Accountability Model for Cloud Governance

Massimo Felici, Hewlett-Packard Laboratories

CSP Forum 2014, Athens, 21-22 May 2014

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

Problem of Data Governance
- Data Governance in the Cloud

Accountability Definitions
- Conceptual Definition of Accountability
- Definition of Accountability for Data Stewardship in the Cloud

Accountability Model
- Accountability Attributes, Practices and Mechanisms

Accountability Governance
- Accountability Framework
- Accountability Context
- Accountability Governance

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

Problem of Data Governance

- Different regulatory regimes
- Complex governance environment
- Lack of trust in the cloud
- Lack of governance and transparency
- Transfer of data into the cloud
Conceptual Definition of Accountability

• 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.

Applicable across different domains and capturing a shared multidisciplinary understanding within the project

Concerned about governance

Responsibly and proactively (explaining, justifying, remedying) delivery of actions

Compliance with respect to internal and external criteria defined by stakeholders
Defining Accountability

Contextualising accountability for data governance in cloud ecosystems

Definition of Accountability for Data Stewardship in the Cloud

- Accountability for an organisation 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.

Deploying different mechanisms

Ethical aspects of accountability

personal and/or confidential data
Accountability Model

From accountability to being accountable

- Operationalise the accountability definitions
- Capture different abstraction levels of accountability
- Identify attributes contributing towards accountability
- Characterise accountable organisations
- Identify elements of accountability practices
- Enable accountability practices
Accountability Model

Accountability Definitions

- Accountability
- Attributes
- Practices
- Mechanisms

Observability
Verifiability
Attributability
Transparency
Responsibility
Liability
Remediability

Defining governance
Ensuring governance
Demonstrating governance
Holding to account

Different mechanisms supporting accountability

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

Preventive – investigating and mitigating risk in order to form policies and determine appropriate mechanisms to put in place; putting in place appropriate policies, procedures and technical mechanisms

Detective – monitoring and identifying policy violation; putting in place detection and traceability measures

Corrective – managing incidents and providing notifications and redress

Supporting accountability at different stages

Co-designing: Responsible and ethical corporate governance, Innovative regulatory frameworks, and Supporting technologies

Supporting cloud actors

Corrective

- Facilitation of redress
- Data accuracy correction

Detective

- Notification of policy violation
- Data subject access
- Other tracking & transparency tools

Preventive

- Risk and trust assessments
- Policy specification
- Certification

1. Cloud Subject
   a. Individual
   b. Organisation

2. Cloud Customer
   a. Individual
   b. Organisation

3. Cloud Provider
4. Cloud Carrier
5. Cloud Broker

6. Cloud Auditor
7. Cloud Supervisory Authority

Inter-disciplinary co-design

- Involvement in privacy impact assessments
- Guidelines & best practice

- Infringement detection
- Monitoring & policy-aware logs
- Reasoning tools

- Audit
- Violation reports

- Dispute resolution
- Evidence to aid punishment

- Notification of policy violation
- Data subject access
- Other tracking & transparency tools

- Notification of policy violation
- Data subject access
- Other tracking & transparency tools

- Notification of policy violation
- Data subject access
- Other tracking & transparency tools

- Notification of policy violation
- Data subject access
- Other tracking & transparency tools

- Notification of policy violation
- Data subject access
- Other tracking & transparency tools

- Notification of policy violation
- Data subject access
- Other tracking & transparency tools

Whole ecosystem approach
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Addressing data governance in the cloud

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