Data Privacy in the Cloud
E-Government Perspective

Herbert Leitold; EGIZ, A-SIT

International Cloud Symposium 2011, Panel on Data Privacy and the Role Policy Plays in Defining Trust Requirements

Ditton Manor, Slough, October 14th, 2011
Outline

- Austrian Approach
  - Position Paper by Platform Digital Austria
  - Main Findings on Privacy and Policy Challenges
- Relation to EU Initiatives
  - How can eID fit in?
Position paper

- Platform Digital Austria
  - Coordination and Strategy Committee of the Federal Government for eGovernment in Austria

- AG Cloud whitepaper (*unpublished*) on
  - Legal
  - Structural
  - Economic
  - Technical
  - Business Process aspects, effects, opportunities, and risks
Cloud and Government IT?

Cloud Computing in the Hype Cycle for Government Transformation, 2010

- Technology Trigger
- Peak of Inflated Expectations
- Trough of Disillusionment
- Slope of Enlightenment
- Plateau of Productivity

Years to mainstream adoption:
- 0 less than 2 years
- 2 to 5 years
- 5 to 10 years
- more than 10 years
- obsolete before plateau

As of July 2010

(From: "Hype Cycle for Government Transformation, 2010." 20 July 2010)
Overview of Findings

- **legal**
  - Data protection issues, ...
  - Influence on contract, ...
  - Procurement law

- **economical**
  - Standardization of IT infrastructure and services, ...
  - Functional adaptation cost adjustments,
  +/- Operating costs vs. capital costs

- **structural**
  + Faster service provisioning
  + Flexible bandwidth, ...
  - LockIn effects
  - Silo solutions
  - Compliance with governance rules, ...

- **technical**
  + Standardization, scalability, ...
  - Identity management
  - Technical audit, ...
Technical Aspects

- Standardization
- Scalability
- Identity and rights management
- Tenancy, security
- Cloud Management
- Technical revision
- Patch Management
Legal Aspects

- **Public Cloud:**
  - processing of personal data largely excluded.
  - no possibility of contractual adjustment
  - “Take it or leave it” contracts

- **Virtual Private Cloud:**
  - minor customization options compared to public cloud

- **Private Cloud:**
  - offers the best conditions to meet data protection
  - non-personal or not ‘very’ sensitive data are an option for Cloud usage

- Contractual issues, procurement law issues!
Data protection issues (1)

- **Controller vs. processor** (as of EU Data Protection Directive)
  - Controller remains responsible and accountable:
    - Data security measures: protection against accidental or unlawful destruction; unauthorized access; access logs
    - Data subject rights: information, deletion, correction, objection
  - ... can be hard to achieve with existing clouds

- **Cross-border transfer**
  - Defined within EEA (and with a few countries where comparable levels of protection of personal data are found)
  - Prior authorization by DPA otherwise
  - Generally prohibited in a few cases
Data protection issues (2)

- Applicable law in cross-border transfer
  - Controller has to fulfill domestic obligations
  - For cross-border permissions, the foreign processor needs to declare adherence to that obligations
    - Clouds possibly operating under various legislations
    - Further complexity with off-shoring

- Aspects to be considered
  - Access: Subject’s information rights
  - Destruction: Defined policies? Residual copies?
  - Retention: How long remains data in the cloud?
  - Compliance: Against what?
  - Audit: Periodic inspections?
E-Government may be

- Informational processes
  - e.g. law information system
  - no immediate data protection dimension

- Transactional processes
  - Processing personal data
  - Authentication / quality eID plays a major role
eID Cloud – something new?

- It is changing some of the basic assumptions
- The one to one model CLIENT-SERVER is no more possible
  - it is CLIENT - CLOUD - SERVER
    - for legal considerations
    - for contractual considerations
    - for technology considerations
    - for data protection and privacy considerations
- Most users will not yet recognize this difference
There is a difference

- eID and security will bring highly impacting changes
- The cloud will show the need to react
  - eID and technological quality
  - security and crypto-based technologies
  - policies and standards
- Yet there is a big difference
  - encryption/crypto-based confidentiality hardly possible
  - user control on the physical level non-existent
Cloud impacting eID?

- New approaches (like eID) must be “cloud compatible”
  - From the point of view of security
  - From the point of view of privacy and intellectual property protection

- We might possibly need to twist on both ends
  - In the eID domain
  - In the cloud domain
  - To yield contractual, legal/regulatory, commercial and technical acceptance
National strategy alone?
Digital Agenda for Europe

Propose by 2012 a Council and Parliament Decision to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents – issued by the public or the private sector).
STORK on EU eID interop.

- Interoperability framework on top of national eID infrastructure
- To a large extend relies on MS-to-MS trust
  - SP trusting MS PEPS
  - MS-to-MS protocol shielding IdPs
  - Different in “MW-model”
- How can a Cloud fit in?
Conclusions

- Cloud Computing on E-Government “radar”
  - Promises of cost reductions
  - Thus might assist getting efficiency gains
- Legal, technical, organizational issues
  - Citizen’s personal data in transactional services
  - May not interfere with citizen fundamental rights
  - Challenging with current public cloud contracts
- Quality eID in the Cloud to be addressed
Thank You!

Herbert.Leitold@a-sit.at