Data protection legislation influence on cloud computing from local as well as EU perspective
• **EU approach to data protection (Directive 95/46)**
  • **Data controller**
    • determines that means and resources
  • **Data processor**
    • processing on behalf of data controller

• **Private/Public/Community/Hybrid**
  • privacy concerns higher where
    • control of data is „outsourced“
    • cross-border transfers (third countries)

• **Data protection legislation – main cloud issues**
  • Contractual processing of personal data
  • Data/information security
  • Export of personal data to third countries
Some open issues

- Who determines and who may change the terms of use?
- Data controller vs data processor
- The balance is lost – should we strive to maintain it or seek other options?

- **Transparency of cloud providers** – a lot to be done
- Data controllers have no answers to the most basic questions
  - Where will our clients’ personal data be processed?
  - How will the data be secured?
  - How and when (if ever) will they be deleted?
  - ..

- „We will process personal data in line with our Privacy Policy...“

- Economies of scope and security  vs  small data controller‘s security
• **Data security is only a part of data protection**
  - function creep effect
  - foreign jurisdictions – law enforcement agencies, civil proceedings etc.
  - are old mechanisms still adequate in the cloud computing era? e.g. Safe Harbor

• **Specific risks**
  - location transparency
  - multitenancy issues
  - vendor lock-in and portability of data
  - data erasure
  - security mechanisms and controls/audits (e.g. logging access to personal data)
  - disclosure during transfer/processing
  - ...

• **2011: increased demand for opinions of data protection authorities (DPAs)**
Datatilsynet (Denmark) - Google Apps to be used by Odense municipality
– data security and contractual relationship concerns
  – similar case in Norway

ULD (DPA of Schleswig-Holstein, Germany)
  – Safe Harbor insufficient, call for independent certification

Opinion of the International Working Group for Data Protection in Telecommunications (IWGDPT)
  – important for its international dimension

Opinion of the Article 29 Working Party
  – contains recommended content of contracts
  – consensus of EU regulators
International Working Group on Data Protection in Telecommunications


**General recommendations**

- **cloud computing must not lead to a lowering of data protection standards as compared with conventional data processing**
- **data controllers**: risk analysis (alone or with/by third parties)
- **cloud providers**: transparency, security, accountability, portability
- **legislators**: reassess the adequacy of existing legal frameworks allowing cross-border transfer of data and consider additional necessary privacy safeguards;
- **supervisory authorities**: awareness and supervision;
- further R&D (e.g., “sealed cloud”, homomorphismic encryption);
- certification and standardization.
• Recs(27) for data controllers and cloud providers
  – **location transparency/auditability**
  – physical location of all processing, including sub-contractors
  – **risk analysis (incl. portability analysis)**
  – actual erasure policies
  – encryption of moving data, data at rest
  – right to audit clauses (third parties allowed)
  – third country and own purpose clauses
  – **data subject rights clauses**
  – **independent third party auditing**
  – less critical data first, additional safeguards for sensitive data
  – distribution of responsibility

• IWGDPT opinon – basis for the international conference resolution.
• A29WP=European DPAs under Directive 95/46/EC + EC + EDPS
• **Opinion 05/2012 on Cloud Computing, 1 July 2012**
• detailed requests regarding the content of contracts
• particular chapter devoted to information security
• **imbalance of contractual power is not an excuse for data controllers**
• Safe Harbor self-certification does not cover all transfers within the Cloud; national legislations and DPAs may have additional requirements
• companies exporting data should not merely rely on the statement of the data importer claiming that he has a Safe Harbor certification.
• recommends
  – t.i. standard contractual clauses,
  – BCRs for processors
• third parties to assess adequacy through standardization, certification and auditing schemes
• IPRS in co-operation with Cloud Security Alliance Slovenia Chapter, Slovenia ISACA Chapter, Zavod e-Oblak - Eurocloud Slovenia

• **raise awareness**, offer a **control list** for Data Protection Act compliance

• issued 15 June 2012, **English translation available**
  – concept and specifics of cloud computing
  – cloud computing through main data protection concerns
  – control list (18)
  – practical examples (5)

• **Control list**
  – for **data controllers** and/or **cloud providers**
  – contains **specific** and minimal **controls**
  – **guideliness for implementation** of controls

---

If minimal controls are not implemented – reconsider moving to the cloud!
Examples of controls

- **The client** knows which **categories of data** will be transferred to the cloud.

- The client has to be **informed at all times about any sub-processors**, that may process its data on behalf of the cloud provider, and about the types of data processing they execute (transparency principle).

- Before using cloud services the client has conducted a **risk analysis**, alone or with a trusted third party.

- **Physical location** of the personal data is **known in every phase** of the processing.

- The provider **encrypts** the data transferred to or inside the cloud over **unprotected communication networks**.
1. **SME and cloud–based office software suite**  
   (location transparency, export to third countries, standard ToU)

2. **Public sector data controllers**  
   (legal ground)

3. **Two enterprise-level examples**  
   (focus on information security)

4. **SME and cloud–based CRM**  
   (ToU negotiations)

5. **Local cloud provider**  
   (using data centers in third countries)
Towards trust

- **Trust** is essential for *legal and practical acceptance* of cloud computing and exploitation of its potentials.

- **Cloud computing should not lower data protection standards!**

- **Trust must be complete and similar to trusting yourself:**
  - security
  - data protection
  - accessibility
  - reliability
  - fairness....

- **Privacy by Design** – how to **seize opportunities and salvage privacy**
- **Transparency** as a **necessary**, but not a sufficient precondition
- Strike a **new balance using third parties’ services**: standardization, certification (Privacy seals), independent third party auditing
Useful resources

- **Information Commissioner’s guidelines**
  - http://bit.ly/MeOGun (Slovenian)
  - http://bit.ly/RWSoeR (English)
  - **Summary for SMEs**

- **Article 29 Working Party opinion**

- **IWGDPT opinion (Sopot Memorandum)**
Thank you for your attention!

andrej.tomsic@ip-rs.si