

LEGAL RISKS AND LIABILITIES RELATED TO **CLOUD COMPUTING** IN EUROPE

Paolo Balboni paolo.balboni@paolobalboni.eu

www.paolobalboni.eu

Friday, January 29th 2010 – CPDP Conference

Central question

“How can we protect the confidentiality, integrity and availability of information that is processed outside our control?”

Structure of the presentation

Step 1: Introduction

Step 2: Identification of the key legal risks

Step 3: Focus on data protection risks and liabilities

Step 4: Practical solutions

Step 5: Answer to the central question / Conclusions

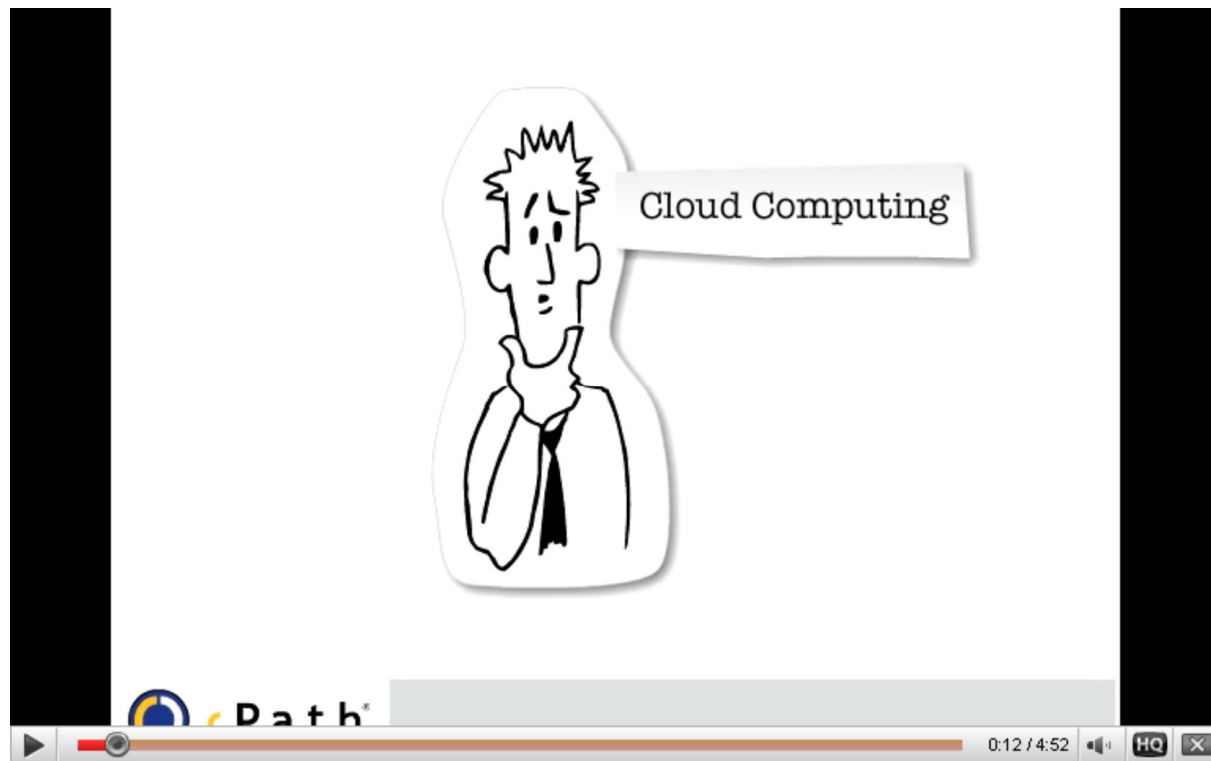
Introduction (I)

*“The cloud-computing model offers four general types of services: (i) Software as a service - **SaaS**; (ii) Infrastructure as a service - **IaaS**; (iii) Platform as a service - **PaaS**; and (iv) Process as a service - **PaaS**.”*

*Analysts estimate that **in 2012**, the size of the enterprise cloud-computing business may reach **\$60 billion to \$80 billion** – or about **10% of the global IT-service and enterprise-software market**”*

(Capturing the Value of Cloud Computing: How Enterprises Can Chart Their Course to the Next Level – The Boston Consulting Group - November 2009)

What is cloud computing?



