



PrivaSense

Privacy and Trust in the Digital Society

Privacy Compliance in een Cloud Omgeving

Jeroen Terstegge

NVvIR

Amsterdam, 17 juni 2010

Even voorstellen

- **mr.drs. Jeroen Terstegge, CIPP**
 - Directeur Privacyadviesbureau PrivaSense
 - *Strategie en beleid*
 - *Compliance*
 - *Risk Management*
 - *Stakeholder Communication*
 - *CPO / FG Consultancy*
 - *Interim CPO / FG Services*
 - *Privacy training*
- **Nevenwerkzaamheden**
 - Voorzitter Commissie Privacy RCO (VNO-NCW / MKB Nederland)
- **Greep uit het verleden:**
 - Corporate Privacy Officer, Philips International
 - Deelnemer Privacy Round Table OESO
 - Voorzitter Privacycommissie DigitalEurope
 - Lid Privacycommissie Internationale Kamer van Koophandel (ICC)
 - Voorzitter Expertgroep Privacy en Nieuwe Technologieën ECP.NL
 - Beleidsmedewerker Registratiekamer

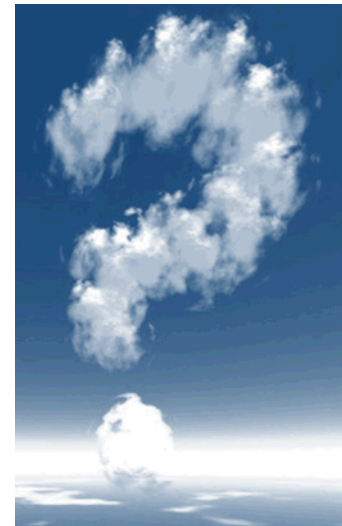
Inleiding

- **Probleemstelling**

- *“Vormt de privacywetgeving een probleem voor outsourcing van IT diensten naar een cloud omgeving ?”*

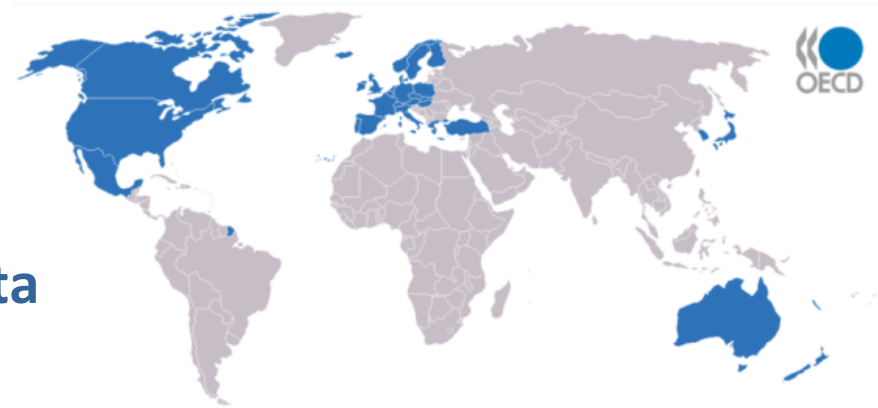
- **Voor de goede orde ... : Wat is Cloud Computing ?**

- Type diensten:
 - Software as a Service (SaaS)
 - Platform as a Service (PaaS)
 - Infrastructure as a Service (IaaS)
- Type Cloud Omgevingen
 - Public cloud
 - Community cloud / Partner cloud
 - Virtual Private cloud
 - Private cloud
 - Hybrid cloud



OESO Privacy Principles

- Doelbinding
- Limitering van data collectie
- Limitering van gebruik van data
- Data kwaliteit
- Beveiliging
- Transparantie
- Rechten van betrokkenen
- Verantwoording



OESO Privacy Principles in de Cloud

- De Cloud lijkt risico's in te houden voor de realisatie van alle Privacy Principles !



- **Risico's m.b.t. service design en delivery**

- | | | |
|----------------------------|---|--|
| – Doelbinding | → | Systeemdwang |
| – Limitering datacollectie | → | Meer gegevens verzameld dan nodig |
| – Data kwaliteit | → | Onduidelijkheid integriteit gegevens |
| – Transparantie | → | Onduidelijkheid wat er precies gebeurt |
| – Beveiliging | → | Onvoldoende beveiliging |

- **Risico's m.b.t. service provider**

- | | | |
|---------------------------|---|---|
| – Limitering gebruik | → | Diefstal / Misbruik gegevens |
| – Rechten van betrokkenen | → | Onvoldoende mogelijkheden om rechten uit te oefenen of te effectueren |
| – Verantwoording | → | Onvoldoende mogelijkheden voor aansprakelijkheidsstelling |

