Public Briefing / mei 2014

Zeven terugkerende rechtsvragen over clouddiensten

Mr. V.A. de Pous[1]

Cloud computing mag dan in het middelpunt van de belangstelling staan, maar het leveringsmodel roept telkens dezelfde vragen op, vooral bij het afnemen van een clouddienst als vorm van uitbesteding. Bestuurders vragen niet alleen op bezorgde toon naar een aantal belangrijke juridische aspecten, maar ook, en hieraan gekoppeld, hoe het zit met de beveiliging van in de cloud verwerkte bedrijfsinformatie en de verantwoordelijkheid hiervoor.

1. *Als ik mijn data in de cloud doe, ben ik dan verantwoordelijk voor de bescherming ervan of wordt de cloud provider dat?*

Wanneer we de vraag beperken tot bedrijfsinformatie die *externe* cloudleveranciers (en hun ketenpartners) in opdracht van een klant verwerken, dringt een vergelijking met het fiscale kader op. Zoals de belastingplichtige organisatie te allen tijde zelf verantwoordelijk is en blijft voor de juiste verwerking van financiële gegevens (ten overstaan van de Belastingdienst), zo geldt dezelfde primaire verantwoordelijkheid voor een bedrijf voor de zorgvuldige gegevensverwerking ten opzicht van de relevante stakeholder. Dat kunnen klanten zijn, maar tevens werknemers, aandeelhouders, business partners, toeleveranciers, et cetera. Informatie*beveiliging* valt daar expliciet onder.

Maar we moeten wel onderscheiden. De belangrijkste (juridische) piketpaal vormt de aard van de informatie. Om welke data gaat het? Persoonsgegevens of andere

[1] Victor de Pous is bestuurslid van de Stichting EuroCloud Nederland en zelfstandig bedrijfsjurist sinds 1983.

(bedrijfs) informatie, bijvoorbeeld financiële bestanden of technische en commerciële knowhow (bedrijfsgeheimen).

In overeenkomsten voor clouddiensten kunnen partijen allerlei afspraken maken over gegevensbescherming en doen dat ook. Zover het niet om dwingend recht gaat, bestaat er veel contractuele vrijheid. In de praktijk komt het er op neer dat beiden een eigen verantwoordelijkheid dragen. Bij de verwerking van persoonsgegevens heeft een cloudleverancier bovendien een eigen, wettelijk bepaalde verplichting tot het nemen van 'passende technische en organisatorische maatregelen' om deze te beveiligen tegen 'verlies of tegen enige vorm van onrechtmatige verwerking', aldus de Wet bescherming persoonsgegevens.

2. *Als mijn data bij een Nederlandse cloud provider zijn ondergebracht, kunnen de Amerikanen daar dan bij?*

Laten we beginnen bij het begin en dat is het brede perspectief. Veel landen kennen wetgeving van extraterritoriale werking. Dat betekent dat de rechtsmacht van een soevereine staat zich over de eigen landgrenzen uitstrekt. Dus zeker niet uitsluitend de VS. Of de Amerikaanse overheid op grond van de Patroit Act in bepaalde gevallen toegang heeft tot in het Nederland verwerkte bedrijfsinformatie, hangt allereerst af of er een verbinding bestaat tussen de Verenigde Staten en het bedrijf dat de gegevens verwerkt en vervolgens de wijze waarop deze verbinding is vormgegeven. Belangrijke criteria zijn de juridische en feitelijke zeggenschap (over de data).

Verder hebben veel staten afspraken gemaakt over rechtshulpverzoeken. In voorkomende gevallen kan ook de VS de Nederlandse overheid vragen om bepaalde informatie te verstrekken, die is opgeslagen in een datacenter in Nederland, van een Nederlandse cloudleverancier, zelfs wanneer een link van deze bedrijven met Amerika ontbreekt.

3. *Er zijn tax havens. Bestaan er ook 'data havens', plaatsen waar je je data uit praktisch oogpunt het beste kunt onderbrengen?*

Wanneer 'praktisch oogpunt' bekent dat niemand behalve de eigen organisatie bij de informatie kan, dan zijn er ongetwijfeld landen die geen partij zijn bij relevante internationale (juridische) verdragen. Deze soevereine staten zullen niet of nauwelijks meewerken aan een informatieverzoek van een ander land, allereerst

omdat de rechtsgrond hiervoor nadrukkelijk ontbreekt. Veder wegen nogal eens nationaal-politieke belangen mee. Een ‘data haven’ kan economisch bezien aantrekkelijk zijn voor een land, net zo als een bankgeheim dat doorgaans is.

Bedenk echter wel dat de beste oplossing (voor de vertrouwelijkheid van gegevensverwerking) bij de techniek begint. Maak gebruik van sterke encryptie en zorg voor goed sleutelmanagement. Amerikaanse bedrijven geven waarschijnlijk gehoor aan het verzoek van *hun* overheid om data van klanten te ontsleutelen, maar wanneer zij als cloudleverancier niet over de sleutel beschikken, kan dat in beginsel niet.

