

CLOUD COMPUTING

Implicaties van de Amerikaanse Patriot Act

Steeds meer bedrijven en organisaties brengen hun (persoons)gegevens naar de cloud. Daarmee verplaatsen zij gegevens van hun eigen interne bedrijfsnetwerk en – servers naar het internet. In de Fenedexpress van oktober 2012 besprak ik een aantal juridische aspecten hiervan. In dit artikel ga ik nader in op de vraag of de overstap naar cloud computing consequenties heeft voor de toegang tot (persoons)gegevens door buitenlandse overheden.



Mirjam Elferink

Implicaties Patriot Act

Is de veiligheid en vertrouwelijkheid van uw gegevens in de cloud wel gewaarborgd? Cloud computing kan namelijk op gespannen voet staan met Europese privacyreggeving (in Nederland omgezet in de Wet bescherming Persoonsgegevens, hierna: Wbp) wanneer de data het subject van een informatieverzoek op grond van de Patriot Act worden. Op basis van de huidige wetgeving in zowel de VS als in Nederland kunnen bevoegde instanties gegevens van ondernemingen opvragen, mits er een verband is met de staatsveiligheid of strafvordering. Juridisch gezien is het niet mogelijk om dergelijke verzoeken tegen te houden. Dat overheden gegevens kunnen opvragen is overigens niet nieuw, maar door de overgang naar cloud computing en de veranderende context die dit met zich brengt, is het zaak dat ondernemingen zich bewust zijn van de mogelijke risico's hiervan.

In de cloud staan uw gegevens niet meer onder volledige controle van uw bedrijf, terwijl u als bedrijf op grond van de Wbp wel verantwoordelijk bent en blijft voor de bescherming van uw gegevens. Bij cloud computing is de klant doorgaans de verantwoordelijke en de leverancier de bewerker in de zin van de Wbp. Uw status als verantwoordelijke in de zin van de Wbp brengt met zich dat u boetes kunt krijgen indien u zich niet aan de privacywetgeving houdt en in het ergste geval kunt u aansprakelijk worden gehouden voor ontstane schade. De Patriot Act kan derhalve verstreckende gevolgen hebben voor zowel diegenen op wie de gegevens betrekking hebben als voor de verantwoordelijke van de persoonsgegevensverwerking.

Als verantwoordelijke bent u verplicht om voorafgaande toestemming te verkrijgen van betrokkenen voordat persoonsgegevens

aan derden mogen worden geopenbaard. Verstrekking van persoonsgegevens aan Amerikaanse autoriteiten is alleen toegestaan als de verantwoordelijke een gerechtvaardigd belang kan aantonen van hemzelf of van een derde aan wie de gegevens worden verstrekt. Een gerechtvaardigd belang bestaat bijvoorbeeld als er een wettelijke verplichting zou bestaan. Omdat het bij een informatieverzoek door de Amerikaanse overheid niet gaat om de naleving van een Nederlandse wettelijke verplichting, kan daar echter geen beroep op worden gedaan. Als er wel een gerechtvaardigd belang zou bestaan om gehoor te geven aan een informatieverzoek, dan nog geldt op basis van de Wbp dat dat belang steeds moet worden afgewogen tegen het privacybelang van de betrokkenen. Bovendien geldt dat nooit meer gegevens mogen worden verstrekt dan strikt noodzakelijk.

Zowel leveranciers als afnemers van cloud-diensten krijgen in dit geval dus te maken met twee tegenstrijdige regimes, de Wbp versus de Patriot Act.

De leverancier van wie de informatie wordt gevraagd, mag daarover niets aan zijn opdrachtgever mededelen. De opdrachtgever die verantwoordelijke is in de zin van de Wbp kan die belangenafweging dus niet zelf maken. Sterker nog, hij weet vaak van niets en kan dus geen invloed op de verstrekking uitoefenen. Omdat de leverancier zelfstandig moet beslissen over het informatieverzoek wordt wel betoogd dat hij daardoor van pet wisselt en in plaats van bewerker, verantwoordelijke in de zin van de Wbp wordt.

