# Data Protection and Cloud Computing: an Overview of the Legal Issues

Christopher Kuner
Partner, Hunton & Williams, Brussels
Research Assistant, University of Copenhagen

Nordic IT Law Conference
Copenhagen, 12 November 2010

# Topics

- What is cloud computing?
- Data protection (DP) issues (not exhaustive!)
  - Applicable law and jurisdiction
  - Legal bases for data processing
  - Data controllers and processors
  - International data transfers
  - Data security
  - Contractual issues
  - Views of DPAs
- Will discuss legal issues from an EU (not a national) point of view

# What is cloud computing?

- Data in the cloud are:
  - Stored in multi-tenant environments, like renting space in an apartment
  - Accessed by parties having differing trust levels (users, tenants, privileged cloud administrators)
  - Located in various countries
  - Enforced by various contractual obligations
  - Governed by various regulations and industry best practices
  - Secured by multiple technologies and services
- Not necessarily new, but represents an intensification of distributed computing, and a set of new business models

# Applicable law and jurisdiction (1)

- EU DP law applies to data processing carried out by:
  - Data controller established in a Member State, irrespective of where the data are processed; and
  - Non-EEA controller using equipment based in EEA
  - Note: data controller/processor distinction is key
- Legal obligations:
  - For data controller: full range of EU DP obligations (registration, information to individuals, etc.)
  - For data processors: ensure adequate security of processing
- Raises many questions:
  - What happens when multiple laws apply?
  - To whom can individuals and authorities turn in case of problems, and what are their rights and obligations?
  - What happens when an individual uses for private purposes a cloud provider established outside the EEA,, does EU law apply?

# Applicable law and jurisdiction (2)

- Applicable and jurisdiction for data protection issues cannot be wholly allocated by contract
- Moves by EU Commission for more harmonization of national law may help lesson the burden on companies
- Further discussion: Kuner, *Data Protection Law and International Jurisdiction on the Internet (Parts 1 and 2)*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1496847 and http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689495

# Legal bases for data processing

- Important in particular when registering data processing with DPAs
- Processing of personal data is allowed only when specific legal grounds apply
- Various legal bases may apply in the case of cloud computing:
  - Consent
  - Performance of a contract between the data subject and the data controller
  - Balancing of interests test
- Each one of these legal bases raises significant issues

# Data controllers and processors

- Distinction between the two terms is crucial in order to properly allocate responsibility and liability, and to determine applicable law
  - Companies outsourcing data to the cloud will normally be considered data controllers
  - Vendors are likely to be considered data processors, with (mostly) no DP compliance obligations, but with data security obligations
  - Status of parties is often an issue in contract negotiations
- However, DPAs may reclassify data processors as controllers (see SWIFT case and WP 29 Opinion 1/2010)

# International data transfers (1)

- Personal data may not be transferred from Europe without "adequate" data protection (Arts. 25 and 26 of Directive 95/46)
  - Some Member States (e.g., Germany) restrict the transfer of certain types of personal data under commercial law as well
- Over 30 other countries around the world also restrict international data transfers
  - See Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future", http://ssrn.com/abstract=1689483
- Features of cloud computing that impact on international data transfers:
  - How to identify the importing jurisdiction (data may be processed in and be accessible from many jurisdictions)
  - How to identify the importing entity (may be any affiliate or sub-processor of the cloud vendor)
  - How to satisfy EU data transfer requirements
- Some vendors have begun offering 'EU clouds'
- Political risk issues (e.g., China, law enforcement access)

# International data transfers (2)

- New tool to use when data are transferred between data processors (e.g., in cloud computing): new set of EU-approved standard contractual clauses for controller-to-processor transfers (proposed by ICC)
  - Commission adequacy decision issued on 5 February 2010
  - See Kuner, “The New EU Standard Contractual Clauses for International Data Transfers to Data Processors”, http://www.hunton.com/files/tbl_s47Details/FileUpload265/2865/EU_Standard_Contractual_Clauses_Intl_Data_Processors.pdf
- Important to note:
  - New clauses replace existing EU-approved clauses for controller to processor transfers
  - Clauses cover transfers from the EU to a data processor outside the EU, but not from a data processor in the EU to a subprocessor outside the EU (but DPAs may allow use of the new clauses in such situations as well)
  - Clauses allow for processor-to-processor transfers (require consent of data controller, written contract between processor and subprocessor)
- Possible use of clauses: master agreement signed by original data controller (customer) and co-signed by cloud computing provider and all its entities and vendors

# Data security

- EU Directives 95/46 and 2002/58 require appropriate technical and organisational measures to protect data against accidental or unlawful destruction, loss, alteration and unauthorised disclosure or access
- Numerous data breaches demonstrate that data security is perhaps the greatest risk of cloud computing
- Features of cloud computing that impact on security:
  - Proliferation of vendors, with lack of clear quality standards
  - Immature market with rapid developments
  - Risk of insolvency
- Requires intensive due diligence by customers
- Many important issues need to be covered by contract, e.g.:
  - Audit rights
  - Mandatory cooperation in case of breach
- Growing number of breach notification laws (and possibility for EU-wide requirement as Directive 95/46 is revised)

# Contractual issues

- Certain provisions should be included in the outsourcing contract in order to address data protection issues
- Examples
  - Clear description of the processing
  - Purpose of processing
  - Duty of service provider to comply with instructions
  - Data security measures
  - Cooperation between the parties
  - Any sub-contracting
  - Duty to inform the customer upon violations
  - Deletion of data after the project ends

# Views of data protection authorities

- Many DPAs are sceptical of cloud computing and the risks it presents
  - Example: Berlin DPA, Yearbook 2008, pp. 15-17
- Some national laws may restrict the use of cloud computing
- Key is ensuring that data protection responsibility is not diluted
- Use of cloud computing may become a labor law issue as well (works councils)

# Future directions

- Business models for cloud computing will evolve and will also affect the data protection issues
- Possible changes to Directive 95/46 to deal with cloud computing issues, e.g.:
  - Clarifying applicable law rules
  - Breach notification requirement
  - Stronger rights for individuals
- Binding corporate rules (BCRs) may provide one set of answers to legal issues, at least for processing within the same corporate group