The problem of cloud data governance

Vasilis Tountopoulos, Athens Technology Center S.A. (ATC)

CSP EU Forum 2014 - Thursday, 22\textsuperscript{nd} May, 2014
Focus on data protection in the cloud

Why data governance in the cloud raises barriers?

- Challenges and Implications

Drivers for accountability

- Cloud complexity and vulnerabilities
- Business driven risks
- Legal complexity and constraints
Challenges in data governance

Based on cloud data processing

Incentives

- Scale of cloud services
- Role in the future business and personal life
- Complexity of the supply chain
- Advanced data mining to manage big data

...but, difficulty in building Chains of Accountability in the cloud

- Complexity of the cloud service provision chain
- Ramifications of failure within the chain
- Involved business risks – size of the organisations involved
- Complexity in implementing right liability measures
- Potential weakness in the transparency and verifiability of the supply chains
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Difficult to plan for the potential business risks
Business Risks of Using Cloud

Support multi-disciplinary data driven business cases

Based on cloud specific features
• How personal and corporate data are handled in the cloud?

Multi-tenancy of cloud applications
• Co-tenants can gain inappropriate access to data of another application instance.

Complex, dynamically changing environment
• Ensuring appropriate data protection, overlapping responsibilities in data management, unauthorised secondary usage, vendor demise, lack of transparency.

Data duplication and proliferation
• Loss of control and transparency in data lifecycle management, especially in cross-border interactions
• Simplified access from multiple locations, but different legislative regimes.

This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Security and privacy concerns

Cloud end users being responsible for cloud security

Governance over data use and processing

• Personal and confidential data management is subject to the purpose of use.

Compliance to laws, regulations, standards and specifications

• Privacy preservation and data protection in data location places.
• Non interoperable regulatory frameworks for cross-boundary communications.

Trust and risk assessment

• Monitoring and controlling cloud service execution with respect to policies and service level agreements.

Incidence response

• Detection and remediation mechanisms should be in place through cross actor exchangeable interfaces.

This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Detection and Remediation

How tools should support runtime governance

Lack of transparency and verifiability by cloud service providers

- Implications in terms of policy violations along the cloud service provision chain.
- Should force auditing from trusted actors.

Complexity of Liability in Service Provision Ecosystems

- Attributed obligations not clear with overlapping responsibilities.
- Obligations vary depending on to whom they refer to.
Constraints

Regulatory and legal issues to consider

Subcontracting and negotiation of contracts

• Customers providing consent to the use of subcontractors needs appropriate contract management.
• Need for enabling cloud customers enforce obligations, according to policies
• Growing Usage of Integrators

Data transfers and guaranteed security levels

• Change of data location
• Unaware of the desired security levels
• Use of free vs paid cloud services in the provision chain
Drivers for an accountability-based approach

Improve level of data stewardship
Provide trustworthy mechanisms for data protection in the cloud
Decrease regulatory complexity
Provide more effective mechanisms for complex and dynamic business environments

Accountability-based approaches for trust and security

This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Defining Accountability

Conceptual Definition:

- Accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly.

- Accountability for an organization consists of accepting responsibility for the stewardship of personal and/or confidential data with which it is entrusted in a cloud environment, for processing, storing, sharing, deleting and otherwise using the data according to contractual and legal requirements from the time it is collected until when the data are destroyed (including onward transfer to and from third parties).

- It involves committing to legal and ethical obligations, policies, procedures and mechanisms, explaining and demonstrating ethical implementation to internal and external stakeholders and remedying any failure to act properly.
This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).