Toepasselijkheid Patriot Act

Hoever reikt de Patriot Act? Daarover is nog veel onduidelijkheid. De Patriot Act heeft in

Inleiding

In het publieke debat daarover valt vaak de term Patriot Act.¹ Deze Amerikaanse wet en andere daaraan verwante regelgeving zouden het mogelijk maken dat gegevens van Nederlandse gebruikers van clouddiensten worden opgevraagd vanuit de Verenigde Staten (VS).² Dit blijkt ook uit recent onderzoek van het Instituut voor Informatierecht van de Universiteit van Amsterdam.³ Dit onderzoek heeft veel stof doen opwaaien. Er zijn zelfs Kamervragen gesteld over de implicaties van de Patriot Act.⁴ Ook op Europees niveau houdt dit onderwerp de gemoederen in beweging.⁵ In dit artikel zal daarom worden ingegaan op de implicaties van de Amerikaanse Patriot Act.⁶

ieder geval betrekking op data die zijn opgeslagen op servers van elk bedrijf gevestigd in:

- de Verenigde Staten;
- de Europese Unie dat een moederbedrijf in de Verenigde Staten heeft;
- de Europese Unie en dat voor data processing gebruik maakt van de diensten van een dochteronderneming die gevestigd is in de Verenigde Staten;
- de Europese Unie en dat gebruik maakt van een derde partij voor data storage of data processing, i.e. een in de Verenigde Staten gevestigde hosting company;
- de Europese Unie, maar dat op structurele basis zaken doet met een bedrijf in de Verenigde Staten.

Op basis van de huidige wetgeving in zowel de VS als in Nederland kunnen bevoegde instanties gegevens van ondernemingen opvragen. Daarbij maakt het in beginsel niet uit of die gegevens in de cloud zijn opgeslagen of in een eigen datacenter. Wanneer de gegevens in een cloud zijn opgeslagen bij een leverancier die onder Amerikaanse jurisdictie valt, kunnen de gegevens rechtstreeks vanuit de VS bij de betreffende onderneming worden opgevraagd. In andere gevallen kan een verzoek tot inzage worden gedaan via de Nederlandse bevoegde instanties.

Doorgifte persoonsgegevens

Verstrekking van persoonsgegevens op basis van de Patriot Act brengt onvermijdelijk doorgifte van persoonsgegevens naar de VS mee. Daarvoor gelden eveneens strikte privacyregels: de Wbp verbiedt verzending van persoonsgegevens naar een land zonder passend beschermingsniveau, zoals de Verenigde Staten.

Veel Amerikaanse bedrijven zullen de bezwaren afdoen met een beroep op de 'Safe Harbour-regeling'. Met deze regeling garanderen die bedrijven dat ze zullen voldoen aan het Europese beschermingsniveau. Het is echter maar zeer de vraag in hoeverre deze bedrijven dergelijke garanties kunnen waarmaken. De Patriot Act gaat immers in alle gevallen voor en wie niet voldoet aan die wet zal strafrechtelijk vervolgd worden.

De Automatiseringsgids van 24 mei 2011 berichtte over deze problematiek als volgt: *"ICT-leveranciers met Amerikaanse roots stellen veelal dat zij Safe Harbour gecertificeerd zijn en dat doorgifte aan de Amerikaanse groepsmaatschappijen daarom toegestaan zou zijn. Op basis van de Safe Harbour afspraken zou de Amerikaanse groepsmaatschappij de verkregen persoonsgegevens dan op haar beurt mogen afstaan aan Amerikaanse autori-*

teiten. Dat een leverancier aan wie informatie wordt gevraagd, daarover niets tegen zijn Amerikaanse groepsmaatschappij mag zeggen, wordt daarbij gemakshalve vergeten."

Uiteraard speelt bovenstaande problematiek niet in het geval u uw gegevens onderbrengt bij een Nederlands bedrijf dat niet onder een van de hiervoor genoemde categorieën valt en waar de Patriot Act derhalve niet op van toepassing is. Dit geldt tenzij het betreffende bedrijf in de toekomst zou worden overgenomen door een Amerikaans bedrijf. Voor een dergelijke omstandigheid raden wij u aan om een specifieke contractuele beperking op te nemen.