Introduction (II)

- ENISA Study on [Cloud Computing Risk Assessment](#)
- *It is foreseeable that the main use of cloud computing services is the commercial benefit, which comes from it being a bulk/commodity service that can be bought at short notice or on a pay-per use basis. This implies **standardisation of services and thus of legal conditions**. Nevertheless, there may be situation, in which cloud computing services will be tailored for big customers (e.g., large companies and public administrations). This implies **specific tailored contracts**.*

Introduction (III)

CLOUD PROVIDER	CLIENT
A) Big company – Strong bargaining power	SME – Weak bargaining power
B) Big company – Strong bargaining power	Big company or Public Administration - Strong bargaining power
C) SME – Weak bargaining power	Big company or Public Administration - Strong bargaining power

Key legal risks

- Data Protection ('Privacy')
- Confidentiality
- Intellectual Property
- Professional Negligence
- Outsourcing Services / Changing of Control

Focus on data protection risks and liabilities

Considering that the services provided by Cloud Providers are related to, e.g., email, messaging, desktops, projects management, payroll, account and finance, CRM, sales management, custom application development, custom application, telemedicine, customers' billing, etc.; **personal data (including sensitive data) will be processed**. Such data may belong to a number of persons (data subjects), i.e., employees, clients, suppliers, patients and, more generally, business partners.

Applicability of the Directive 95/46/EC

Data Protection Directive 95/46/EC

EU Member States provisions by which the Directive has been implemented apply:

- to the processing of personal data, including data held abroad, **where the processing is performed by any entity established** either in the Member State territory or in a place that is under the member State sovereignty;
- to the processing of personal data performed **by an entity established outside the EU, that for purposes of processing makes use of equipment, automated or otherwise, situated in the territory of a Member State**, unless such equipment is used only for purposes of transit through said territory.

Data Controllers and Processors

Controller -> Customer of the Cloud Provider

External Processor / Controller -> Cloud Provider

Clarifications are needed on this –

Art.29 Data Protection Working Party

Controller's duties & obligations

- Principles of lawfulness, finality, proportionality, and data minimization
- Information notice and consent
- **Data security measures**
- Data subject's rights
- **Data transfer to 3rd parties/countries (*Consent / Standard Model Clauses*)**

Possible sanctions

- Failure to comply with data protection law may lead to **administrative, civil and also criminal sanctions**, which varies from country to country, for the Data Controller. Such sanctions are mainly detailed in the relevant statutory instruments by which the Directive 95/46/EC has been implemented in the various EU Member States.

How to deal with data protection risks and liabilities

The issues defined above may all be dealt with **contractually**. In the contract/General Terms and Conditions between the Cloud Provider and its Customers, a Data Protection/Privacy clause has to be included.

This clause should set forth the relevant parties' duties and obligations. In such clause there should be a reference to:

- Scope(s) of the processing
- Information notice and consent
- **Data security measures (SLAs / Annexes)**
- Data subject's rights
- **Data transfer to 3rd parties/countries (*Consent / Standard Model Clauses*)**
- Penalties (possibly)
- Termination clause (possibly)

Answer to the central question / Conclusions

Q: “How can we protect the confidentiality, integrity and availability of information that is processed outside our control?”

A: CONTRACTUALLY

Conclusions:

Data protection/privacy – Confidentiality – Intellectual Property clauses may be suitable of being standardised, except the relevant penalties, which depends on parties' bargaining power.

Whereas the inner content of the Limitation of Liability – Indemnity – Third-party Outsourcing – Change of Control Clauses depend themselves on the bargaining power of the parties, and thus they are less suitable for standardisation.

Qs & As

**Thank you very much for
your attention!**

Check out:

ENISA Study on Cloud Computing Risk Assessment

Paolo Balboni paolo.balboni@paolobalboni.eu

www.paolobalboni.eu