Government Use of Cloud Computing – Legal Challenges

Liesbeth Hellemans
Liesbeth.hellemans@law.kuleuven.be
ICRI/CIR – KU Leuven
IAPP Europe Data Protection Congress
Agenda

1. Cloud for Europe project

2. Legal Challenges of Public Sector Cloud Computing

3. Legal recommendations for Public Sector Cloud Computing
   • Policy-oriented
   • In practice
Public sector cloud use as a collaboration between public authorities and industry through pre-commercial procurement.
Cloud for Europe brings together public authorities and industry to support public sector cloud use.

- Identify **obstacles** for cloud use in the public sector
- Define **services** that overcome those obstacles
- Procure research from industry to find **innovative solutions** for cloud services
Partners
Legal challenges of Public Sector Cloud Computing
Methodology

• Literature overview (current & future legal framework)
• Due diligence consortium partners
  ▪ Austria, Belgium, Portugal, Spain, The Netherlands, Norway
  ▪ Public sector aspects
    - Languages
    - Public procurement
    - Archiving
    - Procedural law (criminal and social)
    - Medical law
    - Bookkeeping/fiscal
    - National Defense and State secrets
  ▪ Legal challenges experienced by consortium partners
Categories of challenges

- 2 categories
  - Common to most cloud services
  - Public sector specific
- Non-exhaustive
Legal challenges common to most cloud services

- Applicable law & jurisdiction
- Consumer protection
- Data protection
- Data portability/interoperability
- Liability
- Contractual framework
Public Sector specific legal challenges

- Governmental Access
- Legislation discouraging cloud transfer
- Inaccurate Procurement legislation
- Fragmented and divering national legislation
- Language requirements
- National defense/State secrets

Government cloud
Legal Recommendations for Public Sector Cloud Computing
Policy - oriented
## Regulatory

- Review, clarify and harmonize legislation in public domain related areas to make it cloud-friendly
- Address the issues on governmental environment and intelligence gathering at European and international level
- Issue clear guidelines when uncertainty on the conditions of cloud use
- Further harmonize and simplify public procurement rules
- Set up a cross-border working group between legal specialists and technological teams to address encryption standards
- Further harmonize and modify data protection legislation to reflect the reality of cloud computing
- Set up a code of conduct for governments as Cloud Consumers, providing for a clear overview of cloud prerequisites for the public sector, including a set of minimum contractual standards
- Set up a code of conduct to provide guidelines in the relationship Public Authority – Cloud End User
Develop Legislation Executing Cloud Services addressing and overcoming legal cloud barriers by accomplishing certain legal requirements
In practice
## Key attention points

**Cross-border cloud:** set up a contractual collaboration model between governments (liability !)

**Federal/regional cloud:** set up a contractual collaboration model between the various government

Assess the needs and practical way of working (call-offs ?)

Comply with local Public Procurement legislation

Conduct a comprehensive and thorough risk analysis

- Sensitivity of the data?

Indicate and specify the location of the data centres

- Preference Europe
- Transfer outside the EEA?
- Location support services?

Segregate the ‘duties’ sufficiently

- Division of cloud project in various lots
## Key attention points

<table>
<thead>
<tr>
<th>Define language requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay specific attention to the danger of ‘lock-in’</td>
</tr>
<tr>
<td>• stand-by Cloud Provider?</td>
</tr>
<tr>
<td>Encrypt all data and ensure the encryption key sits with the public authorities</td>
</tr>
<tr>
<td>Choose a Cloud Provider that complies with data protection legislation (third party certification)</td>
</tr>
<tr>
<td>Define appropriate minimum SLA’s</td>
</tr>
<tr>
<td>Sign an appropriate contractual framework addressing both general contract and data privacy requirements</td>
</tr>
<tr>
<td>• Negotiate</td>
</tr>
<tr>
<td>• Unlimited access to the data</td>
</tr>
<tr>
<td>• Accountability rules</td>
</tr>
<tr>
<td>• Data protection concerns</td>
</tr>
<tr>
<td>Address Cloud End User concerns</td>
</tr>
<tr>
<td>• Security/confidentiality/IPR/privacy protection – data protection policy</td>
</tr>
<tr>
<td>• Redress mechanisms</td>
</tr>
</tbody>
</table>
Source ?
• [http://www.cloudforeurope.eu/](http://www.cloudforeurope.eu/)
• Downloads: Legal Implications of Cloud Computing
• Contact: liesbeth.hellemans@law.kuleuven.be