

Privacy en cloud computing

OCLC Contactdag 4 oktober 2011



Agenda



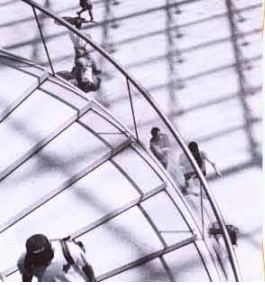
- Wat is cloud computing?
- Gevolgen voor verwerking data
- Juridische implicaties



Wat is cloud computing?



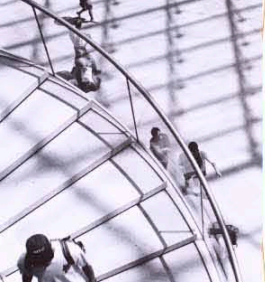
- Kenmerken:
 - On-demand self-service
 - Delen van resources
 - Elasticiteit
- Opdeling in verschillende modellen: SaaS, PaaS, IaaS
- Verschillende varianten: publiek, privaat, gemeenschappelijk, hybride



Gegevens in de cloud

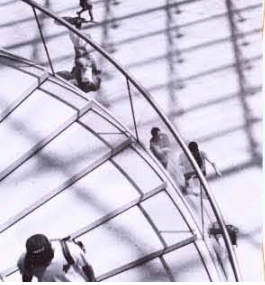
Verminderde controle klant over gegevens:

- Gespreide (internationale) opslag
- Locatie data onbekend
- Gedeeld gebruik gegevensdragers
- Data veel in transit
- Data moeilijk te wissen



Juridische implicaties

- Opnieuw bepalen van de rollen van de klant en leverancier
- Passende waarborgen, denk aan beveiliging
- Internationale doorgifte, noodzaak van een passend beschermingsniveau



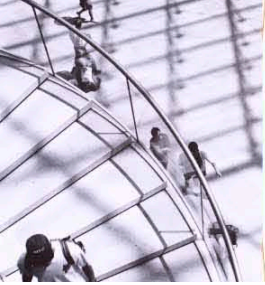
Wet bescherming persoonsgegevens



Van toepassing op iedere geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens

Persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon

Verwerking is elke handeling met betrekking tot persoonsgegevens



Klant en leverancier

- Wbp richt zich primair tot verantwoordelijke
- Verantwoordelijke stelt het doel van en de middelen voor de verwerking vast
- Bewerker verwerkt gegevens voor de verantwoordelijke, zonder dat hij diens ondergeschikte is
- Leverancier bepaalt vaak wijze waarop persoonsgegevens worden verwerkt (middelen)



Beveiligingsmaatregelen

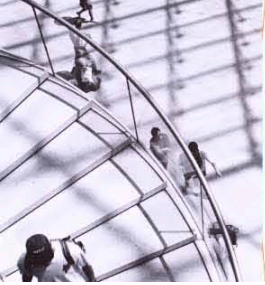


- Klant is verplicht tot treffen passende technische en organisatorische beveiligingsmaatregelen tegen verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens
- Klant dient ervoor zorg te dragen dat leverancier voldoende waarborgen biedt voor beveiliging persoonsgegevens
- Klant moet daadwerkelijk nagaan of cloud oplossing van de leverancier voldoende waarborgen biedt

Voldoende waarborgen?

Contactsbepaling voldoende ?

- Klant moet voor iedere verwerking
 - een risicoanalyse uitvoeren
 - nagaan of de door de leverancier getroffen maatregelen passend zijn
- Balans tussen
 - risicoklasse (hoe hoger het risico, hoe hoger het vereiste niveau van beveiliging)
 - stand van de techniek
 - kosten van tenuitvoerlegging



Is cloud computing veilig?



Cloud computing niet persé (on)veiliger

Cloud Security Alliance : Cloud Computing isn't necessarily more or less secure than your current environment. As with any new technology, it creates new risks and new opportunities.



Internationale doorgifte

Passend beschermingsniveau:

- EU-landen
- Witte lijst van de Europese Commissie
- Waaronder Safe Harbor
- Patriot Act !

Publicaties SURF

- “ Checklist Cloud Security”
(SURFnet, Gartner en SURFibo)
- “ Cloud Computing, de wolk in het onderwijs”
(Centrum voor Recht, Technologie en
Samenleving (TILT) van de Universiteit van
Tilburg)
- “Checklist privacy en cloudcomputing”
opgesteld i.s.m. Project Moore Advocaten.

www.surf.nl

Thema cloud services

Onderwerp	Verplicht of wenselijk	Wbp	Toelichting	In de praktijk	Voorbeeld bepaling	Toelichting op bepaling
Adequaat beveiligen	Verplicht	Art. 13 en 14		Risico analyse		
Controleren beveiliging	Verplicht	Art. 14		Vaak bezwaar tegen audit		
Geen toegang derden	Verplicht	Art. 8,9,12,13 en 14		Geheimhouding verplichting		
Onderaanneming	Verplicht	Art. 12, 13 en 14		Vaak wel opgenomen		Bij buitenlandse partijen aanvullende regels
Bewaartermijn	Verplicht	Art. 10		Doorgaans een standaard bewaartermijn		
Verwerking alleen in landen met passend beschermingsniveau	Verplicht	Art. 76		Lokalisatie of regionalisatie relatief eenvoudige oplossing		Safe harbor
Informereren beveiligingsincidenten	Wenselijk			Vaak niet accoord		

Evelijn Jeunink
Juridisch adviseur
Evelijn.jeunink@surfnet.nl
www.surfnet.nl



Voor deze presentatie geldt een Creative Commons licentie
<http://creativecommons.org/licenses/by/3.0/>