Accountability and Privacy Compliance

Siani Pearson
Principal Research Scientist, Security and Cloud Lab, HP Labs Bristol
Scientific Co-ordinator, EU A4Cloud project

March 2015
The Principle of Accountability

Accountability consists of:

- Defining and accepting responsibility
- Ensuring implementation of appropriate actions
- Explaining and justifying actions
- Remediating failure

Article 29 WP 173, Opinion 3/2010 on the principle of accountability:

Data protection must move from ‘theory to practice’.

(i) the need for a controller to take appropriate and effective measures to implement data protection principles;

(ii) the need to demonstrate upon request that appropriate and effective measures have been taken. Thus, the controller shall provide evidence of (i) above.
## Actor Roles

<table>
<thead>
<tr>
<th>Extended NIST cloud roles</th>
<th>Data protection roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud subject</td>
<td>Data subject</td>
</tr>
<tr>
<td>Cloud customer</td>
<td>Data controller or Data processor</td>
</tr>
<tr>
<td>Cloud provider</td>
<td>Data processor or Data controller</td>
</tr>
<tr>
<td>Cloud carrier</td>
<td>Data processor or Data controller (unlikely) or Not applicable.</td>
</tr>
<tr>
<td>Cloud broker</td>
<td>Data processor or Data controller</td>
</tr>
<tr>
<td>Cloud auditor</td>
<td>(Not Applicable)</td>
</tr>
<tr>
<td>Cloud supervisory authority</td>
<td>Supervisory authority (DPA or NRA)</td>
</tr>
<tr>
<td>(Not Applicable)</td>
<td>Third party</td>
</tr>
<tr>
<td>(Not Applicable)</td>
<td>Recipient</td>
</tr>
</tbody>
</table>
Regulatory Responsibilities

Accountability through cloud service supply chains to cloud customer, and to governance

DC accountable for applicable data protection measures

DP accountable for cooperation with DC to:
• meet data subjects’ rights
• assist DC in providing security measures
• act only on DC’s behalf
Accountability Relationships

*Accountor* is accountable to *accountee* for:

**Norms**
- Obligations & permissions that define data practices
  - Can be expressed in policies
  - Derived from law, contracts and ethics

**Behaviour**
- The actual data processing behaviour of an organisation

**Compliance**
- Entails comparison of organisation’s actual behaviour with the norms
EU Context

- Cybersecurity strategy
- Cloud strategy
- Data Protection Regulation
- ePrivacy Directive
- Breach notification
- Security
- Accountability & transparency
- Privacy by design
- Sanctions
- Customer expectations
Motivations for Accountability Approach

**INCREASE TRUST (FOR CONSUMERS, CLIENTS AND REGULATORS)**

**DECREASE REGULATORY COMPLEXITY**

**HELP ORGANISATIONS IMPLEMENT EFFECTIVE DATA PROTECTION MEASURES**
Business Users’ Ranking of Key Actions to Improve Cloud Adoption

Accountability is a clear supporter of growth in the cloud marketplace
Complex Global Environment

National privacy or data protection law in place
Other significant privacy laws in place
Emerging privacy or data protection laws

Data Flows
No specific Contracts
Model Contracts
Model Contracts
Model Contracts
Model Contracts
Model Contracts
Model Contracts
Model Contracts
BCR (EU only)
Moving to an Accountability-Based Approach

**PREVIOUS**

Questions

CSP

Answers

DPA

**TOMORROW**

Questions

CSP

Answers

DPA

DEMONSTRATE

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
How can Organisations Be Accountable?

1. Define policies regarding data practices
2. Deploy mechanisms to put these policies into effect
3. Monitor data practices
4. Correct policy violations
5. Demonstrate compliance

Organisations must demonstrate willingness and capacity to be responsible and answerable for data practices
How can CSPs provide Support to SMEs?

**Decreasing exposure to risk + increasing transparency**

SMEs could have a high risk potential

*Example mechanisms:*

- Information for evaluation of risk assessment
- Transparency about CSP level of data protection
- Transparency about cloud service provision
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Example:
Cloud Offerings Advisory Tool (COAT)
These factors vary across cloud services, and are reflected in the contracts.
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

Cloud Offerings Advisor Tool (COAT)

Cloud Brokerage tool

Informed choices about
- Data Protection
- Privacy
- Compliance
- Governance

End-users and SMEs

Terms of Use

Contract

Cloud Offerings

Terms of Use

Contract

Contract

Service Provider 1

Service Provider 2

Service Provider 3

Service Provider 4
### Business Questionnaire

Please indicate your requirements

#### Price Range
- **From:** 0
- **To:** 5000

#### Acceptable Storage Locations including Backup
- Europe (EU)
- United States
- Europe (Non-EU)
- China
- Local
- Any

#### Acceptable Data processor location
- Europe (EU)
- United States
- Europe (Non-EU)
- China
- Local
- Any

#### Data transfer in case of emergency?

#### Do you want Encryption?
- Yes
- No
- Doesn't Matter

#### Is it important that any disputes are resolved in your own country?
- Yes

### 10 Matched Offers

<table>
<thead>
<tr>
<th>Offer</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon WebServices</td>
<td>€4500.00/Month</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Color</td>
<td>€75.00/Month</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Mono</td>
<td>€25.00/Month</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud-Drive</td>
<td>€0.00/Month</td>
</tr>
</tbody>
</table>

---

**Acceptable Storage Locations including Backup**

This question concerns where personal data is stored and what data protection and data privacy laws apply to protect it. Personal data is data that relates to identifiable people. In countries within the EU, the data protection laws are similar so transferring and storing data within the EU is treated in the same way.

In countries outside the EU, data protection laws are different. You should not transfer personal data outside the EU without checking whether this data will be adequately protected. Your Service Provider may guarantee in its contract that personal data will be protected if this data is not adequately protection law.
Example:

Data Protection Impact Assessment Tool (DPIAT)
Based on successive questionnaires, for initial and full screening for a given project

Tailored to satisfy the needs of SMEs that intend to process personal data in the cloud

Addresses article 33 of proposed General Data Protection Regulation (EC version)

• Introduces new obligation of data controllers and/or processors to carry out Data Protection Impact Assessment prior to risky processing operations
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Where do we go from here?

Tools for facilitating choice, control, transparency

Technology & best practice for the future that could limit risk, e.g.

- Continuous monitoring
- Audit trails for data use across CSP chains
- Breach detection
- Dynamic assurance
More information.....

www.a4cloud.eu
Thank you

Siani Pearson, Principal Research Scientist, HP Labs
Email: siani.pearson@hp.com
Tel: +44 (0) 117 316 2558