

Privacy in de cloud

Het grensoverschrijdend karakter van clouddiensten zorgt voor ongeëvenaarde privacyrisico's

Cloud computing is per definitie grensoverschrijdend. Staat dit op gespannen voet met de privacywetgeving? Hoe bereik je privacy-compliance bij cloud computing? Het sleutelwoord, zegt **Bieneke Braat**, is controle: technisch en juridisch. Een industriebrede privacy-standaard kan belangrijke belemmeringen wegnemen.



Eerder is in **Automatisering Gids (5 maart 2010)** gesignaleerd dat privacywetgeving een belemmering is voor cloud computing. Een reden daarvoor is dat uitwisseling van persoonsgegevens naar landen buiten de Europese Unie maar beperkt mogelijk is, terwijl uit de aard van cloud computing nu juist volgt dat deze grensoverschrijdend is. Het recht op privacy is een Europees grondrecht. Om dat te waarborgen, hebben we binnen de Europese Unie een privacyniveau vastgesteld dat hoger is dan in de rest van de wereld. In onze vergaande gedigitaliseerde maatschappij is dat geen overbodige luxe. De vraag is dus of het wenselijk is dat cloud computing door die bescherming heen breekt. De benadering kan dan ook worden omgedraaid: hoe kan privacycompliance worden bereikt bij cloud computing en in het bijzonder met betrekking tot uitwisseling van persoonsgegevens?

Een van de grootste privacyrisico's bij cloud computing is de beveiliging van de persoonsgegevens. Hoe groot de financiële risico's zijn, blijkt bijvoorbeeld uit de boete (van circa 2.700.000 euro) die de Britse tak van verze-

kearaar Zurich kreeg opgelegd. Reden daarvoor was dat het in Zuid-Afrika een back-up tape was verloren met persoonsgegevens van zo'n 46.000 klanten. Maar beveiliging bij cloud computing is niet een privacyrisico in het bijzonder. Net zomin als consumenten willen dat hun persoonsgegevens toegankelijk zijn voor onbevoegde derden (bijvoorbeeld overheden in landen buiten de Europese Unie), willen bedrijven dat derden toegang kunnen krijgen tot hun vertrouwelijke en concurrentiegevoelige informatie. Adequate beveiliging is dus een noodzakelijke voorwaarde voor de levering van clouddiensten. De omvang, mogelijkheden en met name het grensoverschrijdende karakter van clouddiensten (per definitie via internet) zorgen voor ongeëvenaarde privacyrisico's. Bij cloud computing onttrekt de verwerking van persoonsgegevens zich niet alleen aan het oog – en de controle – van de persoon op wie de gegevens betrekking hebben, maar ook aan de partij die verantwoordelijk is voor de verwerking van persoonsgegevens (zie kader). Er zal hierna van uit worden gegaan dat de klant van de cloudserviceprovider (CSP) een professionele partij is en geen consument.

Het sleutelwoord bij privacycompliance is: controle. Als de klant van een CSP volledige controle over zijn data heeft, dan kan hij zelf zorgen voor privacycompliance. Die controle moet niet alleen bestaan uit technische, en dus feitelijke controle, maar ook uit juridische controle. De CSP moet door de klant aanspra-

Privacyniveau Europese Unie hoger dan in de rest van de wereld

kelijk kunnen worden gehouden voor overtreding van contractuele (privacy)verplichtingen.

Als het gaat om uitwisseling van persoonsgegevens, is het eerst van belang om te vermelden dat uitwisseling binnen de Europese Unie – strikt genomen de Europese Economische Ruimte (EER), dit zijn de landen van de

Europese Unie en Noorwegen, Liechtenstein en IJsland – vrijelijk mogelijk is. De klant kan zorgen voor compliance wanneer hij zelf kan bepalen dat data alleen in landen binnen de EER worden opgeslagen (Amazon.com biedt bijvoorbeeld deze mogelijkheid). Het probleem ontstaat dan ook wanneer de cloud 'buiten de grenzen van de EER' treedt. Het doorgeven van persoonsgegevens naar niet-EER-landen waar geen passend privacybeschermingsniveau bestaat, is in beginsel niet toegestaan. Het kan slechts op grond van een beperkt aantal uitzonderingen, dat bij cloud computing doorgaans niet geldt of niet praktisch is. Toch is het mogelijk om persoonsgegevens door te geven aan landen buiten de EER met behulp van een aantal juridische oplossingen (zie kader). Deze oplossingen zijn alleen niet altijd eenvoudig te bereiken. Het is aan de Europese Unie om doorgifte van gegevens naar landen buiten de EER te vereenvoudigen. Vanaf 15 mei 2010 heeft de Europese Commissie daar al een begin mee gemaakt door de 'modelcontracten' (zie kader) minder beperkend te maken. De eenvoudigste oplossing voor het tackelen van doorgifterisico's is louter gebruik te

maken van een private cloud (kort gezegd een cloud die door maar één CSP in de lucht wordt gehouden), waarbij de klant volledige controle heeft over de data-uitwisseling. Maar vanuit kostenopbouw is louter gebruikmaken van een private cloud niet altijd wenselijk. Een belangrijk probleem bij niet-private clouds

