PRIVACY WET (WBP) EN DE CLOUD

Auteur: Wiebe Zijlstra (16 January 2015)

Steeds meer organisaties maken voor een deel van hun informatieverwerking gebruik van de cloud, soms ter vervanging van hun eigen servers en opslag, soms door gebruik van SaaS-software. Vrijwel altijd zijn hierbij ook persoonsgegevens betrokken. Daarom is het goed de juridische aspecten hiervan te kennen.

Hieronder volgt eerst een opsomming van juridische aspecten die van belang zijn bij de keuze om al dan niet 'in de cloud' te gaan. De meeste zijn een gevolg van de eisen die worden gesteld door de Wet bescherming persoonsgegevens (Wbp). Verderop in dit artikel werken we een aantal van deze aspecten verder uit.

Juridische aspecten van de cloud

We gaan uit van de veelvoorkomende situatie dat een leverancier een softwareprogramma ter beschikking stelt aan een klant. Deze klant gaat zelf werken met de toepassing (bijvoorbeeld een boekhoudprogramma) of stelt deze ter beschikking aan eindgebruikers (zoals bij een webwinkel).

- Bewerkersovereenkomst
  Een leverancier van clouddiensten zal vaak persoonsgegevens van de klant verwerken of heeft toegang tot deze persoonsgegevens als hij beheeractiviteiten uitvoert. Op grond van de Wbp moet de klant met de leverancier schriftelijk afspraken maken over bijvoorbeeld aspecten als beveiliging en geheimhouding.
- Beveiliging
  De leverancier moet de persoonsgegevens van zijn klant voldoende beveiligen. De beveiligingsmaatregelen moeten schriftelijk worden vastgelegd in de bewerkersovereenkomst. Daarnaast moet de klant controleren of de leverancier zijn verplichtingen nakomt. Deze controle kan eventueel door een onafhankelijke derde partij gebeuren.
- Doorgifte naar buitenland
  Aan het plaatsen van persoonsgegevens op servers buiten de Europese Unie worden strenge eisen gesteld. De klant zal bij de leverancier moeten informeren naar de locatie van zijn gegevens om zodoende de juiste maatregelen te kunnen (laten) treffen. Eventueel zal hij voor een andere leverancier moeten kiezen, die uitsluitend gebruikmaakt van servers binnen de Europese Unie of in een land met een 'passend beschermingsniveau'. Ook wanneer de persoonsgegevens op een EU-server staan die toegankelijk is voor een helpdesk in bijvoorbeeld India, is er eveneens sprake van doorgifte naar het buitenland, die bijzondere maatregelen vergt.
- Exit-strategie
  De leverancier mag persoonsgegevens niet langer bewaren dan voor de dienstverlening

nodig is. Na beëindiging van het cloudcontract moet de leverancier de gegevens van zijn servers verwijderen. Ook moet geregeld worden, dat er op een nette manier overdracht van gegevens plaatsvindt, bij beëindiging van het contract. Vergeet hierbij niet de situatie, dat de leverancier failliet gaat.

- Meldplicht datalekken
  De leverancier moet de klant onmiddellijk op de hoogte stellen als beveiligingsincidenten plaatsvinden. De klant blijft vervolgens verantwoordelijk voor een tijdige melding bij de autoriteiten en kan zich niet verschuilen achter het excuus dat de cloudleverancier hem niets heeft verteld.
- Buitenlandse wetgeving: export control laws
  Door gebruik te maken van de diensten van een Amerikaanse cloudleverancier kan een Nederlandse onderneming ongemerkt de strenge Amerikaanse exportregels overtreden en hoge boetes riskeren. De Amerikaanse exportregels zijn over het algemeen strenger dan de Europese. Een bedrijf dat in overeenstemming met de Europese regels handel drijft met een land dat op de Amerikaanse embargolijst staat en besluit gebruik te gaan maken van Office 365 of GoogleDocs loopt hier risico!
- Buitenlandse wetgeving: state control powers
  In sommige landen heeft de overheid de wettelijke bevoegdheid om van providers toegang tot de servers te eisen. In deze context zijn vooral de US Patriot Act en de FISA/FISAA berucht. Ook andere landen kennen dergelijke bevoegdheden.

Cloudcontracten en de bescherming van persoonsgegevens

De reden dat privacyregelgeving bij clouddiensten een rol speelt, is dus gelegen in het feit dat de leverancier van een clouddienst vaak persoonsgegevens van zijn klanten verwerkt. Zo zet bijvoorbeeld een bedrijf dat gebruikmaakt van Office 365, zijn data niet meer op de harde schijf van zijn computer(s), maar rechtstreeks bij Microsoft op de server. Hiermee krijgt Microsoft direct of indirect toegang tot die data. Deze data kunnen bedrijfsgegevens bevatten, maar ook persoonsgegevens. Als persoonsgegevens onderdeel uitmaken van deze data, speelt in veel gevallen de Wet bescherming persoonsgegevens een rol. Hetzelfde geldt voor diensten als: webhosting, pure opslagruimte (SkyDrive, Dropbox), fotobewerking en -opslag (Picasa), kantoorapplicaties, boekhoudprogramma's en natuurlijk de diverse sociale media, zoals Facebook en LinkedIn. Expliciet moet de klant altijd aangeven, dat hij akkoord gaat met de voorwaarden van de leverancier, maar de meeste mensen klikken blind het hiervoor benodigde vinkje aan.
In de volgende paragrafen werken we een aantal eisen en aspecten die hierbij mogelijk een rol spelen verder uit.

