit jaarlijks worden aangetoond;
    - Per direct volledige informatie over een datalek;
    - Volledige hulp en ondersteuning bij het in kaart brengen van een datalek;
    - Een toegankelijk incidentenregister inzake datalekken bij de Cloud Service Provider;
    - Aansprakelijkheid (vrijwaring) bij datalekken.

- Bij de gebruiker van een cloudoplossing – uw eigen organisatie - moeten natuurlijk ook (organisatorische) beveiligingsmaatregelen worden getroffen. Denk aan: gebruik van wachtwoorden, thuiswerk protocollen, bescherming van wachtwoorden, toekennen van toegangsrechten, up to date houden van toegangsrechten, tijdig installeren van updates van computerprogramma's en de implementatie van een draaiboek datalekken.
- Ook hier geldt weer, indien het niet mogelijk is om concreet te onderhandelen: stel dan in ieder geval de privacy settings zo in zodat wordt voldaan aan de eisen van de Wbp. Bij twijfel of onduidelijkheid, kies een andere Cloud Services Provider. Tegenwoordig is privacy ook een marketingtool voor cloudaanbieders. Er is er vast een te vinden die wél rekening houdt met de privacyvoorwaarden van de gebruiker. Een private cloudoplossing zou al uitkomst kunnen bieden.

Bewerkersovereenkomst

- Als de afnemer van een clouddienst kwalificeert als verantwoordelijke, dan is de Cloud Service Provider de bewerker. Soms is de cloudaanbieder ook (mede)verantwoordelijke.
- In ieder geval zal er een bewerkersovereenkomst gesloten moeten worden.
- Dit kan als onderdeel van een Service Level Agreement.
- In de bewerkersovereenkomst zullen tenminste de beveiligingsafspraken zoals hiervoor vermeld afgesproken moeten worden.
- Clouddiensten kunnen worden aangeboden via meerdere Cloud Service Providers of een cloudaanbieder kan voor zijn dienstverlening gebruik maken van derden die ook een stukje dienstverlening verzorgen.
- Kortom, wees erop bedacht dat sprake kan zijn van sub-bewerkers. De verantwoordelijke – gebruiker van de clouddienst – is aansprakelijk voor de gehele keten van bewerkers. Maak hier dus afspraken over, zorg dat dit onderwerp inzichtelijk is.
- Neem ook de verplichting op dat het systeem zo werkt dat indien een betrokkene zijn wettelijke bevoegdheden uitoefent (o.a. inzage, verwijdering) dit te allen tijde direct kan worden uitgevoerd.
- Zorg voor duidelijke continuïteitsafspraken. Wat gebeurt er als de clouddienstverlener failliet gaat? Zijn de data dan nog toegankelijk? En in welke vorm? Worden er dan nog backups gemaakt? En hoe zijn de backups toegankelijk/beschikbaar? Hoe wordt dataportabiliteit geregeld? Hoe gaat een overstap naar een andere clouddienstverlener in zijn werk? En hoe worden de bewaartermijnen nagekomen? Worden de gegevens vernietigd?

Waar zijn de gegevens?

Bij een derde

- Een van de voordelen van een cloudoplossing, geen vaste server waar alle data wordt opgeslagen, is gelijk ook het grootste nadeel. Volgens privacywetgeving moet je nu juist wél weten waar de data wordt opgeslagen.
- Bij de "Bewerkersovereenkomst" is dit onderwerp al aangestipt. Een cloudoplossing van een Cloud Service Provider staat vaak niet op zichzelf. Het is goed mogelijk, en gebruikelijk, dat producten of diensten van andere partijen worden aangeboden of gebruikt bij het aanbieden van een clouddienst.
- Deze derde partijen zijn geen directe contractspartijen van de gebruiker van een clouddienst, dat is alleen de Cloud Service Provider. Deze derde partijen kunnen echter wel inzicht hebben of

toegang hebben tot de gegevens die door de gebruiker van de clouddienst in de cloud worden gezet. Kortom, zorg dat voor het sluiten van een clouddienst de hele keten van betrokken partijen inzichtelijk is.

- Als verantwoordelijke, gebruiker van de clouddienst, mag je niet zomaar persoonsgegevens aan derde verstrekken. De partijen die via de cloudaanbieder ook bij de gegevens kunnen, zijn derden. Zorg dus zodra in beeld is gebracht wie er mogelijk bij de gegevens kunnen (al is het maar voor een helpdeskfunctie), dat dit in de informatieverstrekking naar de betrokkene (klanten, patiënten, leden, deelnemers, sponsors) tot uitdrukking komt. Dit kan via het privacystatement.
- Ook ten aanzien van deze derde moet worden nagedacht over continuïteitsafspraken. Hoe groot is de rol van deze derde? Hoe afhankelijk is een organisatie bij gebruik van de cloudoplossing van deze derde? Kortom, maak ook hier afspraken over.

<u>en dan ook nog buiten Europa?</u>

- Zodra data buiten Europa wordt opgeslagen of raadpleegbaar is, gelden strenge privacy regels. Het aspect raadpleegbaar of toegankelijk wordt vaak over het hoofd gezien. Indien er een helpdesk vanuit India werkt, backups worden gedraaid in Korea of monitoring plaatsvindt vanuit de Verenigde Staten dan wordt juridisch gezien de data verstrekt aan een land buiten Europa.
- Verstrekken van data buiten Europa (doorgifte) is verboden, tenzij sprake is van een passend beschermingsniveau in deze landen of sprake is van een uitzonderingssituatie (zoals ondubbelzinnige toestemming) of indien een vergunning is verkregen of indien wordt gewerkt met Standard Contract Clauses van de Europese Commissie. Van de Safe Harbor route met de Verenigde Staten kan vooralsnog geen gebruik meer worden gemaakt.
- Bij cloud computing is de locatie van de data (naast beveiliging) het meest onoverzichtelijke punt. Om te voorkomen dat data hoe dan ook buiten Europa terecht komt, kan gekozen worden voor Europese Cloudoplossingen. Er is dan nog steeds sprake van cloud, maar de data blijft binnen Europa. Door diverse cloud aanbieders wordt handig ingespeeld op de situatie die is ontstaan na de afschaffing van de Safe Harbor route.