EU privacyrecht

- **OESO Privacy principes zijn overgenomen in Richtlijn 95/46/EG**

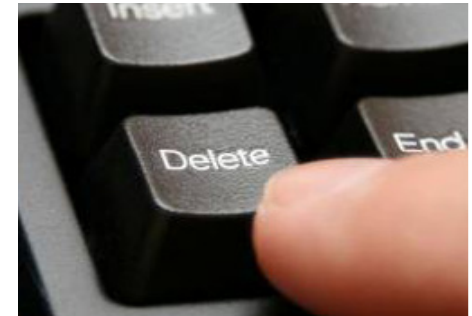
- In Nederland geïmplementeerd in de Wet Bescherming Persoonsgegevens (WBP)
 - Naleving is een verplichting van de “verantwoordelijke”
 - “Bewerker” is verantwoordelijk voor beveiliging van gegevens
- NB. De Data Controller is ook verantwoordelijk als de verwerking plaatsvindt bij/door een service provider (“bewerker”)
 - Bewerkerscontract
 - Instructies, toezicht
- De mogelijkheden voor doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (“EER”) zijn beperkt
 - Reden: Bescherming van persoonsgegevens is Europees grondrecht
 - Doorgifte is OK als derde-land een “adequaat beschermingsniveau” garandeert
 - NB. Doorgifte is zowel opslag in het buitenland als toegang vanuit het buitenland
 - EER = EU + Noorwegen, IJsland en Liechtenstein



Compliance risico's (1)



- **Is de privacywetgeving van toepassing?**
 - Verwerking persoonsgegevens ?
 - Infrastructuurdiensten: verwerking persoonsgegevens moet worden verondersteld
 - SaaS: alleen als persoonsgegevens onderdeel zijn van de service
 - **MAAR ALTIJD**: verwerking van persoonsgegevens van gebruikers !
 - Welke wetgeving is van toepassing ?
 - Welke EU lidstaat ?
 - Soms ook andere wetgeving, bijv. VS
- **Bewaartermijnen**
 - “Ongelimeerde” opslagcapaciteit door schaalbaarheid
 - Risico op onvolledige verwijdering
- **Juistheid / Nauwkeurigheid gegevens**
 - In hoeverre is de integriteit van de gegevens gewaarborgd ? “Resource pooling” ?
 - Kunnen wijzigingen worden aangebracht in de software ?



Compliance risico's (2)

- **Beveiligingsmaatregelen**

- **De “voorkant”: Toegangsbeveiliging**

- Identificatie- / authenticatie methoden
 - Single Sign-on: “ID-as-a-Service” (bijv. Open ID)
- Spoofing

- **Verbindingen**

- Betrouwbaarheid verbindingen
- Betrouwbaarheid betrokken partijen

- **De “achterkant”**

- Betrouwbaar personeel ?
- Beveiligde omgeving ? Resource pooling ?
- Integriteit van de service delivery ?
- Beschikbaarheid gegevens ?
- Wat gebeurt er met de back-ups ?
- Hoe is de support geregeld ?



Compliance risico's (3)

- **Informatie aan betrokkenen**

- “alle nadere informatie om zorgvuldige gegevensverwerking jegens de betrokkene te waarborgen”, maar wat is dat dan ?
 - Bijv. Export van bijzondere data naar buitenland ?

- **Rechten van betrokkenen**

- Inzagerecht: Alle relevante informatie ?
- Correctierecht: Systeemdwang ?
- Blokkering: Systeemdwang ?
- Toestemming / Opt-out: Systeemdwang ?

Your privacy
is important to us...



- **Locatie v.d. verwerkingen**

- Onzichtbaarheid locatie (opslag en support !)
- Naleving regels internationaal gegevensverkeer
 - NB. Ook andere wetgeving kan invloed hebben op de aanvaardbaarheid vd locatie
Bijv. Export Controle wetgeving.

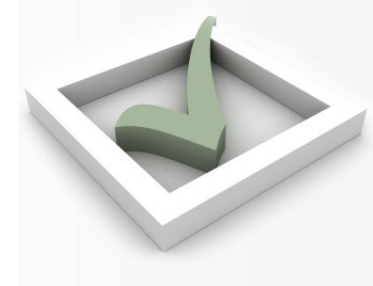
Compliance risico's (4)

- **Bewerkerscontract**

- **Bewerkerscontract is wettelijk verplicht**
- **Mogelijkheid tot onderhandelingen ?**
 - Hangt mede af van het type cloud
- **Zo nee, voldoen Terms & Conditions van de service provider aan de wettelijke eisen ?**
 - Hoe is de beveiliging van de gegevens geregeld?
 - Is subcontracting mogelijk? Zo ja, wat is er geregeld?
 - Hoe is evt. internationaal gegevensverkeer geregeld?
- **Andere aandachtspunten:**
 - Kan je instructies geven? Heb je auditrechten?
 - Evt. toegang tot gegevens door derden, incl. de overheid
 - Wordt je geïnformeerd over beveiligingsincidenten en wijzigingen in het recht?
 - Mate van aansprakelijkheid cloud provider ? Verzekering voor beveiligingsincidenten?
 - Wat gebeurt er met de gegevens bij einde contract of i.g.v. bankroet cloud provider



Ten slotte



- **Compliance is complex**
 - o.a. privacywetgeving, export controle wetgeving
 - Zorgvuldigheid is geboden
- **Weet waar de gegevens blijven**
 - Breng de hele keten in kaart
- **In principe geen compliance-gevoelige gegevens verwerken in een publieke Cloud**
 - Ga voor een (virtual) private cloud omgeving
 - Denk na over de locatie
- **Let ook op Support services**
 - Locatie, beveiliging, overige compliance maatregelen

Discussiepunt

- *Heb je een compliance probleem als de gegevens in de Cloud volledig zijn versleuteld ?*
 - Is dat een “verwerking van persoonsgegevens” in de zin van de WBP?





PrivaSense

Privacy and Trust in the Digital Society

Dank voor uw aandacht

Contact

Jeroen Terstegge
terstegge @ privasense.nl
www.privasense.nl