Schriftelijke overeenkomst cloud computing

De leverancier van een clouddienst heeft dus vaak toegang tot de data die zijn afnemers op zijn server hebben opgeslagen. Bevatten deze data persoonsgegevens, dan geldt de leverancier als bewerker van deze persoonsgegevens.
Wanneer er sprake is van 'bewerking' is de afnemer van de clouddienst verplicht om met de leverancier een zogenoemde bewerkersovereenkomst te sluiten. De bewerkersovereenkomst is ter bescherming van de privacy van de eindgebruiker. In deze overeenkomst verplicht de leverancier zich zorgvuldig met de persoonsgegevens om te gaan. Onderwerpen die in deze overeenkomst aan de orde komen zijn onder andere: beveiliging van de data, geheimhouding, het inschakelen van derden en de locatie van de servers.

De privacywetgeving stelt hoge eisen aan de doorgifte van persoonsgegevens naar landen buiten de Europese Unie. Het plaatsen van persoonsgegevens op een server in een datacentrum buiten de Europese Unie geldt als zo'n doorgifte.
De afnemer van de clouddienst zal dan ook bij de leverancier moeten informeren naar de locatie van zijn gegevens om zodoende de juiste maatregelen te (laten) treffen. Wanneer niet aan alle wettelijk eisen is voldaan, is de feitelijke consequentie dat er een andere leverancier of een ander product moet worden gekozen.

Scenario's in locatie en export van data

Bij de opslag van de data (met persoonsgegevens) kunnen de volgende situaties zich voordoen:

- Datacentrum in de Europese Economische Ruimte
  De Europese Economische Ruimte bestaat uit de landen van de Europese Unie en Liechtenstein, Noorwegen en IJsland. Staat het datacentrum in een van deze landen, dan zijn geen bijzondere maatregelen nodig.
- Datacentrum in een land van de witte lijst
  Staat het datacentrum in een van deze landen, dan zijn geen bijzondere maatregelen nodig. De witte lijst is een lijst van landen die volgens de Europese Commissie een passend beschermingsniveau hebben. Dit zijn:
  - Andorra
  - Argentinië
  - Australië
  - Canada (Canadian Personal Information Protection and Electronic Documents Act)
  - Faroer Eilanden
  - Guernsey,
  - Isle of Man,
  - Israel
  - Jersey
  - Uruguay
  - Verenigde Staten
  - Zwitserland
- Datacentrum in de Verenigde Staten
  Hoewel de VS op de witte lijst staan, is het een apart geval. Een passend beschermingsniveau wordt uitsluitend geboden door bedrijven en organisaties in de VS die zijn aangesloten bij Safe Harbor.
- Datacentrum in ander land
  Staat het datacentrum in een ander land dan de hierboven genoemde, dan is de klant in de meeste gevallen verplicht met de cloudleverancier een EU Model Contract te sluiten.

Wanneer de persoonsgegevens op een EU-server staan die toegankelijk is voor een helpdesk in bijvoorbeeld India, is sprake van een doorgifte naar een land zonder passend beschermingsniveau. Hiervoor zal een EU Model Contract moeten worden gesloten.

Amerikaanse wetgeving en de privacy van Europeanen

Nog los van de praktijken van de NSA die in 2013 door Edward Snowden werden onthuld, loopt de privacy van alle niet-Amerikanen ernstig gevaar. Er zijn de laatste jaren namelijk verschillende Amerikaanse wetten in het leven geroepen die het Amerikaanse instanties mogelijk maken de gegevens van niet-Amerikanen in te zien. Dit in combinatie met de opkomst van cloud services maakt dat de privacyschending vanuit de VS sterk is toegenomen.

In het algemeen geldt: clouddiensten die door Amerikaanse bedrijven worden aangeboden, zijn voor niet-Amerikanen onveilig.

Leveranciers van 'euroclouds'

Enkele grote cloudleveranciers, zoals Microsoft en Amazon, bieden cloudhosting binnen Europa aan. Uitgangspunt daarbij is dat de aanwezige data Europa niet zullen verlaten. Dit is een stap in de goede richting - maar laat nog steeds onverlet dat volgens Amerikaanse wetgeving (Patriot Act enz.) de data opgevraagd kunnen worden door de Amerikaanse overheid. Dit is eind 2014 nog eens bevestigd door de uitspraak van het Amerikaanse Hooggerechtshof.
Microsoft heeft twee locaties in Europa voor (euro)clouddiensten: Ierland (Dublin) en Nederland (Amsterdam). In contracten voor B2B kan worden afgesproken dat de data daar worden opgeslagen. Hiermee vervalt feitelijk een van de kenmerkende aspecten van de cloud, namelijk dat je niet weet waar je data zijn opgeslagen.