Maak een risicoanalyse

Mocht u overwegen om diensten af te nemen bij een cloud provider dan raden wij u aan om een goede risicoanalyse te maken van de diverse soorten gegevens binnen uw bedrijf die het onderwerp zouden kunnen zijn van een informatieverzoek van de Amerikaanse overheid. Om de positie van uw bedrijf met betrekking tot de toepassing van de Patriot Act en de mogelijke risico's daarvan te onderzoeken, raden wij u aan om het antwoord op de volgende – niet uitputtende lijst van – vragen duidelijk voor ogen te hebben:

1. Valt de cloudaanbieder onder de Amerikaanse jurisdictie? Waar is de provider gevestigd? Doet hij (nu of later) zaken met de VS? Waar staan zijn datacentra?
2. Worden delen van de dienstverlening uitbesteed aan derden (bijvoorbeeld voor het maken van back-ups, of wordt gebruik gemaakt van de infrastructuur van derden)?
3. Welke data zet ik in de cloud en welke niet?
4. Welke risico's loopt mijn bedrijf?
5. Neem een aparte clause op in uw contract over de handelwijze bij een toegangsverzoek in het kader van de Patriot Act. Leg daarbij vast dat nooit meer dan de noodzakelijke gegevens worden verstrekt ter voldoening aan een informatieverzoek.
6. Bepaal indien mogelijk, dat de leverancier verplicht is om (in rechte) bezwaar te maken tegen informatieverzoeken en het verbod om derden te informeren over deze verzoeken.
7. Neem een informatieverplichting op voor de leverancier over gedane verzoeken en gegevensverstrekkingen, zodra hij dat mag.
8. Stem af of en hoe de betrokkenen moeten worden geïnformeerd.
9. Check of het zinvol is om een specifieke vrijwaringsverplichting overeen te komen.

ICT Protocol

Ten slotte verdient het te allen tijde aanbeveling uw organisatie bewust te maken van de risico's. Zonder dat u er erg in heeft kunnen uw werknemers namelijk belangrijke gegevens in de cloud zetten en ze zo in theorie openbaar maken voor de Amerikaanse overheid. Hotmail, Gmail, Google Docs en Dropbox zijn immers ook clouddiensten en vallen in beginsel onder de jurisdictie van de Patriot Act. Het kan raadzaam zijn uw werknemers te instrueren geen bedrijfs- en privacygevoelige informatie naar dergelijke diensten te uploaden. Desnoods kunt u uw werknemers daartoe verplichten middels een ICT-protocol.

Conclusie

Uit recent onderzoek van het Instituut voor Informatierecht van de Universiteit van Amsterdam blijkt dat Nederlandse afnemers het risico lopen dat Amerikaanse opsporingsdiensten toegang hebben tot hun gegevens. Ondanks de verreikende implicaties die de Patriot Act kan hebben bestaat er discussie of er praktisch wel sprake is van een probleem. De wet bestaat immers geruime tijd en uit de praktijk blijkt dat er tot nu toe terughoudend gebruik van wordt gemaakt. Dat neemt in mijn ogen echter niet weg dat de dreiging bestaat en dat het raadzaam is om de risico's zo veel als mogelijk contractueel af te dekken.

Mirjam Elferink, Advocaat KienhuisHoving Advocaten en Notarissen, gespecialiseerd in Intellectuele Eigendom en ICT.

Meer weten? www.fenedexpress.nl, zoek op  Cloud computing, ICT-diensten

Voetnoten

- 1 Het Amerikaanse Congres heeft in 2003, in het kader van de terrorismebestrijding na 9/11, de Patriot Act aangenomen.
- 2 Waar in dit artikel wordt gesproken over de Patriot Act wordt tevens bedoeld op de daaraan aanverwante wetgeving.
- 3 J.V.J. van Hoboken, A.M. Arnbak, N.A.N.M. van Eijk, Cloud diensten in hoger onderwijs en onderzoek en de USA Patriot Act, rapport Instituut voor Informatierecht Universiteit van Amsterdam, september 2012.
- 4 Kamerstukken II, 2012/2013, Aanhangsel van de Handelingen nr. 535, 9 november 2012.
- 5 Er circuleert een Voorstel Verordening bescherming persoonsgegevens. European Commission, 'Proposal for a Regulation of the European Parliament and of the Council of the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', COM(2012) 11 final, 25.01.2012.
- 6 Met dank aan mijn collega mr. Martijn Kortier.