Probleem is dat de klant maar met één provider een contract sluit

is dat de klant maar met één CSP een contract sluit, waarin – als het goed is – verplichtingen ten aanzien van privacy en beveiliging en controle over data zijn opgenomen. De contracterende CSP wisselt data uit met andere CSP's die geen contractuele verplichtingen hebben jegens de klant. Een oplossing daarvoor is de CSP te verplichten contracten aan te gaan met de derde

CSP's op grond waarvan de klant bij de derde CSP's privacycompliance kan afdwingen. De CSP's zouden ook onderling algemene contracten met elkaar aan kunnen gaan om privacycompliance te waarborgen.

Om de efficiëntie en het vertrouwen van de klant in clouddiensten te vergroten, kan ook gedacht worden aan zelfregulering door de (Europese) 'cloudindustrie'. Dit zou bijvoorbeeld kunnen door een industriebrede privacystandaard te introduceren waaraan CSP's zich verbinden en waarin zij privacyverplichtingen op zich nemen, en bijvoorbeeld via een arbitrageprocedure aansprakelijk kunnen worden gehouden door verantwoordelijken maar ook door de personen op wie de persoonsgegevens betrekking hebben. Als een dergelijke standaard ook door de Europese Commissie zou kunnen worden goedgekeurd voor de uitwisseling van persoonsgegevens naar landen buiten de EER, zou dit een belangrijke privacybelemmering wegnemen. De privacystandaard zou in de lijn kunnen liggen van de modelbepalingen van de Europese Commissie. En er zou een met 'Safe Harbor' vergelijkbaar programma kunnen worden opgezet. CSP's uit landen buiten

Verantwoordelijkheid

Wie is aan te merken als 'verantwoordelijk' voor de gegevensverwerking? Dit is de partij die het 'doel en de middelen' van de gegevensverwerking bepaalt. In de meeste gevallen is dit de klant van de cloudserviceprovider (CSP). Als de CSP echter vergaande controle heeft over de persoonsgegevens en bijvoorbeeld zelfstandig bepaalt in welke landen ze worden opgeslagen, zou deze ook als verantwoordelijke kunnen worden aangemerkt. In dat geval heeft de CSP verzwaaarde privacyverplichtingen. Om dat te voorkomen moet contractueel worden vastgelegd dat de CSP louter uitvoering geeft aan de instructies van de klant.

Veilig gegevensverkeer

Wat zijn juridische oplossingen voor het veilig doorgeven van persoonsgegevens aan landen buiten het grondgebied van de EER?

- 1. Voldoende bescherming**
Een aantal landen buiten de EER heeft een voldoende hoog privacyniveau om vrijelijk persoonsgegevens mee uit te mogen wisselen. Voorbeelden zijn Argentinië, Canada en Zwitserland.
- 2. Safe Harbor**
Voor de Verenigde Staten geldt de zogenaamde Safe Harbor-regeling. Een Amerikaanse onderneming die persoonsgegevens uit de Europese Unie ontvangt, kan ook een voldoende hoog privacyniveau bereiken als het voldoet aan de Safe Harbor-principes. Het bedrijf wordt dan opgenomen op de Safe Harbor-lijst. Het kan van deze lijst worden verwijderd wanneer blijkt dat het niet langer aan de Safe Harbor-principes voldoet.

- 3. Binding Corporate Rules**
Bedrijven die in meerdere landen buiten de EER actief zijn, kunnen door middel van 'Binding Corporate Rules' tot privacycompliance komen. BCR's zijn in wezen interne richtlijnen die ervoor zorgen dat de vestigingen in verschillende landen hetzelfde privacyniveau in acht nemen als het niveau dat binnen de EER wordt vereist. De Europese hoofdstvestiging ziet toe op de naleving van de BCR door de vestigingen.

- 4. Modelcontractbepalingen Europese Commissie**
Voor minder 'internationale' ondernemingen is er ook nog de mogelijkheid om een vergunning te vragen voor doorgifte van de persoonsgegevens naar landen buiten de EER. Voor het verkrijgen van een vergunning moet de partij die verantwoordelijk is voor de gegevensverwerking een overeenkomst sluiten met de partij die de persoonsgegevens ontvangt. Daarin moeten minimaal door de Europese Commissie vastgelegde modelbepalingen zijn opgenomen. Omdat het aanvragen van de vergunning de nodige administratieve lasten met zich meebrengt, wordt er in de praktijk niet vaak gebruik van gemaakt. Daarnaast kunnen de modelbepalingen alleen worden gebruikt door de verantwoordelijke – dus de klant – zelf en een buiten de EER gevestigde ontvanger van de gegevens.

▀ Voor reacties en nieuwe bijdragen van deskundigen: Henk Ester (h.ester@sdu.nl, (070) 378 03 97).