De bewerkersovereenkomst bij persoonsgegevens in de cloud

De Wet bescherming persoonsgegevens (hierna: Wbp) stelt regels voor het opslaan, verzamelen, verstrekken en combineren (kort gezegd: het verwerken) van persoonsgegevens. Daarbij gelden verschillende regels voor de verantwoordelijke en de bewerker, zoals de Wbp ze noemt. De verantwoordelijke is degene die de doelen van en de middelen voor de verwerking van de persoonsgegevens vaststelt. De bewerker is degene door de verantwoordelijke wordt ingeschakeld om de verwerking uit te voeren.
Omdat de klant bepaalt met welk doel, bijvoorbeeld facturatie, de persoonsgegevens worden opgeslagen en met welk middel (het systeem van de leverancier) de persoonsgegevens worden verwerkt, wordt de klant als verantwoordelijke voor de gegevensverwerking aangemerkt. De leverancier is dus bewerker van de persoonsgegevens. Hij doet namelijk niets anders dan het leveren van de software voor de bewerking van persoonsgegevens en het regelen van de opslag hiervan voor de klant. Hij heeft geen zeggenschap over de gegevens. Hij mag bijvoorbeeld niet zelfstandig besluiten een nieuwsbrief uit te sturen aan de klanten van de klant. Maar als de klant opdracht geeft, dan moet hij een nieuwsbrief versturen.
De klant is daarmee degene die door de betrokken personen aangesproken kan worden op schendingen van de Wbp. Maar de leverancier staat hier niet volledig buiten. De klant moet namelijk op grond van de Wbp passende technische en organisatorische maatregelen nemen om de persoonsgegevens te beveiligen tegen verlies of tegen andere vormen van onrechtmatige verwerking van de persoonsgegevens. Deze maatregelen kan de klant uiteraard niet nemen wanneer de gegevens niet bij hemzelf, maar bij op de server in het datacenter worden opgeslagen. Dat moet de leverancier dus doen.
De Wbp bepaalt daarom dat de klant ervoor zorg dient te dragen dat de leverancier een passend beveiligingsniveau biedt om een onrechtmatige verwerking van de persoonsgegevens te voorkomen. Wat passend is wordt bepaald door de verantwoordelijke, dus de klant. Hierbij kunnen de richtsnoeren van het College Bescherming persoonsgegevens gebruikt worden, maar dat is niet verplicht. (Zie ook ‘CBP misleidend met privacy richtsnoeren’.) De klant moet dus bij de leverancier nagaan hoe hij de opslag van persoonsgegevens heeft geregeld. Worden bestanden bijvoorbeeld versleuteld opgeslagen en wordt er gebruik gemaakt van een SSL-verbinding wanneer er gegevens vanuit de applicatie naar een server worden verzonden?
Indien de leverancier voldoet aan de eisen van de klant, moet er altijd een overeenkomst tussen leverancier en klant worden gesloten waarin de afspraken en verplichtingen over en

weer worden vastgelegd. In deze zogeheten bewerkersovereenkomst wordt afgesproken:

- voor welke doelen de leverancier de gegevens gaat verwerken;
- met welke middelen de leverancier de gegevens gaat verwerken;
- aan wie de leverancier de gegevens mag afstaan;
- welke beveiligingsmaatregelen de leverancier heeft genomen (of gaat nemen) om de opgeslagen gegevens te beveiligen;
- hoe aan de controle- en correctierechten van de betrokkene wordt voldaan;
- een exitscenario;
- dat de klant de leverancier vrijwaart van aanspraken van derden met betrekking tot de persoonsgegevens.

Het is ook weer de verantwoordelijkheid van de klant dat deze overeenkomst daadwerkelijk wordt gesloten. Voor de leverancier is het handig om een standaard bewerkersovereenkomst te hebben, die de klant kan ondertekenen. Daarmee wordt maatwerk voorkomen.

De Privacy Officer

Zeker gelet op de nieuwe EU-regelgeving en de verhoging van de maximale boete van € 4500 naar 1 miljoen euro bij inbreuk op de Nederlandse en Europese wetgeving is duidelijk, dat ieder bedrijf zich in dit onderwerp moet verdiepen.
Vanaf 2016 wordt iedere publieke organisatie, iedere private organisatie met meer dan 250 medewerkers en ieder bedrijf, dat dataverwerking als core business heeft (dus ook cloud leveranciers) geacht een Privacy Officer aangesteld te hebben. (Zie ook ‘Privacy Officer of Functionaris Gegevensbescherming - FG’.) Deze moet dus goed op de hoogte zijn welke verplichtingen voor de organisatie voortvloeien uit de Wbp en de EU-regelgeving. Zoals het er nu naar uitziet, gaan veel organisaties een dergelijke functionaris parttime inhuren. Maar u kunt natuurlijk ook een eigen medewerker hiervoor laten opleiden via bijvoorbeeld de ‘Cursus Privacy Officer in de praktijk’.