EUROPEAN DATA PROTECTION SUPERVISOR

Cloud Computing at EU Institutions

Achim Klabunde

DPO Meeting, Thessaloniki
7 November 2014

EUROPEAN DATA PROTECTION SUPERVISOR

Cloud Computing Policy initiatives

- **Commission**
  - *DG CNECT:*
    - *Communication on Strategy of 27 September 2012*
    - *Several working groups & initiatives*
    - *Research projects*
  - *DG HR:*
    - *Staff working document on implementation*
  - *DIGIT:*
    - *Cloud Virtual Task Force*
      - *Inter-institutional Work on principles for use of CC*
    - *Pilot for Cloud services procurement*
      - *Limited to basic requirements, not suitable for personal data*

EUROPEAN DATA PROTECTION SUPERVISOR

Cloud Computing Policy initiatives

- **ICTAC**:
  - *Survey on use in agencies*
- **EDPS**
  - *Opinion on Commission Communication*
  - *Survey and forthcoming Guidelines on Cloud Computing*
  - *Participation in CVTF*
  - *Participation on Pilot Tender documents*

EDPS Case Study: Case Management System

The CMS will support the entire cooperative process from the creation to the closure of a case and will also provide current information on the state of progress of cases.

- Document management
- Document storage
- Authenticity and integrity
- Confidentiality (configurable to specific users)
- Security
- Workflow

EUROPEAN DATA PROTECTION SUPERVISOR

EDPS Case Management System: Constraints

- Cases contain personal data -> need to respect data protection and security obligations
- EDPS very small, limited resources
- Outsourcing operation recommended for budgetary, resource and quality reasons
- Provider had developed own standard terms and conditions
- Necessity to negotiate compliant contract and service level agreement

EUROPEAN DATA PROTECTION SUPERVISOR

CMS: issues arising

- **Data Protection:** segregated data (level of multi-tenancy), deletion of back-ups (retention limits)
- **Service Compliance levels:** availability, response times, monitoring
- **Collateral tasks required when developing CMS:**
  - **Policies**: filing plan, records management, data retention
  - **Requirements**: Processes, data model, user interface …
  - **Implementation and acceptance:** test data, test cases, test specifications, testing environment, testers, scripts
  - **Before go live:** data migration, training, first level support, …

EUROPEAN DATA PROTECTION SUPERVISOR

Hosting options evaluation criteria

- Costs (OPEX)
- Staff requirements
- Procurement conditions
- Service quality level
  - completeness, availability, response times, …
- Security -> risk assessment
- Policy impact
- Legal requirements

(9 hosting options)

EUROPEAN DATA PROTECTION SUPERVISOR

Risk Assessment

- Definition of security objectives and data protection obligations
- SLA security parameters requirements vs. provider offerings
- All certified for ISO 27001 and other standards
- On-site visits at 2 potential 3rd party providers premises
  - Overall positive, but some issues detected:
    - » VM sharing, backup policy
- Provider adapted configuration and procedures relevant for SLA

CMS: specific safeguards

set out in 2 annexes:

Data Protection Specifications

These Data Protection Specifications stipulate confidentiality, security and personal data protection requirements …

Service Level Compliance Table

The service provider will *be fully responsible for the installation, operation, maintenance etc of the software and perform all related tasks, including back-ups*

EUROPEAN DATA PROTECTION SUPERVISOR

Data Protection Specifications I

- **Responsibility**
  - EDPS controller, contractor processor
  - Sub-processors limited, must respect equivalent standards
  - Cooperation (e.g. right to be forgotten) and indemnification
- **Location and applicable law**
  - Servers must be situated within EEA (in Austria)
  - Application of PPI, Reg 45 and Austrian law
  - Retention and access for law enforcement
- **Portability and termination**
  - Portability within 48 hours (specified format)
  - Right to suspend/terminate
  - Time limited retention, then destruction or return of all data

EUROPEAN DATA PROTECTION SUPERVISOR

Data Protection Specifications II

- **Security and confidentiality**
  - Articles 22 and 23 of Reg 45
  - Advance audit and audit on request to verify compliance
  - Warranty of appropriate operational, technical and organisational measures to protect personal data against accidental or unlawful destruction, alteration, unauthorised disclosure or access
  - Investment in reasonable means to ensure level of security appropriate to the risks and the nature of the processing
  - Mechanisms for data breaches and security incidents
  - Staff information on confidentiality, need-to-know access

EUROPEAN DATA PROTECTION SUPERVISOR

Service Compliance Requirements

- **Availability:** core hours, targets, reliability, service and business continuity
- **Performance**
- **Incidence management:** procedure, testing
- **Change management:** updates, tests
- **User management**
- **Security:** ISO/IEC 27001, secure deletion, staff
- **Segmentation** of EDPS data
- **Transparency:** information to EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

CMS: lessons learned

- SaaS is cheaper than licenses, hosting and support
  - *Costs include license, maintenance, operation, support*
- Difficult but necessary to negotiate security and data protection safeguards
  - *No alternative to 'privacy by design', retrofitting difficult if not impossible*
- The EU administration is big enough to obtain its own terms and conditions
  - *able to resist standard terms and conditions normally imposed by cloud providers*
  - *smaller bodies need to be able to negotiate their own solutions with the weight of the EU system behind them*

Next steps for EU Institutions (1)

- CVTF
  - Work on comprehensive cloud service requirements on-going
  - Results expected in 2015
  - Should contain comprehensive safeguards on data protection and security at contract and SLA level
  - Should also address operations of systems

EUROPEAN DATA PROTECTION SUPERVISOR

Next steps for EU Institutions (2)

- Pilot tender
  - **Learning exercise** for EU institutions
  - **Not** the blueprint for large scale cloudsourcing
  - invitation sent to Institutions, publication 2014
  - Limited service offerings
    - (only IaaS and PaaS), does not include SaaS
  - Limited area of applications
    - Only for *public* and *limited-basic* security requirements
    - Not aimed at processing of personal data

How to proceed?

- Precautionary approach for using cloud services
- Using cloud services may include international transfers
- Processing of special categories of data can be sensitive
- Comprehensive risk assessment necessary
- Case by case guidance from DPO/EDPS
- Guidelines to describe process

EUROPEAN DATA PROTECTION SUPERVISOR

Thank you for your attention!

For more information:

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS