



Contracting in de cloud.

A selection of some of the challenges

Jeroen Schouten
Legal Counsel

Introduction

- Google and the cloud
- Relevant (technical) aspects

Contractual challenges

- Protection of personal data
 - Data Transfer
 - Data Security
 - Data Controller vs Data Processor
- Vendor Lock-In
- Standards compliance

“Risks should always be understood in relation to overall business opportunity and appetite for risk – sometimes risk is compensated by opportunity”

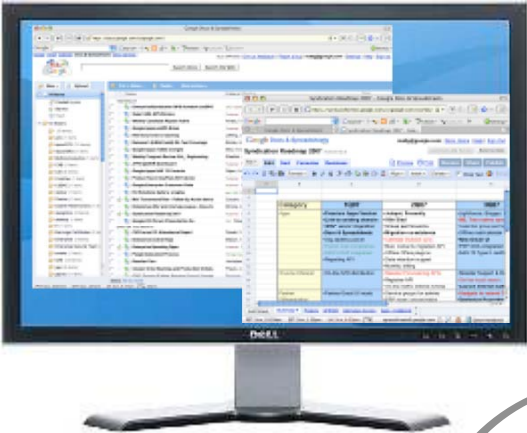
“Ultimately you can outsource responsibility but you can’t outsource accountability”

Cloud Computing – Benefits, risks and recommendations for information security, ENISA November 2009

Google and the cloud

Green

Cloud Computing



Messaging



Collaboration



Security



Compliance



Google Apps Premier Ed.

- €40 / user / year
- 25GB mailbox per user
- 99.9% SLA
- Support for admins
- APIs & migration tools