4. *Als de cloud provider failliet gaat of wordt overgenomen, houd ik dan toegang tot mijn data?*

Bij een bedrijfsovername gaan doorgaans ook alle rechten en verplichting over. Dat zal dus uit continuïteitsoogpunt van een clouddienst meestal geen probleem vormen. Faillissement van een ICT-dienstverlener betreft een ander verhaal. Over een gefailleerde onderneming zwaait de curator de scepter. Om een zo naadloos mogelijke overgang naar een andere cloudleverancier mogelijk te maken, paste Luxemburg vorig jaar haar wetgeving aan. De curator ter plaatste is nu wettelijk verplicht de bedrijfsinformatie van de klanten van de failliete service provider *stante pede* aan de betreffende klant ter beschikking stellen. Geen discussie.

Nederland is nog niet zo ver. Faillissement kan voor problemen bij gebruikersorganisaties zorgen en dat wringt des te meer omdat het bij cloud computing altijd om (vaak continue en uitbestede) *diensten* gaat.

Het juridische uitgangspunt luidt dat bij de afname van clouddiensten eigendom op data van de klant *niet* overgaat op de leverancier. Daarmee zijn we er overigens niet. Een cloudleverancier verwerft doorgaans ook een licentie — een gebruiksrecht — op de bedrijfsinformatie van de klant, maar — let op — de reikwijdte hiervan behoort beperkt te blijven tot het voor een goede technische en administratieve verwerking strikt noodzakelijke.

Ten aanzien van het faillissement van een clouddienstverlener geldt opnieuw dat primair feitelijke maatregelen (net zo als bij gegevensbescherming) uitkomsten bieden, terwijl het recht ‘slechts’ borgt. Zorg dus tenminste voor een (dagelijkse) back-up van in de cloud verwerkte bedrijfsinformatie (in geval van software-als-clouddienst), kies wanneer mogelijk voor een open dataformat zoals XML (dit

maakt portabiliteit van data en dus ook leverancierswissel eenvoudiger) en overweeg vervolgens escrow-achtige zekerheidsconstructies. Hierbij gaat het naast de toegang tot de eigen bedrijfsinformatie om de continuïteit van de applicatiedienst via Internet.

5. *Wat is de status van de Europese privacywetgeving?*

Naar verwachting wordt nieuwe Algemene Verordening Gegevensbescherming (AVG) dit jaar vastgesteld en kan in 2015 in werking treden. Naast inhoudelijke verschillen — onder andere aanscherping van privacyrechten en een meldplicht bij datalekken — is het vooral relevant dat het niet om een *richtlijn* gaat — die immers om implementatie in 28 nationale rechtsstelsels vraagt, waardoor onvermijdelijk en ongewenst verschillen per lidstaat ontstaan — maar een *verordening,* dus met rechtstreekse werking. Deze route vormt in feite *de* manier voor het realiseren van een heus geharmoniseerd en uniform wettelijke kader (voor de verwerking van persoonsgegevens) voor de interne markt.

6. *Hoe is het gesteld met informatiebeveiliging in Nederland?*

Zegge en schrijven *een* bug in het veel gebruikte (open source) beveiligingsprogramma OpenSLL voor versleutelde communicatie, genaamd Heartbleed, geeft, zoals de naam treffend suggereert, een desastreus en tevens ontluisterend beeld. De cruciale fout maakte *tweederde* van het immense World Wide Web kwetsbaar. Opnieuw wordt hierdoor de vinger op de zere plek gelegd: onze zo belangrijke (wereldwijde) digitale infrastructuur hangt met touwtjes aan elkaar. Dat geldt ook voor Nederland. Een van de allergrootste problemen betreft het gebrek aan kwaliteit van digitale code. De ene kwetsbaarheid, stapelt zich op de andere fout, bug of flaw – hoe we de gebreken ook allemaal noemen. Technische problemen, cybercriminaliteit en datalekken zijn letterlijk aan de orde van de seconde. Dat moet en kan anders, dus door kwaliteitsnormen te stellen en die vervolgens te codificeren.

7. *Hoe worden die gegevens beveiligd?*

Zowel door technische en als organisatorische maatregelen. Belangrijk is dat in het domein *cybersecurity* er een communautaire richtlijn ligt. Dit Europese ontwerp bepaalt onder meer dat exploitanten van essentiële infrastructuur in een

aantal sectoren (financiële dienstverlening, vervoer, energie, gezondheidszorg), aanbieders van diensten van de informatiemaatschappij (met name appstores, platforms voor elektronische handel, betalingsdiensten via Internet, cloud computing, zoekmachines en sociale netwerken) en overheden *risicobeheersregelingen* moeten invoeren en tevens ernstige incidenten met betrekking tot hun kerndiensten moeten melden (*wettelijke meldplicht*).