Google Message Security

- £6/ user / year
- Anti-virus & anti-spam
- Policy management

Google Message Discovery

- £12.50 / user / year
- Google Message Security +
- Archiving & legal discovery



Enables third party developers to build applications on Google's infrastructure

Google cloud printing



Relevant (technical) aspects

Cloud Computing Lowers Costs



Add € for High Availability

Add € for Scale and Capacity

Add € for Operational Support

Add € for Hardware and Storage

€€€ Software License

Legacy Approach



High Availability included

Scale and Capacity included

Operational Support included

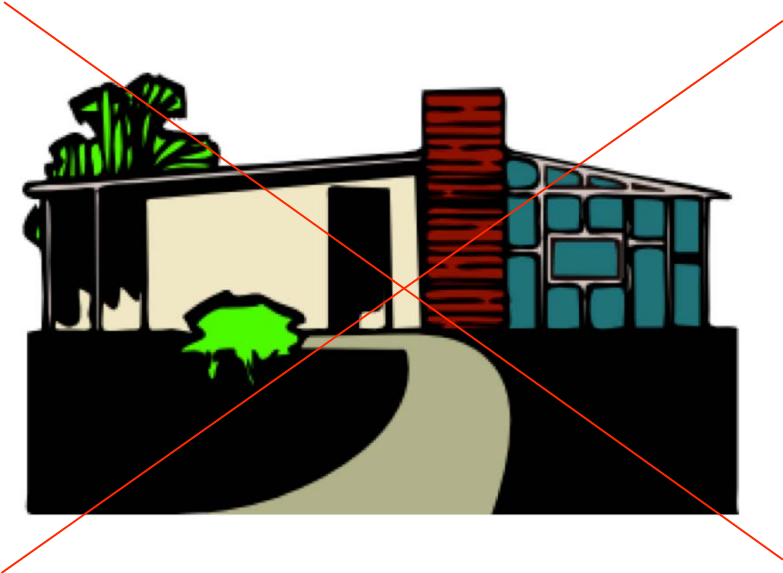
Hardware and Storage included

One Low Price

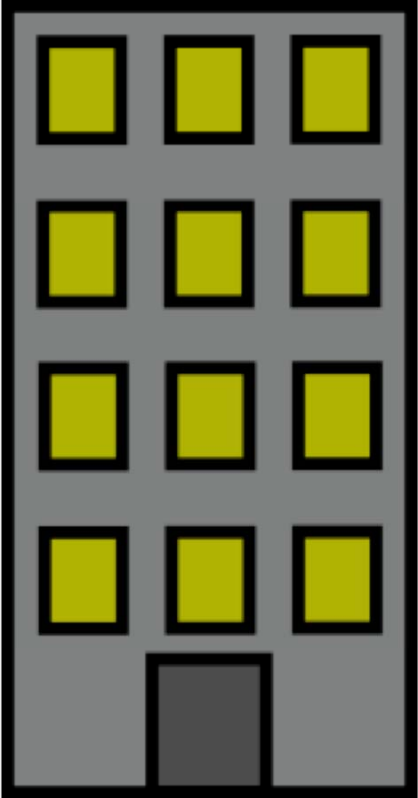
Cloud Approach



Multi tenanted environment



Villa

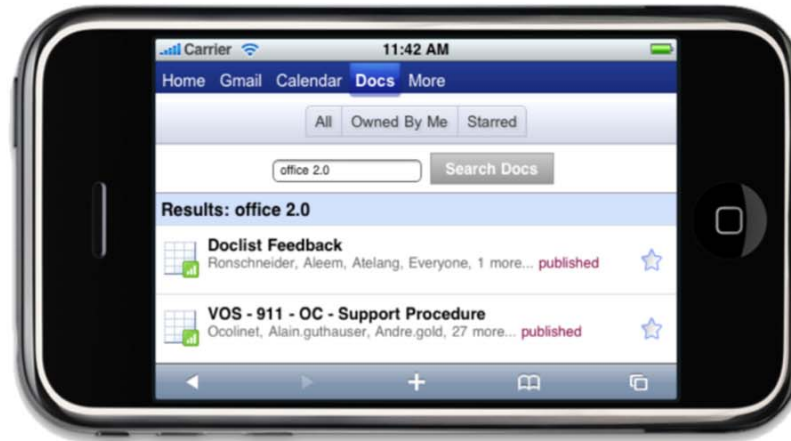


Furnished Apartment Building

The cloud is global



Access Data From Anywhere, Anytime



- Users don't need a powerful computer to use the cloud, since data and software are stored in the cloud
- Mobile phones, PDAs, video recorders, online game consoles, etc. can be cloud interfaces



Contractual Challenges



Cross border transfer



Cross border transfer; the rules



- Directive 95/46 EC; article 25-26
- Dutch Data Protection Act; article 76-78
- US Safe Harbor principles

Contractual challenges



- Cloud provider only subscribes to Safe Harbor principles
- Data centers are in countries in which for which the EU Commission has **not** established that it has “an adequate level of protection of personal data”
- Data location is not always clear in the cloud
- Is Customer data restricted to country boundaries in the cloud?
- US Safe Harbor principle of onward transfer

Data Security



Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

Contractual challenges



- Varying implementations of article 17 in EU Member States
- Security in the cloud is not bespoke
- Cloud provider does not provide a specific customer audit right (SaaS 70)
- How about the use of sub-processors and security

Data controller vs processor



PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

Contractual challenges



- How to effectively allocate data processor responsibilities
- Cloud provider utilizes a standard privacy policy you don't agree with
- Article 16 Directive 95/46 EC; no processing by processor except on the instructions of the data controller
- Establishment of data controller determines applicable law to processing (exception article 17 Directive 95/46 EC).

Vendor lock-in



Contractual challenges



- How do we contractually safeguard our data migration?
- Will export API's and native protocol support remain in the future?
- Google <http://www.dataliberation.org>





PCI DSS

9001



9002

27001

Contractual challenges



- The Cloud provider is not ISO certified nor does it going to be
- I want to use the Cloud Services to process credit card numbers
- The Cloud provider does not allow me to do specific audits
- Cloud computing standards are still being developed
- My data needs to stay in the EU

Thank You!

Q&A